Joe's signed it. The Publisher transmits the signed Distribution Agreement to the Authority, Ethical Inc.

Ethical Inc. now combines the signed TIA certificate and the Distribution Agreement into a single message, and signs the entire message using its private key. Ethical has now created a Publisher Identification message to go into its own stega-cipher channel in the content. Ethical Inc. now generates new stega-cipher masks and encodes this message into a copy of the content using a stega-cipher encoder. The Authority saves the masks as a Receipt in a database, along with information on the details of the transfer, including the title, artist and publisher.

Ethical then transfers this watermarked copy to the Joe's Online Emporium, the Publisher. Well known encryption methods could be used to protect the transfer between the Authority and the Publisher. The Authority may now destroy its copy, which the Publisher has received. The Publisher, Joe's Online Emporium now assumes responsibility for any copies made to its version of the content, which is a Publisher Master copy.

Finally, the Consumer, John Q. Public wishes to purchase a copy of the content from Joe's Online Emporium. Joe's Emporium sends the John Q. Public a short agreement via an electronic communication link, similar to Publisher's Distribution Agreement, only this is a Purchase Agreement, which lists

the content title
consumer identification
the terms of distribution
the consideration pas for the content
a brief statement of agreement with the terms above

John Q. Public signs this agreement with his private key and returns it to the Joe's Online Emporium. The Publisher, Joe's prepares to encode its own stega-cipher

watermark onto a copy of the content by generating a set of masks for the algorithm. Joe's Online Emporium then stores these masks (a receipt) in its own database, indexed by title and consumer. Joe's Online Emporium signs the agreement received from John Q. Public with the Emporium's own private key, and forwards it to the Authority, Ethical Inc., along with a copy of the masks. It is important to note that this communication should be done over a secured channel. The Authority verifies the Publisher and Consumer information and adds its own signature to the end of the message, approving the transaction, creating a Contract of Sale. The Authority adds the Publisher's receipt (mask set) to its database, indexed by the title, the publisher, and the consumer identification. The Authority signs the Contract of Sale by encrypting it with their private key. So anyone with the Authority's public key (any Publisher) could decrypt the Contract of Sale and verify it, once it was extracted from the content. The Publisher then transmits the signed Contract of Sale back to the Publisher, who uses a stega-cipher device to imprint this Contract as its own watermark over the content. The Publisher then transmits the newly watermarked copy to the Consumer, who is accepting responsibility for it. The Publisher destroys their version of the consumer's copy.

If this procedure is followed for all content distribution within such an online system then it should be possible for the Authority to identify the owner of a piece of content which appears to be unauthorized. The Authority could simply try its database of stega-cipher keys to decode the watermark in the content in question. For instance, if a copy of Seal's latest single originally distributed with stega-cipher watermarks showed up on an Internet ftp site the Authority should be able to extract a TIA Certificate and Distribution Agreement or a Contract of Sale identifying the responsible party. If a Publisher sold this particular copy to a Consumer, that particular publisher should be able to extract a Contract of Sale, which places responsibility with the Consumer. This is not a time critical application, so even if it takes days or weeks, it is still worthwhile.

In a modification to the protocol discussed above, each Publisher might act as its own Authority. However, in the context of online services, this could open avenues of fraud committed by the collusion of certain Publishers and Consumers. Using an Authority, or one of several available Authorities to keep records of Publisher-Consumer transactions and verify their details decreases the likelihood of such events.

It should also be obvious that a similar watermarking system could be used by an individual entity to watermark its own content for its own purposes, wether online or in physical media. For instance, a CD manufacturer could incorporate unique stega-cipher watermarks into specific batches of its compact discs to identify the source of a pirate ring, or to identify unauthorized digital copies made from its discs. This is possible because the stega-cipher encoding works with the existing formats of digital samples and does not add any new structures to the sample data that cannot be handled on electronic or mechanical systems which predate the stega-cipher.

VI. Increasing Confidence in the Stega-Cipher

The addition of a special pre-encoding process can make stega-cipher certificates even more secure and undeniable. Hash values may be incorporated which match exactly the content containing the watermark to the message in the watermark itself. This allows us a verification that the watermark decoded was encoded by whomever signed it into this precise location in this specific content.

Suppose one wants to use a 256 bit (32 byte) hash value which is calculated with a secure one-way hash function over each sample in each sample window that will contain the message. The hash starts with a seed value, and each sample that would be processed by the encoder when encoding the message is incorporated into the hash as it is processed. The result is a 256 bit number one can be highly confident is

unique, or sufficiently rare to make intentionally duplicating it with another series of samples difficult.

It is important that the hash function be insensitive to any changes in the samples induced by the stega-cipher itself. For instance, one might ignore the least significant bit of each sample when computing the hash function, if the stega-cipher was implemented using a least significant bit encode mode.

Based on the size of the non-hash message, one knows the hash-inclusive message requires 32 more bytes of space. One can now calculate the size of a signed encrypted copy of this message by signing and encrypting exactly as many random bytes as are in the message, and measuring the size of the output in bytes. One now knows the size of the message to be encoded. One can pre-process the sample stream as follows.

Proceed through the stega-cipher encode loop as described in the claims. Instead of encoding, however, calculate hash values for each window series which will contain the message, as each sample is processed. At the end of each instance of "encoding" take the resultant hash value and use it to create a unique copy of the message which includes the hash value particular to the series of sample windows that will be used to encode the message. Sign and encrypt this copy of the message, and save it for encoding in the same place in the sample stream.

A memory efficient version of this scheme could keep on hand the un-hashed message, and as it creates each new copy, back up in the sample stream to the first window in the series and actually encode each message, disposing of it afterwards.

The important result is evident on decoding. The decoding party can calculate the same hash used to encode the message for themselves, but on the encoded samples. If the value calculated by the decoding party does not match the value contained in the signed message, the decoder is alerted to the fact that this watermark was

transplanted from somewhere else. This is possible only with a hash function which ignores the changes made by the stega-cipher after the hash in the watermark was generated.

This scheme makes it impossible to transplant watermarks, even with the keys to the stega-cipher.

Appendix - Psuedo-code

```
const int WINDOW_RESET = 256;
const int WINDOW_SIZE = 128;
const int MARKER_BITS = 1024;
const int CHUNK_BITS = 2048 * 8;

int window_offset;
int msg_bit_offset;
int frequency_offset;
Boolean useCell;

/* 8 bits per bye, 1 byte per char */
unsigned char frequency_mask[WINDOW_SIZE/8];
unsigned char window_mask[WINDOW_RESET/8];
unsigned char msg_start_marker[MARKER_BITS/8];
unsigned char msg_end_marker[MARKER_BITS/8];
Int16 amplitude_sample_buffer[WINDOW_SIZE];
float power_frequency_buffer[WINDOW_SIZE];
unsigned char message_buffer[CHUNK_BITS/8];

void doFFT(Int16 *amp_sample_buffer, float *power_freq_buffer,int size);
void doInverseFFT(Int16 *amp_sample_buffer, float *power_freq_buffer,int size);
void initialize();
Bit getBit(unsigned char *buffer,int bitOffset);
Boolean map(Bit window_bit, Bit band_bit, int window, int frequency);
Boolean getSamples(Int16 *amplitude_sample_buffer,int samples);
void encode()

void initialize()
{
        /* message to be encoded is generated */
        /* message is prefixed with 1024 bit msg_start_marker */
        /* message is suffixed with 1024 bit msg_end _marker */
        /* remaining space at end of message buffer padded with random bits */
        window_offset = 0;
        msg_bit_offset = 0;
        frequency_offset = 0;
        frequency_mask loaded
        window_mask loaded
        zeroAmpSampleBuffer();
}
```

```
Boolean getSamples(Int16 *buffer,int samples)
{
        /* get samples number of samples and shift them contiguously into the sample
           buffer from right to left*/
        if(samples < samples available)
                return false;
        else
                return true;
}

void doFFT(Int16 *sample_buffer, float *spectrum_buffer, int size)
{
        calculate FFT on sample_buffer, for size samples
        store result in spectrum buffer
}

void doInverseFFT(Int16 *sample_buffer,float *spectrum_buffer,int size)
{
        calculate inverse FFT on spectrum_buffer
        store result in sampe_buffer
}

Bit getBit(unsigned char *buffer,in bitOffset)
{
        returns value of specified bit in specified buffer
        either 0 or 1, could use Boolean (true/false) values for bit set of bit off
}

Boolean map(Bit window_bit,Bit band_bit,int window, int frequency_
{
        /* this is the function that makes the information difficult to find */
        /* the inputs window_bit and band_bit depend only on the mask values
                used for encoding the information, they are 1) random, 2) secret */
        /* window and frequency values are used add time and frequency band dependent
                complexity to this function */
        /* this function is equivalent to a Boolean truth table with window * frequency * 4
        possible input combinations and 2 possible output */
        /* for any input combination, the output is either true or false */
        /* window ranges from 0 to WINDOW_RESET -1 */
        /* frequency ranges from 0 to WINDOW_SIZE - 1 */
        return calculated truth value
}
```

```
void encodeBit(float *spectrum_buffer,int freq_offset,Bit theBit)
{
        /* modifies the value of the cell in spectrum_buffer, indexed by freq_offset
                in a manner that distinguishes each of the 2 possible values of theBit,
                1 or 0
        */
        /* suggested method of setting the Least Significant bit of the cell == theBit */
        /* alternative method of rounding the value of the cell upward or downward to
                certain fractional values proposed
                i.e. <= .5 fractional remainder signifies 0, > .5 fraction remainder
                        signifies 1
        */
}

void encode()
{
        initialize();

        do {

        if(getSamples(amplitude_sample_buffer) == false)
                return

        doFFT(amplitude_sample_buffer,power_frequency_buffer,WINDOW_SIZE);

        for (frequency_offset = 0; frequency_offset < WINDOW_SIZE;
        frequency_offset++){

                useCell = map(getBit(window_mask,window_offset),
                                getBit(frequency_mask,frequency_offset),
                                window_offset, frequency_offset);

                if(useCell == true){
                        encodeBit(power_frequency_buffer,frequency_offset,
                                getBit(message_buffer,msg_bit_offset));
                        message_bit_offset ++;
                        if(msg_bit_offset == MESSAGEBITS){
                                initialize();
                                break; /* exit frequency loop */
                        }
                }
        }
```

```
            doInverseFFT(amplitude_sample_buffer,power_frequency_buffer,
                    WINDOW_SIZE);

            outputSamples(amplitude_sample_buffer);

            window_offset++;
            if(window_offset == WINDOW_RESET){
                    window_offset = 0;
            }


            }while(true);
    }
```

The encode() procedure processes an input sample stream using the specified frequency and window masks as well as a pre-formatted message to encode.

encode() processes the sample stream in windows of WINDOW_SIZE samples, contiguously distributed in the sample stream, so it advances WINDOW_SIZE samples at a time.

For each sample window, encode() first compute the FFT of the window, yielding its Power Spectrum Estimation. For each of these window PSEs, encode() then uses the map() function to determine where in each PSE to encode the bits of the message, which it reads from the message buffer, on ebit at a time. Each time map() returns true, encode() consumes another sample from the message.

After each window is encoded, encode() computes the inverse FFT on the PSE to generate a modified sample window, which is then output as the modified signal. It is important the sample windows NOT overlap in the sample stream, since this would potentially damage the preceeding encoding windows in the stream.

Once the message is entirely encoded, including its special end of message marker bit stream, encode() resets it internal variables to begin encoding the message once more in the next window. encode() proceeds in this manner until the input sample stream is exhausted.

```
enum {
        Synchronizing,
        Locked
}; /* decode states */
```

```
unsigned char message_end_buffer[MARKER_BITS];

Bit decodeBit(float *spectrum_buffer,int freq_offset)
{
        /* reads the value of the cell in spectrum_buffer, indexed by freq_offset
                in a manner that distinguishes each of the 2 possible values of an
                encoded bit, 1 or 0
        */
        /* suggested method of testing the Least Significant bit of the cell */
        /* alternative method of checking the value of the cell versus certain fractional
remainders proposed.
                i.e. <= .5 fractional remainder signifies 0, > .5 fraction remainder
                        signifies 1
        */
        return either 1 or 0 as appropriate
}

Boolean decode()
{
        /* Initialization */
        state = Synchronizing
        window_offset = 0;
        set frequency mask
        set window mask
        clear sample buffer
        int nextSamples = 1;
        int msg_start_offset = 0;
        clear message_end_buffer
        Bit aBit;
        Boolean bitsEqual;

        do {

                if(state == Synchronizing){
                        nextSamples = 1;
                        window_offset = 0;
                }
                else
                        nextSamples = WINDOW_SIZE;

                if(getSamples(amplitude_sample_buffer) == false)
                        return false;
```

```
doFFT(amplitude_sample_buffer,power_frequency_buffer,
        WINDOW_SIZE);  /* 2 */

for (frequency_offset = 0; frequency_offset < WINDOW_SIZE;
frequency_offset++){

    useCell = map(getBit(window_mask,window_offset),
            getBit(frequency_mask,frequency_offset),
            window_offset, frequency_offset);

    if(useCell == true){
            aBit = decodeBit(power_frequency_buffer,
                        frequency_offset);
            setBit(message_buffer,message_bit_offset,aBit);
            message_bit_offset ++;
    }
    else
            continue;
    if(state == Synchronizing){
            bitsEqual =
            compareBits(message_start_marker,message_buffer,
                    message_bit_offset);
            if(!bitsEqual){
                    message_bit_offset = 0;
                    misaligned = true;
                    break; /* exit frequency loop */
            }
            else if (message_bit_offset == MARKER_BITS)
                    state == Locked;
    }
    else {
            /* locked onto encoded stream */
            shift aBit into right side of message_end_buffer
            bitsEqual = compareBits(message_end_buffer,
                    msg_end_marker,MARKER_BITS);
            if(bitsEqual)
                    return true;
    }
}

}while (true);
}
```

The decode() procedure scans an input sample stream using specified window and frequency masks, until it either decodes a valid message block, storing it in a message buffer, or exhausts the sample stream.

The decode() procedure starts in state Synchronizing, in which it does not know where in the sample stream the encoding windows are aligned. The procedure advances the sample window through the sample stream one sample at a time, performing the FFT calculation on each window, and attempting to decode valid message bits from the window. As it extracts each bit using the map() function, the decode() procedure compares these bits against the start of message marker. As soon as a mismatch is detected, the decode() procedure knows it is not yet properly aligned to an encoding window, and immediately ceases decoding bits from the current window and moves to the next window, offset by 1 sample. The decode() procedure continues in this manner until it matches successfully the complete bitstream of a start of message marker. At this point the decode() procedure assumes it is aligned to an encoded message and can then decode bits to the message buffer quickly, advancing the sample window fully at each iterations. It is now in Locked mode. For each bit it stores in the message buffer when in Locked mode, the decode() procedure also shifts the same bit value into the least significant bit of the message_end_buffer. After each bit is decoded in Locked mode, the decode() procedure checks compares the message_end_buffer with the msg_end_marker in a bit by bit manner. When a complete match is found, decode() is finished and returns true. If the sample stream is exhausted before this occurs, decode() returns false. If decode() returns true, a valid message is stored in the message buffer, including the start and end of message markers.

Claims

1. A steganographic method comprising the steps of :

using random keys in combination with steganography to encode additional information into digitized samples such that a signal generated from the modified sample stream is not significantly degraded and such that the additional information cannot be extracted without the keys and such that the signal generated from the modified sample stream will be degraded by attempts to erase, scramble, or otherwise obliterate the encoded additional information.

2. An apparatus for encoding or decoding a message, represented as series of data bits into or out of a series of digitized samples, comprising:

a) a sample buffer for holding and accessing and transforming digitized samples;

b) a digital signal processor capable of performing fast fourier transforms;

c) a memory to contain information representing

1) primary mask,
2) convolutional mask,
3) start to message delimiter,
4) a mask calculation buffer,
5) a message buffer,
6) an integer representing a message bit index,
7) a position integer M representing message size,
8) an integer representing an index into said primary mask,
9) an integer representing an index into said convolution mask,
10) an integer representing the state of a decode process,
11) a table representing a map function;
12) a flag indicating a complete message has been decoded or encoded,

13) a positive integer S representing a number of samples to read into said sample buffer, and

14) a flag indicating the size of a message which has been decoded;

d) an input to acquire digital samples;

e) an output to output modified digital samples;

f) an input for inputting the values of (c1) - (c5) and (c11) and (c13);

g) an output to output the message stored in (c5) as the result of a decode process and the value of (c10) to an attached digital circuit;

h) at least one data bus to transfer information from

(d) to (a),

(a) to (b),

(b) to (a),

(a) to (e),

(f) to (c), and

(c) to (e); and

i) a clock which generates a clock signal to drive (b) and control the operation of the apparatus.

3. A method of encoding information into a sample stream of data, said method comprising the steps of:

A) generating a mask set to be used for encoding, said set including:

a random or pseudo-random primary mask,

a random or pseudo-random convolution mask,

a random or pseudo-random start of message delimiter, wherein said mask set can be concatenated and manipulated as a single bit stream;

B) obtaining a message to be encoded;

C) generating a message bit steam to be encoded such that the stream includes

1) a start of message delimiter, and

2) an integer representing the number of message bytes to follow the message;

D) loading the message bit stream, a map table, the primary mask, the convolution mask, and the start of message delimiter into a memory;

E) resetting a primary mask index, a convolution mask and message bit index, and setting the message size integer equal to the total number of bits in the message bit stream;

F) clearing a message encoded flag;

G) reading a window of samples from a sample input device and storing them sequentially in a sample buffer;

H) resetting the primary mask index and looping through the sample buffer from a first sample to a last sample incrementing the primary mask index each time a sample is visited, such that for each sample position, a value of the mapping function is computed, which is either true or false, by using a bit of the primary mask representing a current sample and a bit of the convolution mask indicated by the convolution index to calculate an offset in the map table;

I) obtaining the bit value stored in the map table and encoding the bit of the message indicated by the message bit index into the current sample if the bit value obtained from the map table is a certain value and incrementing the message bit index, determining whether the message bit index equals the number of message bits, and if it does re-performing step A), setting the message encoded flag, and exiting the loop;

J) outputting the modified samples in the sample buffer, and if the message encoded flag is set jumping back to said step E);

K) incrementing the convolution index, wherein if the convolution index equals the length of the convolution mask in bits then set the convolution index to 0; and

L) jumping back to step G).

4. A method of encoding information into a sample stream of data, comprising the steps of:

A) generating a mask set to be used for encoding, including:
a random or pseudo-random primary mask,
a random or pseudo-random convolution mask, and
a random or pseudo-random start of message delimiter, wherein said mask set can be concatenated and manipulated as a single bit stream;

B) inputting a message to be encoded;

C) generating a message bit stream to be encoded including
a start of message delimiter, and
an integer representing of number of message bytes to follow the message;

D) loading the message bit stream, a map table, and the mask set into a memory;

E) resetting a primary mask index, a convolution mask and message bit index, setting the message size index equal to the number of bits in the message bitstream, and clearing a message encoded flag;

F) reading a window of samples of the inputted message and storing the samples sequentially in a sample buffer;

G) computing a spectral transform of the samples in the buffer;

H) obtaining the bit value stored in the map table, wherein if the bit value is true, then encoding the bit of the message indicated by the message bit index into the current sample and incrementing the message bit index, where the message bit index equals the number of message bits, and then reperforming step A), setting the message encoded flag, and exiting the loop;

I) computing the inverse spectral of the spectral values stored in the sample buffer;

J) outputting the values in the sample buffer, and if the sample encoded flag is set, then clear the flag and jump back to step E);

K) incrementing the convolution index and when the convolution index equals the length of the convolution mask in bits resetting the convolution index; and

L) jumping back to step F).

5. The method of claim 3 wherein the encoding of the message bit into the sample in step I includes encoding a single bit of the sample to match the message bit.

6. The method of claim 4 wherein the encoding of the message bit into the sample in step H includes altering the sample value such that said sample value falls within a prespecified range of valves relative to its original value.

7. A method of decoding information from a sample stream of data, comprising the steps of:

A) obtaining a mask set including:

(1) a random or pseudo-random primary mask,

(2) a random or pseudo-random convolution mask, and

(3) a random or pseudo-random start of message delimiter;

B) loading a map table, and the mask set into a memory;

C) resetting a primary mask index and convolution mask index and setting a message size integer equal to 0;

D) clearing a message decoded flag;

E) setting a state of the decode process to SYNCHRONIZED;

F) checking the state of the decode process and if the decode state is UNSYNCHRONIZED, setting a number of samples to equal 1 and resetting the convolution index to 0; otherwise, setting the number of samples to equal S ($S \geq 1$);

G) reading the number of samples specified in step F) into a sample buffer;

H) resetting the primary mask index, and looping through the sample buffer from the first sample to the last sample, incrementing the primary mask index each time, and for each sample position, computing the value of a mapping function to calculate an offset into the map table;

I) obtaining the bit value in the map table, and if the value is true, decoding the bit of the message indicated by the message bit index, storing the bit into the message buffer at the message bit index, and incrementing the message bit index;

J) comparing the decoded bits in the message buffer to the start of message delimiter, and if the number of bits in the message buffer is less than or equal to the number of bits in the start of message delimiter and the bits match, then setting the state of the decode process to SYNCHRONIZED; otherwise setting the state of the decode process to UNSYNCHRONIZED;

K) if the state of the decode process is SYNCHRONIZED and the number of bits in the message buffer is greater than or equal to the sum of the number of bits of the start of delimiter and the message size, then setting the state of the decode process to SYNC-AND-SIZE and copying certain bits from the message buffer to a message size integer container;

L) if the state of the decode process is SYNC-AND-SIZE and the number of bits in the message buffer divided by 8 is greater than or equal to the message size, then setting the message decoded flag, outputting the message and the message decoded flag and ending the method;

M) incrementing the convolution index, and if the convolution index equals the number of bits in the convolution mask resetting the convolution index; and

N) jumping to step F).

8. A method of decoding information from sampled data, comprising the steps of:

A) Obtaining a mask set including

(1) a random or pseudo-random primary mask,

(2) a random or pseudo-random convolution mask, and

(3) a random or pseudo-random start of message delimiter;

B) loading a map table, and the mask set into a memory;

C) resetting a primary mask index and convolution mask index and setting a message size integer equal to 0;

D) clearing a message decoded flag;

E) setting a state of the decode process to SYNCHRONIZED;

F) checking the state of the decode process and if the decode state is UNSYNCHRONIZED, setting a number of samples to equal 1 and resetting the convolution index to 0; otherwise, setting the number of samples to equal S (S>1);

G) reading the number of samples specified in step F) into a sample buffer;

H) computing a spectral transform of the samples stored in the sample buffer;

I) resetting the primary mask index and looping through the sample buffer from the first sample to the last sample, incrementing the primary mask index each time, and for each sample position, computing the value of a mapping function by using the bit of the primary mask corresponding to the primary mask index and the bit of the convolution masks indicated by the convolution phase to calculate an offset into the map table representing the mapping function;

J) obtaining a bit value stored in the map, and if the value is true, decoding the bit of the message indicated by the message bit index from the current sample, storing the bit into the message buffer at the message bit index, and incrementing the message bit index;

K) comparing the decoded bits in the message buffer to the start of message delimiter, and if the number of bits in the message buffer is less than or equal to the number of bits in the start of message delimiter and the bits match, then

setting the state of the decode process to SYNCHRONIZED; otherwise, setting the state of the decode process UNSYNCHRONIZED;

L) if the state of the decode process is SYNCHRONIZED, and the number of bits in the message buffer is greater than or equal to the sum of the number of bits of the start of delimiter and the message size, then setting the state of the decode process to SYNC-AND-SIZE and copying certain bits from the message buffer to a message size integer container;

M) if the state of the decode process is SYNC-AND-SIZE and the number of bits in the message buffer divided by 8 is greater than or equal to the message size, then setting the message decoded flag, outputting the message and the message decoded flag and ending the method;

N) incrementing the convolution index, wherein if the convolution index equals the number of bits in the convolution mask, then resetting the convolution index; and

O) jumping to step F).

9. The method of claim 7 wherein the decoding of the message bit from the sample in step I includes reading a single bit of the sample.

10. The method of claim 7 wherein the decoding of the message bit from the sample in step I includes mapping a range of sample values onto a particular message bit value.

11. The method of claim 4 wherein the map table is defined such that any index of the map table directs the process to encode information.

12. The method of claim 1 wherein the samples are obtained from a sample stream representing digitized sound or music.

13. The method of claim 12 wherein the identical encode process is performed on two sample streams representing channel A and channel B of digitized stereo sound.

14. The method of claim 12 wherein the sample streams represent channel A and channel B of digitized stereo sound and are interleaved before being input as a single sample stream and are separated into two channels upon output.

15. The method of claim 1 wherein the samples are obtained from a sample stream representing digitized video.

16. The method of claim 1 wherein the samples are obtained from a sample stream representing a digitized image.

17. The apparatus of claim 2, further comprising a tamper-resistant packaging, enclosing said apparatus wherein circuitry and information stored therein are destroyed if said packaging is opened.

18. The method of claim 3, further comprising a pre-encoding step which customizes the message to be encoded including: calculating over which windows in the samples stream a message will be encoded, computing a secure one way hash function of the samples in those windows, and placing the resulting hash values in the message before the message is encoded;

wherein the hash calculating step includes: calculating the size of the original message plus the size of an added hash value, and pre-processing the sample stream for the purpose of calculating hash values of each series of windows that will be used to encode the message and creating a modified copy of the message containing the hash value such that each message containing a hash value matches each window series uniquely.

19. The method of claim 1, wherein an authority for on line distribution of content encodes at least one of the following items into a sample stream ;

the title,

the artist,

the copyright holder,

the body to which royalties should be paid, and

general terms for publisher distribution.

20. The method of claim 19, wherein the authority combines at least one item with a secure private key signed message from a publisher containing at least one of the following pieces of information:

the title,

the publisher's identification,

the terms of distribution,

any consideration paid for the right to distribute the content,

a brief statement of agreement, and

the publisher signs and encrypts the combined message using a public key cryptosystem and encodes the signed and encrypted message into the sample stream.

21. The method of claim 20, wherein a publisher obtains the encoded sample stream and additionally obtains information form the authority and combines this with a message received from a consumer, which has been signed using a public key cryptosystem and wherein the signed message contains at least one of the following data

the content title,

consumer identification,

the terms of distribution,

the consideration paid for the content,

a brief statement of agreement, and

the publisher uses a public key cryptosystem to sign the combined information and finally encodes the signed information.

22. The method of claim 1, wherein the sample stream is obtained from at least one audio track contained within a digitized movie, video game software, or other software.

23. The method of claim 1, wherein the sample stream is obtained from at least one digitized movie or still image contained within a video game or other software.

24. The method of claim 1, wherein encoded information is contained in the differences or relationship between samples or groups of samples.

25. The method of claim 4, wherein the encoding of the message bit into the sample in step H includes encoding a single bit of the sample to match the message bit.

26. The method of claim 3, wherein the encoding of the message bit into the sample in step I includes altering the sample value such that said sample value falls within a prespecified range of valves relative to its original value.

27. The method of claim 8, wherein the decoding of the message bit in step J includes reading a single bit of the sample.

28. The method of claim 8, wherein the decoding of the message bit in step J includes mapping a range of supply values onto a particular message bit value.

29. The method of claim 3, wherein the map table is defined such that any index of the map table directs the process to encode information.

30. The method of claim 7, wherein the map table is defined such that any index of the map table directs the process to encode information.

31. The method of claim 8, wherein the map table is defined such that any index of the map table directs the process to encode information.

32. The method of claim 4, further comprising a pre-encoding step which customizes the message to be encoded including: calculating over which windows in the samples stream a message will be encoded, computing a secure one way hash function of the samples in those windows, and placing the resulting hash values in the message before the message is encoded;

wherein the hash calculating step includes: calculating the size of the original message plus the size of an added hash value, and pre-processing the sample stream for the purpose of calculating hash values of each series of windows that will be used to encode the message and creating a modified copy of the message containing the hash value such that each message containing a hash value matches each window series uniquely.--

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number:
H04L 9/00	A1	WO 97/26732
		(43) International Publication Date: 24 July 1997 (24.07.97)

(21) International Application Number: PCT/US97/00651

(22) International Filing Date: 16 January 1997 (16.01.97)

(30) Priority Data:
08/587,943 17 January 1996 (17.01.96) US

(71) Applicant: THE DICE COMPANY [US/US]; 20191 E. Country Club Drive, Townhouse 4, Aventura, FL 33180 (US).

(72) Inventors: MOSKOWITZ, Scott, A.; 20191 E. Country Club Drive, Townhouse 4, Aventura, FL 33180 (US). COOPERMAN, Marc; 2929 Ramona, Palo Alto, CA 94306 (US).

(74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).

(81) Designated States: AL, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GE, HU, IL, IS, JP, KP, KR, LC, LK, LR, LT, LV, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD FOR STEGA-CIPHER PROTECTION OF COMPUTER CODE

(57) Abstract

A method for protecting computer code copyrights by encoding the code into a data resource with a digital watermark. The digital watermark contains licensing information interwoven with essential code resources encoded into data resources. The result is that while an application program can be copied in an uninhibited manner, only the licensed user having the license code can access essential code resources to operate the program and any descendant copies bear the required license code.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic			SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

METHOD FOR STEGA-CIPHER PROTECTION OF COMPUTER CODE

FIELD OF INVENTION

With the advent of computer networks and digital multimedia, protection of intellectual property has become a prime concern for creators and publishers of digitized copies of copyrightable works, such as musical recordings, movies, video games, and computer software. One method of protecting copyrights in the digital domain is to use "digital watermarks."

The prior art includes copy protection systems attempted at many stages in the development of the software industry. These may be various methods by which a software engineer can write the software in a clever manner to determine if it has been copied, and if so to deactivate itself. Also included are undocumented changes to the storage format of the content. Copy protection was generally abandoned by the software industry, since pirates were generally just as clever as the software engineers and figured out ways to modify the software and deactivate the protection. The cost of developing such protection was not justified considering the level of piracy which occurred despite the copy protection.

Other methods for protection of computer software include the requirement of entering certain numbers or facts that may be included in a packaged software's manual, when prompted at start-up. These may be

overcome if copies of the manual are distributed to unintended users, or by patching the code to bypass these measures. Other methods include requiring a user to contact the software vendor and to receive "keys" for unlocking software after registration attached to some payment scheme, such as credit card authorization. Further methods include network-based searches of a user's hard drive and comparisons between what is registered to that user and what is actually installed on the user's general computing device. Other proposals, by such parties as AT&T's Bell Laboratories, use "kerning" or actual distance in pixels, in the rendering of text documents, rather than a varied number of ASCII characters. However, this approach can often be defeated by graphics processing analogous to sound processing, which randomizes that information. All of these methods require outside determination and verification of the validity of the software license.

Digital watermarks can be used to mark each individual copy of a digitized work with information identifying the title, copyright holder, and even the licensed owner of a particular copy. When marked with licensing and ownership information, responsibility is created for individual copies where before there was none. Computer application programs can be watermarked by watermarking digital content resources used in conjunction with images or audio data. Digital watermarks can be encoded with random or pseudo random keys, which act as secret maps for locating the watermarks. These keys make it impossible for a party to find the watermark without having the key. In addition, the encoding method can be enhanced to force a party to cause damage to a watermarked data stream when trying to erase a random-key watermark. Digital watermarks are described in "Steganographic Method and Device" - The DICE Company, Serial No. 08/489,172, the disclosure of which is hereby incorporated by reference.

Other information is disclosed in "Technology: Digital Commerce", Denise Caruso, New York Times, August 7, 1995; and "Copyrighting in the Information Age", Harley Ungar, ONLINE MARKETPLACE, September 1995, Jupiter Communications.

Additionally, other methods for hiding information signals in content signals, are disclosed in U.S. Patent No. 5,319,735 - Preuss et al. and U.S. Patent No. 5,379,345 - Greenberg.

It is desirable to use a "stega-cipher" or watermarking process to hide the necessary parts or resources of the executable object code in the digitized sample resources. It is also desirable to further modify the underlying structure of an executable computer application such that it is more resistant to attempts at patching and analysis by memory capture. A computer application seeks to provide a user with certain utilities or tools, that is, users interact with a computer or similar device to accomplish various tasks and applications provide the relevant interface. Thus, a level of authentication can also be introduced into software, or "digital products," that include digital content, such as audio, video, pictures or multimedia, with digital watermarks. Security is maximized because erasing this code watermark without a key results in the destruction of one or more essential parts of the underlying application, rendering the "program" useless to the unintended user who lacks the appropriate key. Further, if the key is linked to a license code by means of a mathematical function, a mechanism for identifying the licensed owner of an application is created.

It is also desirable to randomly reorganize program memory structure intermittently during program run time, to prevent attempts at memory capture or object code analysis aimed at eliminating licensing or ownership information, or otherwise modifying, in an unintended manner, the functioning of the application.

In this way, attempts to capture memory to determine underlying functionality or provide a "patch" to facilitate unauthorized use of the "application," or computer program, without destroying the functionality and thus usefulness of a copyrightable computer program can be made difficult or impossible.

It is thus the goal of the present invention to provide a higher level of copyright security to object code on par with methods described in digital watermarking systems for digitized media content such as pictures, audio, video and multimedia content in its multifarious forms, as described in previous disclosures, "Steganographic Method and Device" and "Human Assisted Random Key Generation and Application for Digital Watermark System", filed on even date herewith, the disclosure of which is hereby incorporated by reference.

It is a further goal of the present invention to establish methods of copyright protection that can be combined with such schemes as software metering, network distribution of code and specialized protection of software that is designed to work over a network, such as that proposed by Sun Microsystems in their HotJava browser and Java programming language, and manipulation of application code in proposed distribution of documents that can be exchanged with resources or the look and feel of the document being preserved over a network. Such systems are currently being offered by companies including Adobe, with their Acrobat software. This latter goal is accomplished primarily by means of the watermarking of font, or typeface, resources included in applications or documents, which determine how a bitmap representation of the document is ultimately drawn on a presentation device.

The present invention includes an application of the technology of "digital watermarks." As described in previous disclosures, "Steganographic Method and

DISH-Blue Spike-842
Exhibit 1004, Page 0681

Device" and "Human Assisted Random Key Generation and Application for Digital Watermark System," watermarks are particularly suitable to the identification, metering, distributing and authenticating digitized content such as pictures, audio, video and derivatives thereof under the description of "multimedia content." Methods have been described for combining both cryptographic methods, and steganography, or hiding something in plain view. Discussions of these technologies can be found in Applied Cryptography by Bruce Schneier and The Code Breakers by David Kahn. For more information on prior art public-key cryptosystems see US Pat No 4,200,770 Diffie-Hellman, 4,218,582 Hellman, 4,405,829 RSA, 4,424,414 Hellman Pohlig. Computer code, or machine language instructions, which are not digitized and have zero tolerance for error, must be protected by derivative or alternative methods, such as those disclosed in this invention, which focuses on watermarking with "keys" derived from license codes or other ownership identification information, and using the watermarks encoded with such keys to hide an essential subset of the application code resources.

SUMMARY OF THE INVENTION

It is thus a goal of the present invention, to provide a level of security for executable code on similar grounds as that which can be provided for digitized samples. Furthermore, the present invention differs from the prior art in that it does not attempt to stop copying, but rather, determines responsibility for a copy by ensuring that licensing information must be preserved in descendant copies from an original. Without the correct license information, the copy cannot function.

An improvement over the art is disclosed in the present invention, in that the software itself is a set of commands, compiled by software engineer, which can be

configured in such a manner as to tie underlying functionality to the license or authorization of the copy in possession by the user. Without such verification, the functions sought out by the user in the form of software cease to properly work. Attempts to tamper or "patch" substitute code resources can be made highly difficult by randomizing the location of said resources in memory on an intermittent basis to resist most attacks at disabling the system.

DETAILED DESCRIPTION

An executable computer program is variously referred to as an application, from the point of view of a user, or executable object code from the point of view of the engineer. A collection of smaller, atomic (or indivisible) chunks of object code typically comprise the complete executable object code or application which may also require the presence of certain data resources. These indivisible portions of object code correspond with the programmers' function or procedure implementations in higher level languages, such as C or Pascal. In creating an application, a programmer writes "code" in a higher level language, which is then compiled down into "machine language," or, the executable object code, which can actually be run by a computer, general purpose or otherwise. Each function, or procedure, written in the programming language, represents a self-contained portion of the larger program, and implements, typically, a very small piece of its functionality. The order in which the programmer types the code for the various functions or procedures, and the distribution of and arrangement of these implementations in various files which hold them is unimportant. Within a function or procedure, however, the order of individual language constructs, which correspond to particular machine instructions is important, and so functions or procedures are considered

DISH-Blue Spike-842
Exhibit 1004, Page 0683

indivisible for purposes of this discussion. That is, once a function or procedure is compiled, the order of the machine instructions which comprise the executable object code of the function is important and their order in the computer memory is of vital importance. Note that many "compilers" perform "optimizations" within functions or procedures, which determine, on a limited scale, if there is a better arrangement for executable instructions which is more efficient than that constructed by the programmer, but does not change the result of the function or procedure. Once these optimizations are performed, however, making random changes to the order of instructions is very likely to "break" the function. When a program is compiled, then, it consists of a collection of these sub-objects, whose exact order or arrangement in memory is not important, so long as any sub-object which uses another sub-object knows where in memory it can be found.

The memory address of the first instruction in one of these sub-objects is called the "entry point" of the function or procedure. The rest of the instructions comprising that sub-object immediately follow from the entry point. Some systems may prefix information to the entry point which describes calling and return conventions for the code which follows, an example is the Apple Macintosh Operating System (MacOS). These sub-objects can be packaged into what are referred to in certain systems as "code resources," which may be stored separately from the application, or shared with other applications, although not necessarily. Within an application there are also data objects, which consist of some data to be operated on by the executable code. These data objects are not executable. That is, they do not consist of executable instructions. The data objects can be referred to in certain systems as "resources."

DISH-Blue Spike-842
Exhibit 1004, Page 0684

When a user purchases or acquires a computer program, she seeks a computer program that "functions" in a desired manner. Simply, computer software is overwhelmingly purchased for its underlying functionality. In contrast, persons who copy multimedia content, such as pictures, audio and video, do so for the entertainment or commercial value of the content. The difference between the two types of products is that multimedia content is not generally interactive, but is instead passive, and its commercial value relates more on passive not interactive or utility features, such as those required in packaged software, set-top boxes, cellular phones, VCRs, PDAs, and the like. Interactive digital products which include computer code may be mostly interactive but can also contain content to add to the interactive experience of the user or make the underlying utility of the software more aesthetically pleasing. It is a common concern of both of these creators, both of interactive and passive multimedia products, that "digital products" can be easily and perfectly copied and made into unpaid or unauthorized copies. This concern is especially heightened when the underlying product is copyright protected and intended for commercial use.

The first method of the present invention described involves hiding necessary "parts" or code "resources" in digitized sample resources using a "digital watermarking" process, such as that described in the "Steganographic Method and Device" patent application. The basic premise for this scheme is that there are a certain sub-set of executable code resources, that comprise an application and that are "essential" to the proper function of the application. In general, any code resource can be considered "essential" in that if the program proceeds to a point where it must "call" the code resource and the code resource is not present in memory, or cannot be loaded, then the program fails.

DISH-Blue Spike-842
Exhibit 1004, Page 0685

However, the present invention uses a definition of "essential" which is more narrow. This is because, those skilled in the art or those with programming experience, may create a derivative program, not unlike the utility provided by the original program, by writing additional or substituted code to work around unavailable resources. This is particularly true with programs that incorporate an optional "plug-in architecture," where several code resources may be made optionally available at run-time. The present invention is also concerned with concentrated efforts by technically skilled people who can analyze executable object code and "patch" it to ignore or bypass certain code resources. Thus, for the present embodiment's purposes, "essential" means that the function which distinguishes this application from any other application depends upon the presence and use of the code resource in question. The best candidates for this type of code resources are NOT optional, or plug-in types, unless special care is taken to prevent work-a-rounds.

Given that there are one or more of these essential resources, what is needed to realize the present invention is the presence of certain data resources of a type which are amenable to the "stega-cipher" process described in the "Steganographic Method and Device" patent application. Data which consists of image or audio samples is particularly useful. Because this data consists of digital samples, digital watermarks can be introduced into the samples. What is further meant is that certain applications include image and audio samples which are important to the look and feel of the program or are essential to the processing of the application's functionality when used by the user. These computer programs are familiar to users of computers but also less obvious to users of other devices that run applications that are equivalent in

DISH-Blue Spike-842
Exhibit 1004, Page 0686

some measure of functionality to general purpose computers including, but not limited to, set-top boxes, cellular phones, "smart televisions," PDAs and the like. However, programs still comprise the underlying "operating systems" of these devices and are becoming more complex with increases in functionality.

One method of the present invention is now discussed. When code and data resources are compiled and assembled into a precursor of an executable program the next step is to use a utility application for final assembly of the executable application. The programmer marks several essential code resources in a list displayed by the utility. The utility will choose one or several essential code resources, and encode them into one or several data resources using the stega-cipher process. The end result will be that these essential code resources are not stored in their own partition, but rather stored as encoded information in data resources. They are not accessible at run-time without the key. Basically, the essential code resources that provide functionality in the final end-product, an executable application or computer program, are no longer easily and recognizably available for manipulation by those seeking to remove the underlying copyright or license, or its equivalent information, or those with skill to substitute alternative code resources to "force" the application program to run as an unauthorized copy. For the encoding of the essential code resources, a "key" is needed. Such a key is similar to those described in the "Steganographic Method and Device." The purpose of this scheme is to make a particular licensed copy of an application distinguishable from any other. It is not necessary to distinguish every instance of an application, merely every instance of a license. A licensed user may then wish to install multiple copies of an application, legally or with authorization. This method, then, is to

DISH-Blue Spike-842
Exhibit 1004, Page 0687

choose the key so that it corresponds, is equal to, or is a function of, a license code or license descriptive information, not just a text file, audio clip or identifying piece of information as desired in digital watermarking schemes extant and typically useful to stand-alone, digitally sampled content. The key is necessary to access the underlying code, i.e., what the user understands to be the application program.

The assembly utility can be supplied with a key generated from a license code generated for the license in question. Alternatively, the key, possibly random, can be stored as a data resource and encrypted with a derivative of the license code. Given the key, it encodes one or several essential resources into one or several data resources. Exactly which code resources are encoded into which data resources may be determined in a random or pseudo random manner. Note further that the application contains a code resource which performs the function of decoding an encoded code resource from a data resource. The application must also contain a data resource which specifies in which data resource a particular code resource is encoded. This data resource is created and added at assembly time by the assembly utility. The application can then operate as follows:

1) when it is run for the first time, after installation, it asks the user for personalization information, which includes the license code. This can include a particular computer configuration;

2) it stores this information in a personalization data resource;

3) Once it has the license code, it can then generate the proper decoding key to access the essential code resources.

Note that the application can be copied in an uninhibited manner, but must contain the license code issued to the licensed owner, to access its essential code resources. The goal of the invention, copyright

DISH-Blue Spike-842
Exhibit 1004, Page 0688

protection of computer code and establishment of responsibility for copies, is thus accomplished.

This invention represents a significant improvement over prior art because of the inherent difference in use of purely informational watermarks versus watermarks which contain executable object code. If the executable object code in a watermark is essential to an application which accesses the data which contains the watermark, this creates an all-or-none situation. Either the user must have the extracted watermark, or the application cannot be used, and hence the user cannot gain full access to the presentation of the information in the watermark bearing data. In order to extract a digital watermark, the user must have a key. The key, in turn, is a function of the license information for the copy of the software in question. The key is fixed prior to final assembly of the application files, and so cannot be changed at the option of the user. That, in turn, means the license information in the software copy must remain fixed, so that the correct key is available to the software. The key and the license information are, in fact, interchangeable. One is merely more readable than the other. In the earlier developed "Steganographic Method and Device," the possibility of randomization erasure attacks on digital watermarks was discussed. Simply, it is always possible to erase a digital watermark, depending on how much damage you are willing to do to the watermark-bearing content stream. The present invention has the significant advantage that you must have the watermark to be able to use the code it contains. If you erase the watermark you have lost a key piece of the functionality of the application, or even the means to access the data which bear the watermark.

A preferred embodiment would be implemented in an embedded system, with a minimal operating system and

DISH-Blue Spike-842
Exhibit 1004, Page 0689

memory. No media playing "applets," or smaller sized applications as proposed in new operating environments envisioned by Sun Microsystems and the advent of Sun's Java operating system, would be permanently stored in the system, only the bare necessities to operate the device, download information, decode watermarks and execute the applets contained in them. When an applet is finished executing, it is erased from memory. Such a system would guarantee that content which did not contain readable watermarks could not be used. This is a powerful control mechanism for ensuring that content to be distributed through such a system contains valid watermarks. Thus, in such networks as the Internet or set-top box controlled cable systems, distribution and exchange of content would be made more secure from unauthorized copying to the benefit of copyright holders and other related parties. The system would be enabled to invalidate, by default, any content which has had its watermark(s) erased, since the watermark conveys, in addition to copyright information, the means to fully access, play, record or otherwise manipulate, the content.

A second method according to the present invention is to randomly re-organize program memory structure to prevent attempts at memory capture or object code analysis. The object of this method is to make it extremely difficult to perform memory capture-based analysis of an executable computer program. This analysis is the basis for a method of attack to defeat the system envisioned by the present invention.

Once the code resources of a program are loaded into memory, they typically remain in a fixed position, unless the computer operating system finds it necessary to rearrange certain portions of memory during "system time," when the operating system code, not application code, is running. Typically, this is done in low memory systems, to maintain optimal memory utilization. The

DISH-Blue Spike-842
Exhibit 1004, Page 0690

MacOS for example, uses Handles, which are double-indirect pointers to memory locations, in order to allow the operating system to rearrange memory transparently, underneath a running program. If a computer program contains countermeasures against unlicensed copying, a skilled technician can often take a snapshot of the code in memory, analyze it, determine which instructions comprise the countermeasures, and disable them in the stored application file, by means of a "patch." Other applications for designing code that moves to prevent scanning-tunnelling microscopes, and similar high sensitive hardware for analysis of electronic structure of microchips running code, have been proposed by such parties as Wave Systems. Designs of Wave Systems' microchip are intended for preventing attempts by hackers to "photograph" or otherwise determine "burn in" to microchips for attempts at reverse engineering. The present invention seeks to prevent attempts at understanding the code and its organization for the purpose of patching it. Unlike systems such as Wave Systems', the present invention seeks to move code around in such a manner as to complicate attempts by software engineers to reengineer a means to disable the methods for creating licensed copies on any device that lacks "trusted hardware." Moreover, the present invention concerns itself with any application software that may be used in general computing devices, not chipsets that are used in addition to an underlying computer to perform encryption. Wave Systems' approach to security of software, if interpreted similarly to the present invention, would dictate separate microchip sets for each piece of application software that would be tamperproof. This is not consistent with the economics of software and its distribution.

Under the present invention, the application contains a special code resource which knows about all the other code resources in memory. During execution

DISH-Blue Spike-842
Exhibit 1004, Page 0691

time, this special code resource, called a "memory scheduler," can be called periodically, or at random or pseudo random intervals, at which time it intentionally shuffles the other code resources randomly in memory, so that someone trying to analyze snapshots of memory at various intervals cannot be sure if they are looking at the same code or organization from one "break" to the next. This adds significant complexity to their job. The scheduler also randomly relocates itself when it is finished. In order to do this, the scheduler would have to first copy itself to a new location, and then specifically modify the program counter and stack frame, so that it could then jump into the new copy of the scheduler, but return to the correct calling frame. Finally, the scheduler would need to maintain a list of all memory addresses which contain the address of the scheduler, and change them to reflect its new location.

The methods described above accomplish the purposes of the invention - to make it hard to analyze captured memory containing application executable code in order to create an identifiable computer program or application that is different from other copies and is less susceptible to unauthorized use by those attempting to disable the underlying copyright protection system. Simply, each copy has particular identifying information making that copy different from all other copies.

DISH-Blue Spike-842
Exhibit 1004, Page 0692

What is Claimed Is:

1. A method of associating executable object code with a digital sample stream by means of a digital watermark wherein the digital watermark contains executable object code and is encoded into the digital sample stream.

2. The method of claim 1 wherein a key to access the digital watermark is a function of a collection of license information pertaining to the software which is accessing the watermark

where license information consists of one or more of the following items:

- Owning Organization name;
- Personal Owner name;
- Owner Address;
- License code;
- Software serialization number;
- Distribution parameters;
- Appropriate executable general computing device architecture;
- Pricing; and
- Software Metering details.

3. The method of claim 1 further comprising the step of transmitting the digital sample stream, via a transmission means, from a publisher to a subscriber

wherein transmission means can selected from the group of

- soft sector magnetic disk media;
- hard sector magnetic disk media;
- magnetic tape media;
- optical disc media;
- Digital Video Disk media;
- magneto-optical disk media;
- memory cartridge;
- telephone lines;

DISH-Blue Spike-842
Exhibit 1004, Page 0693

SCSI;
Ethernet or Token Ring Network;
ISDN;
ATM network;
TCP/IP network;
analog cellular network;
digital cellular network;
wireless network;
digital satellite;
cable network;
fiber optic network; and
electric powerline network.

4. The method of claim 1 where the object code to be encoded is comprised of series of executable machine instructions which perform the function of processing a digital sample stream for the purpose of modifying it or playing the digital sample stream.

5. The method of claim 3 further comprising the steps of:
decoding said digital watermark and extracting object code;
loading object code into computer memory for the purpose of execution;
executing said object code in order to process said digital sample stream for the purpose of playback.

6. A method of assembling an application to be protected by watermark encoding of essential resources comprising the steps of:
assembling a list of identifiers of essential code resources of an application where identifiers allow the code resource to be accessed and loaded into memory;
providing license information on the licensee who is to receive an individualized copy of the application;

DISH-Blue Spike-842
Exhibit 1004, Page 0694

storing license information in a personalization resource which is added to the list of application data resources;

generating a digital watermark key from the license information; using the key as a pseudo-random number string to select a list of suitable digital sample data resources, the list of essential code resources, and a mapping of which essential code resources are to be watermarked into which data resources;

storing the map, which is a list of paired code and data resource identifiers, as a data resource, which is added to the application;

adding a digital watermark decoder code resource to the application, to provide a means for extracting essential code resource from data resources, according to the map;

processing the map list and encoding essential code resources into digital sample data resources with a digital watermark encoder;

removing self-contained copies of the essential code resources which have been watermarked into data resources; and

combining all remaining code and data resources into a single application or installer.

7. A method of intermittently relocating application code resources in computer memory, in order to prevent, discourage, or complicate attempts at memory capture based code analysis.

8. The method of claim 7 additionally comprising the step of

assembling a list of identifiers of code resources of an application where identifiers allow the code resource to be accessed and loaded into memory.

DISH-Blue Spike-842
Exhibit 1004, Page 0695

9. The method of claim 8 additionally comprising the step of modifying application program structure to make all code resource calls indirectly, through the memory scheduler, which looks up code resources in its list and dispatches calls.

10. The method of claim 9 additionally comprising the step of intermittently rescheduling or shuffling all code resources prior to or following the dispatch of a code resource call through the memory scheduler.

11. The method of claim 10 additionally comprised of the step of the memory scheduler copying itself to a new location in memory.

12. The method of claim 11 additionally comprising the step of modifying the stack frame, program counter, and memory registers of the CPU to cause the scheduler to jump to the next instruction comprising the scheduler, in the copy, to erase the previous memory instance of the scheduler, and changing all memory references to the scheduler to reflect its new location, and to return from the copy of the scheduler to the frame which called the previous copy of the scheduler.

DISH-Blue Spike-842
Exhibit 1004, Page 0696

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00651

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/00
US CL : 380/54
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/54, 2, 4, 9, 21, 23, 25, 28, 49, 50, 59; 283/73, 113, 17

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,349,655 A (MANN) 20 September 1994, see Abstract.	1
X	US 4,262,329 A (BRIGHT et al) 14 April 1981, see Abstract.	7

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 04 APRIL 1997	Date of mailing of the international search report 29 APR 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer BERNARR EARL GREGORY Telephone No. (703) 306-4153

Form PCT/ISA/210 (second sheet)(July 1992)*

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 — A1

(11) International Publication Number: WO 97/26733

(43) International Publication Date: 24 July 1997 (24.07.97)

(21) International Application Number: PCT/US97/00652

(22) International Filing Date: 17 January 1997 (17.01.97)

(30) Priority Data:
08/587,944 17 January 1996 (17.01.96) US

(71) Applicant: THE DICE COMPANY [US/US]; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US).

(72) Inventors: COOPERMAN, Marc; 2929 Ramona, Palo Alto, CA 94306 (US). MOSKOWITZ, Scott, A.; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US).

(74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).

(81) Designated States: AL, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GE, HU, IL, IS, JP, KP, KR, LC, LK, LR, LT, LV, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD FOR AN ENCRYPTED DIGITAL WATERMARK

(57) Abstract

A method for the human-assisted generation and application of pseudo-random keys for the purpose of encoding and decoding digital watermarks to and from a digitized data stream. A pseudo-random key and key application "envelope" are generated and stored using guideline parameters input by a human engineer interacting with a graphical representation of the digitized data stream. Key "envelope" information is permanently associated with the pseudo-random binary string comprising the key. Key and "envelope" information are then applied in a digital watermark system to the encoding and decoding of digital watermarks.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic			SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

METHOD FOR AN ENCRYPTED DIGITAL WATERMARK

FIELD OF INVENTION

With the advent of computer networks and digital multimedia, protection of intellectual property has become a prime concern for creators and publishers of digitized copies of copyrightable works, such as musical recordings, movies, and video games. One method of protecting copyrights in the digital domain is to use "digital watermarks". Digital watermarks can be used to mark each individual copy of a digitized work with information identifying the title, copyright holder, and even the licensed owner of a particular copy. The watermarks can also serve to allow for secured metering and support of other distribution systems of given media content and relevant information associated with them, including addresses, protocols, billing, pricing or distribution path parameters, among the many things that could constitute a "watermark." For further discussion of systems that are oriented around content-based addresses and directories, see U.S. Patent No. 5,428,606 Moskowitz. When marked with licensing and ownership information, responsibility is created for individual copies where before there was none. More information on digital watermarks is set forth in "Steganographic Method and Device" - The DICE Company, U.S. application Serial No. 08/489,172, the disclosure of which is hereby incorporated by reference. Also, "Technology: Digital

Commerce", Denise Caruso, New York Times, August 7, 1995 "Copyrighting in the Information Age", Harley Ungar, ONLINE MARKETPLACE, September 1995, Jupiter Communications further describe digital watermarks.

Additional information on other methods for hiding information signals in content signals, is disclosed in U.S. Patent No. 5,319,735 - Preuss et al. and U.S. Patent No. 5,379,345 - Greenberg.

Digital watermarks can be encoded with random or pseudo random keys, which act as secret maps for locating the watermarks. These keys make it impossible for a party without the key to find the watermark - in addition, the encoding method can be enhanced to force a party to cause damage to a watermarked data stream when trying to erase a random-key watermark.

It is desirable to be able to specify limitations on the application of such random or pseudo random keys in encoding a watermark to minimize artifacts in the content signal while maximizing encoding level. This preserves the quality of the content, while maximizing the security of the watermark. Security is maximized because erasing a watermark without a key results in the greatest amount of perceptible artifacts in the digital content. It is also desirable to separate the functionality of the decoder side of the process to provide fuller recognition and substantiation of the protection of goods that are essentially digitized bits, while ensuring the security of the encoder and the encoded content. It is also desirable that the separate decoder be incorporated into an agent, virus, search engine, or other autonomously operating or search function software. This would make it possible for parties possessing a decoder to verify the presence of valid watermarks in a data stream, without accessing the contents of the watermark. It would also be possible to scan or search archives for files containing watermarked

DISH-Blue Spike-842
Exhibit 1004, Page 0701

content, and to verify the validity of the presence of such files in an archive, by means of the information contained in the watermarks. This scenario has particular application in screening large archives of files kept by on-line services and internet archives. It is further a goal of such processes to bring as much control of copyrights and content, including its pricing, billing, and distribution, to the parties that are responsible for creating and administering that content. It is another goal of the invention to provide a method for encoding multiple watermarks into a digital work, where each watermark can be accessed by use of a separate key. This ability can be used to provide access to watermark information to various parties with different levels of access. It is another goal of the invention to provide a mechanism which allows for accommodation of alternative methods encoding and decoding watermarks from within the same software or hardware infrastructure. This ability can be used to provide upgrades to the watermark system, without breaking support for decoding watermarks created by previous versions of the system. It is another goal of the invention to provide a mechanism for the certification and authentication, via a trusted third party, and public forums, of the information placed in a digital watermark. This provides additional corroboration of the information contained in a decoded digital watermark for the purpose of its use in prosecution of copyright infringement cases. It also has use in any situation in which a trusted third party verification is useful. It is another goal of this invention to provide an additional method for the synchronization of watermark decoding software to an embedded watermark signal that is more robust than previously disclosed methods.

DISH-Blue Spike-842
Exhibit 1004, Page 0702

SUMMARY OF THE INVENTION

The invention described herein is a human-assisted random key generation and application system for use in a digital watermark system. The invention allows an engineer or other individual, with specialized knowledge regarding processing and perception of a particular content type, such as digital audio or video, to observe a graphical representation of a subject digital recording or data stream, in conjunction with its presentation (listening or viewing) and to provide input to the key generation system that establishes a key generation "envelope", which determines how the key is used to apply a digital watermark to the digital data stream. The envelope limits the parameters of either or both the key generation system and the watermark application system, providing a rough guide within which a random or pseudo random key may be automatically generated and applied. This can provide a good fit to the content, such that the key may be used to encode a digital watermark into the content in such a manner as to minimize or limit the perceptible artifacts produced in the watermarked copy, while maximizing the signal encoding level. The invention further provides for variations in creating, retrieving, monitoring and manipulating watermarks to create better and more flexible approaches to working with copyrights in the digital domain.

Such a system is described herein and provides the user with a graphical representation of the content signal over time. In addition, it provides a way for the user to input constraints on the application of the digital watermark key, and provides a way to store this information with a random or pseudo random key sequence which is also generated to apply to a content signal. Such a system would also be more readily adaptable by current techniques to master content with personal

DISH-Blue Spike-842
Exhibit 1004, Page 0703

computers and authoring/editing software. It would also enable individuals to monitor their copyrights with decoders to authenticate individual purchases, filter possible problematic and unpaid copyrightable materials in archives, and provide for a more generally distributed approach to the monitoring and protection of copyrights in the digital domain.

DETAILED DESCRIPTION

Digital watermarks are created by encoding an information signal into a larger content signal. The information stream is integral with the content stream, creating a composite stream. The effectiveness and value of such watermarks are highest when the informational signal is difficult to remove, in the absence of the key, without causing perceptible artifacts in the content signal. The watermarked content signal itself should contain minimal or no perceptible artifacts of the information signal. To make a watermark virtually impossible to find without permissive use of the key, its encoding is dependent upon a randomly generated sequence of binary 1s and 0s, which act as the authorization key. Whoever possesses this key can access the watermark. In effect, the key is a map describing where in the content signal the information signal is hidden. This represents an improvement over existing efforts to protect copyrightable material through hardware-based solutions always existing outside the actual content.

"Antipiracy" devices are used in present applications like VCRs, cable television boxes, and digital audio tape (DAT) recorders, but are quite often disabled by those who have some knowledge of the location of the device or choose not to purchase hardware with these "additional security features." With digital watermarks, the "protection," or more accurately, the

DISH-Blue Spike-842
Exhibit 1004, Page 0704

deterrent, is hidden entirely in the signal, rather than a particular chip in the hardware.

Given a completely random key, which is uniformly applied over a content signal, resulting artifacts in the watermarked content signal are unpredictable, and depend on the interaction of the key and the content signal itself. One way to ensure minimization of artifacts is to use a low information signal level. However, this makes the watermark easier to erase, without causing audible artifacts in the content signal. This is a weakness. If the information signal level is boosted, there is the risk of generating audible artifacts.

The nature of the content signal generally varies significantly over time. During some segments, the signal may lend itself to masking artifacts that would otherwise be caused by high level encoding. At other times, any encoding is likely to cause artifacts. In addition, it might be worthwhile to encode low signal level information in a particular frequency range which corresponds to important frequency components of the content signal in a given segment of the content signal. This would make it difficult to perform bandpass filtering on the content signal to remove watermarks.

Given the benefits of such modifications to the application of the random key sequence in encoding a digital watermark, what is needed is a system which allows human-assisted key generation and application for digital watermarks. The term "human-assisted key generation" is used because in practice, the information describing how the random or pseudo random sequence key is to be applied must be stored with the key sequence. It is, in essence, part of the key itself, since the random or pseudo random sequence alone is not enough to encode, or possibly decode the watermark.

DISH-Blue Spike-842
Exhibit 1004, Page 0705

Encoding of digital watermarks into a content signal can be done in the time domain, by modifying content samples on a sample by sample basis, or in the frequency domain, by first performing a mathematical transform on a series of content samples in order to convert them into frequency domain information, subsequently modifying the frequency domain information with the watermark, and reverse transforming it back into time-based samples. The conversion between time and frequency domains can be accomplished by means of any of a class of mathematical transforms, known in general as "Fourier Transforms." There are various algorithmic implementations and optimizations in computer source code to enable computers to perform such transform calculations. The frequency domain method can be used to perform "spread spectrum" encoding implementations. Spread spectrum techniques are described in the prior art patents disclosed. Some of the shortcomings evident in these techniques relate to the fixed parameters for signal insertion in a sub audible level of the frequency-based domain, e.g., U.S. Patent No. 5,319,735 Preuss et al. A straightforward randomization attack may be engaged to remove the signal by simply over-encoding random information continuously in all sub-bands of the spread spectrum signal band, which is fixed and well defined. Since the Preuss patent relies on masking effects to render the watermark signal, which is encoded at -15 dB relative to the carrier signal, inaudible, such a randomization attack will not result in audible artifacts in the carrier signal, or degradation of the content. More worrisome, the signal is not the original but a composite of an actual frequency in a known domain combined with another signal to create a "facsimile" or approximation, said to be imperceptible to a human observer, of the original copy. What results is the forced maintenance of one

original to compare against subsequent "suspect" copies for examination. Human-assisted watermarking would provide an improvement over the art by providing flexibility as to where information signals would be inserted into content while giving the content creator the ability to check all subsequent copies without the requirement of a single original or master copy for comparison. Thus the present invention provides for a system where all necessary information is contained within the watermark itself.

Among other improvements over the art, generation of keys and encoding with human assistance would allow for a better match of a given informational signal (be it an ISRC code, an audio or voice file, serial number, or other "file" format) to the underlying content given differences in the make-up of the multitudes of forms of content (classical music, CD-ROM versions of the popular game DOOM, personal HTML Web pages, virtual reality simulations, etc.) and the ultimate wishes of the content creator or his agents. This translates into a better ability to maximize the watermark signal level, so as to force maximal damage to the content signal when there is an attempt to erase a watermark without the key. For instance, an engineer could select only the sections of a digital audio recording where there were high levels of distortion present in the original recording, while omitting those sections with relatively "pure" components from the watermark process. This then allows the engineer to encode the watermark at a relatively higher signal level in the selected sections without causing audible artifacts in the signal, since the changes to the signal caused by the watermark encoding will be masked by the distortion. A party wanting to erase the watermark has no idea, however, where or at what level a watermark is encoded, and so must choose to "erase" at the maximum level across the

DISH-Blue Spike-842
Exhibit 1004, Page 0707

entire data stream, to be sure they have obliterated every instance of a watermark.

In the present invention, the input provided by the engineer is directly and immediately reflected in a graphical representation of content of that input, in a manner such that it is overlaid on a representation of the recorded signal. The key generation "envelope" described by the engineer can be dictated to vary dynamically over time, as the engineer chooses. The graphical representation of the content is typically rendered on a two dimensional computer screen, with a segment of the signal over time proceeding horizontally across the screen. The vertical axis is used to distinguish various frequency bands in the signal, while the cells described by the intersection of vertical and horizontal unit lines can signify relative amplitude values by either a brightness or a color value on the display.

Another possible configuration and operation of the system would use a display mapping time on the horizontal axis versus signal amplitude on the vertical axis. This is particularly useful for digital audio signals. In this case, an engineer could indicate certain time segments, perhaps those containing a highly distorted signal, to be used for watermark encoding, while other segments, which contain relatively pure signals, concentrated in a few bandwidths, may be exempt from watermarking. The engineer using a time vs. amplitude assisted key generation configuration would generally not input frequency limiting information.

In practice, the system might be used by an engineer or other user as follows:

The engineer loads a file containing the digitized content stream to be watermarked onto a computer. The engineer runs the key generation application and opens the file to be watermarked. The application opens a

DISH-Blue Spike-842
Exhibit 1004, Page 0708

window which contains a graphical representation of the digitized samples. Typically, for digital audio, the engineer would see a rectangular area with time on the horizontal axis, frequency bands on the vertical axis, and varying color or brightness signifying signal power at a particular time and frequency band. Each vertical slice of the rectangle represents the frequency components, and their respective amplitude, at a particular instant ("small increment") of time. Typically, the display also provides means for scrolling from one end of the stream to the other if it is too long to fit on the screen, and for zooming in or out magnification in time or frequency. For the engineer, this rectangular area acts as a canvas. Using a mouse and/or keyboard, the engineer can scroll through the signal slowly marking out time segments or frequency band minima and maxima which dictate where, at what frequencies, and at what encoding signal level a watermark signal is to be encoded into the content, given a random or pseudo random key sequence. The engineer may limit these marks to all, none or any of the types of information discussed above. When the engineer is finished annotating the content signal, he or she selects a key generation function. At this point, all the annotated information is saved in a record and a random or pseudo random key sequence is generated associated with other information. At some later point, this combined key record can be used to encode and/or decode a watermark into this signal, or additional instances of it.

A suitable pseudo-random binary sequence for use as a key may be generated by: collecting some random timing information based on user keystrokes input to a keyboard device attached to the computer, performing a secure one way hash operation on this random timing data, using the results of the hash to seed a block cipher algorithm

DISH-Blue Spike-842
Exhibit 1004, Page 0709

loop, and then cycling the block cipher and collecting a sequence of 1s and 0s from the cipher's output, until a pseudo-random sequence of 1s and 0s of desired length is obtained.

The key and its application information can then be saved together in a single database record within a database established for the purpose of archiving such information, and sorting and accessing it by particular criteria. This database should be encrypted with a passphrase to prevent the theft of its contents from the storage medium.

Another improvement in the invention is support for alternate encoding algorithm support. This can be accomplished for any function which relates to the encoding of the digital watermark by associating with the pseudo-random string of 1s and 0s comprising the pseudo-random key, a list of references to the appropriate functions for accomplishing the encoding. For a given function, these references can indicate a particular version of the function to use, or an entirely new one. The references can take the form of integer indexes which reference chunks of computer code, of alphanumeric strings which name such "code resources," or the memory address of the entry point of a piece of code already resident in computer memory. Such references are not, however, limited to the above examples. In the implementation of software, based on this and previous filings, each key contains associated references to functions identified as CODEC - basic encode/decode algorithm which encodes and decodes bits of information directly to and from the content signal, MAP - a function which relates the bits of the key to the content stream, FILTER - a function which describes how to pre-filter the content signal, prior to encoding or decoding, CIPHER - a function which provides encryption and decryption services for information

DISH-Blue Spike-842
Exhibit 1004, Page 0710

contained in the watermark, and ERRCODE - a function which further encodes/decodes watermark information so that errors introduced into a watermark may be corrected after extraction from the content signal.

Additionally, a new method of synchronizing decoder software to an embedded watermark is described. In a previous disclosure, a method whereby a marker sequence of N random bits was generated, and used to signal the start of an encoded watermark was described. When the decoder recognizes the N bit sequence, it knows it is synchronized. In that system the chance of a false positive synchronization was estimated at 1/(N^2) ("one over (N to the power of 2)"). While that method is fairly reliable, it depends on the marker being encoded as part of the steganographic process, into the content stream. While errors in the encoded bits may be partially offset by error coding techniques, error coding the marker will require more computation and complexity in the system. It also does not completely eliminate the possibility that a randomization attack can succeed in destroying the marker. A new method is implemented in which the encoder pre-processes the digital sample stream, calculating where watermark information will be encoded. As it is doing this, it notes the starting position of each complete watermark, and records to a file, a sequence of N-bits representing sample information corresponding to the start of the watermark, for instance, the 3rd most significant bit of the 256 samples immediately preceding the start of a watermark. This would be a 256 bit marker. The order in which these markers are encountered is preserved, as it is important. The decoder then searches for matches to these markers. It processes the markers from first to last, discarding each as it is found, or possibly not found within a certain scanning distance, and proceeding with the remaining markers. This method does not modify

DISH-Blue Spike-842
Exhibit 1004, Page 0711

the original signal with marker information and has the added benefit that high-significance sequences can be used, requiring that an attack based on randomizing markers do very obvious damage to the content stream.

With multichannel encoding, both private and public keys, similar in use to those from public-key cryptosystems, could be provided for authentication by concerned third party vendors and consumers, as well as contribute to better management and protection of copyrights for the digital world that already exist in the physical world. For more information on public-key cryptosystems see US Pat No 4,200,770 Diffie-Hellman, 4,218,582 Hellman, 4,405,829 RSA, 4,424,414 Hellman Pohlig. In addition, any number of key "designations" between "public" and "private" could be established, to provide various access privileges to different groups. Multi-channel watermarks are effected by encoding separate watermark certificates with separate keys by either interleaving windows in the time domain or by using separate frequency bands in the frequency domain. For instance, 3 separate watermarks could be encoded by using every third sample window processed to encode a corresponding certificate. Alternatively, complete watermarks could be interleaved. Similarly, the frequency range of an audio recording might be partitioned into 3 sub-ranges for such a purpose. Use of multi-channel watermarks would allow groups with varying access privileges to access watermark information in a given content signal. The methods of multichannel encoding would further provide for more holographic and inexpensive maintenance of copyrights by parties that have differing levels of access priority as decided by the ultimate owner or publisher of the underlying content. Some watermarks could even play significant roles in adhering to given filtering (for example, content that is not intended for all

DISH-Blue Spike-842
Exhibit 1004, Page 0712

observers), distribution, and even pricing schemes for given pieces of content. Further, on-the-fly watermarking could enhance identification of pieces of content that are traded between a number of parties or in a number of levels of distribution. Previously discussed patents by Preuss et al. and Greenberg and other similar systems lack this feature.

Further improvements over the prior art include the general capacity and robustness of the given piece of information that can be inserted into media content with digital watermarks, described in **Steganographic Method and Device** and further modified here, versus "spread spectrum-only" methods. First, the spread spectrum technique described in US. Patent No. 5,319,735 Preuss et al. is limited to an encoding rate of 4.3 8-bit symbols per second within a digital audio signal. This is because of the nature of reliability requirements for spread spectrum systems. The methods described in this invention and those of the previous application, "Steganographic Method and Device," do not particularly adhere to the use of such spread spectrum techniques, thus removing such limitation. In the steganographic derived implementation the inventors have developed based on these filings, watermarks of approximately 1,000 bytes (or 1000x 8 bits) were encoded at a rate of more than 2 complete watermarks per second into the carrier signal. The carrier signal was a two channel (stereo) 16-bit, 44.1 Khz recording. The cited encoding rate is per channel. This has been successfully tested in a number of audio signals. While this capacity is likely to decrease by 50% or more as a result of future improvements to the security of the system, it should still far exceed the 4.3 symbols per second envisioned by Preuss et al. Second, the ability exists to recover the watermarked information with a sample of the overall piece of digitized content (that is, for instance, being

DISH-Blue Spike-842
Exhibit 1004, Page 0713

able to recover a watermark from just 10 seconds of a 3 minute song, depending on the robustness or size of the data in a given watermark) instead of a full original. Third, the encoding process described in **Steganographic Method and Device** and further modified in this invention explicitly seeks to encode the information signal in such a way with the underlying content signal as to make destruction of the watermark cause destruction of the underlying signal. The prior art describes methods that confuse the outright destruction of the underlying content with "the level of difficulty" of removing or altering information signals that *may* destroy underlying content. This invention anticipates efforts that can be undertaken with software, such as Digidesign's Sound Designer II or Passport Design's Alchemy, which gives audio engineers (similar authoring software for video also exists, for instance, that sold by Avid Technology, and others as well as the large library of picture authoring tools) very precise control of digital signals, "embedded" or otherwise, that can be purely manipulated in the frequency domain. Such software provides for bandpass filtering and noise elimination options that may be directed at specific ranges of the frequency domain, a ripe method for attack in order to hamper recovery of watermark information encoded in specific frequency ranges.

Separating the decoder from the encoder can limit the ability to reverse the encoding process while providing a reliable method for third parties to be able to make attempts to screen their archives for watermarked content without being able to tamper with all of the actual watermarks. This can be further facilitated by placing separate signals in the content using the encoder, which signal the presence of a valid watermark, e.g. by providing a "public key accessible" watermark channel which contains information comprised

DISH-Blue Spike-842
Exhibit 1004, Page 0714

of a digitally signed digital notary registration of the watermark in the private channel, along with a checksum verifying the content stream. The checksum reflects the unique nature of the actual samples which contain the watermark in question, and therefore would provide a means to detect an attempt to graft a watermark lifted from one recording and placed into another recording in an attempt to deceive decoding software of the nature of the recording in question. During encoding, the encoder can leave room within the watermark for the checksum, and analyze the portion of the content stream which will contain the watermark in order to generate the checksum before the watermark is encoded. Once the checksum is computed, the complete watermark certificate, which now contains the checksum, is signed and/or encrypted, which prevents modification of any portion of the certificate, including the checksum, and finally encoded into the stream. Thus, if it is somehow moved at a later time, that fact can be detected by decoders. Once the decoder functions are separate from the encoder, watermark decoding functionality could be embedded in several types of software including search agents, viruses, and automated archive scanners. Such software could then be used to screen files or search out files from archive which contain specific watermark information, types of watermarks, or lack watermarks. For instance, an online service could, as policy, refuse to archive any digital audio file which does not contain a valid watermark notarized by a trusted digital notary. It could then run automated software to continuously scan its archive for digital audio files which lack such watermarks, and erase them.

Watermarks can be generated to contain information to be used in effecting software or content metering services. In order to accomplish this, the watermark

DISH-Blue Spike-842
Exhibit 1004, Page 0715

would include various fields selected from the following information:

title identification;

unit measure;

unit price;

percentage transfer threshold at which liability is incurred to purchaser;

percent of content transferred;

authorized purchaser identification;

seller account identification;

payment means identification;

digitally signed information from sender indicating percent of content transferred; and

digitally signed information from receiver indicating percent of content received.

These "metering" watermarks could be dependent on a near continuous exchange of information between the transmitter and receiver of the metered information in question. The idea is that both sides must agree to what the watermark says, by digitally signing it. The sender agrees they have sent a certain amount of a certain title, for instance, and the receiver agrees they have received it, possibly incurring a liability to pay for the information once a certain threshold is passed. If the parties disagree, the transaction can be discontinued before such time. In addition, metering watermarks could contain account information or other payment information which would facilitate the transaction.

Watermarks can also be made to contain information pertaining to geographical or electronic distribution restrictions, or which contain information on where to locate other copies of this content, or similar content. For instance, a watermark might stipulate that a recording is for sale only in the United States, or that it is to be sold only to persons connecting to an online

DISH-Blue Spike-842
Exhibit 1004, Page 0716

distribution site from a certain set of internet domain names, like ".us" for United States, or ".ny" for New York. Further a watermark might contain one or more URLs describing online sites where similar content that the buyer of a piece of content might be interested in can be found.

A digital notary could also be used in a more general way to register, time stamp and authenticate the information inside a watermark, which is referred to as the certificate. A digital notary processes a document which contains information and assigns to it a unique identification number which is a mathematical function of the contents of the document. The notary also generally includes a time stamp in the document along with the notary's own digital signature to verify the date and time it received and "notarized" the document. After being so notarized, the document cannot be altered in any way without voiding its mathematically computed signature. To further enhance trust in such a system, the notary may publish in a public forum, such as a newspaper, which bears a verifiable date, the notarization signatures of all documents notarized on a given date. This process would significantly enhance the trust placed in a digital watermark extracted for the purpose of use in settling legal disputes over copyright ownership and infringement.

Other "spread spectrum" techniques described in the art have predefined time stamps to serve the purpose of verifying the actual time a particular piece of content is being played by a broadcaster, e.g., U.S. Patent No. 5,379,345 Greenberg, not the insertion and control of a copyright or similar information (such as distribution path, billing, metering) by the owner or publisher of the content. The Greenberg patent focuses almost exclusively on concerns of broadcasters, not content creators who deal with digitized media content when

DISH-Blue Spike-842
Exhibit 1004, Page 0717

distributing their copyrightable materials to unknown parties. The methods described are specific to spread spectrum insertion of signals as "segment timing marks" to make comparisons against a specific master of the underlying broadcast material-- again with the intention of specifying if the broadcast was made according to agreed terms with the advertisers. No provisions are made for stamping given audio signals or other digital signals with "purchaser" or publisher information to stamp the individual piece of content in a manner similar to the sales of physical media products (CDs, CD-ROMs, etc.) or other products in general (pizza delivery, direct mail purchases, etc.). In other words, "interval-defining signals," as described in the Greenberg patent, are important for verification of broadcasts of a time-based commodity like time and date-specific, reserved broadcast time, but have little use for individuals trying to specify distribution paths, pricing, or protect copyrights relating to given content which may be used repeatedly by consumers for many years. It would also lack any provisions for the "serialization" and identification of individual copies of media content as it can be distributed or exchanged on the Internet or in other on-line systems (via telephones, cables, or any other electronic transmission media). Finally, the Greenberg patent ties itself specifically to broadcast infrastructure, with the described encoding occurring just before transmission of the content signal via analog or digital broadcast, and decoding occurring upon reception.

While the discussion above has described the invention and its use within specific embodiments, it should be clear to those skilled in the art that numerous modifications may be made to the above without departing from the spirit of the invention, and that the

scope of the above invention is to be limited only by the claims appended hereto.

DISH-Blue Spike-842
Exhibit 1004, Page 0719

What is Claimed:

1. A method for using a computer to generate a random or pseudo random key for a digital watermark system wherein said random key includes:

a random or pseudo random sequence of binary 1s and 0s

information describing the application of the random sequence to a stream of digitized samples wherein said information includes:

at least one list of time delimiters describing segments of the stream;

at least one list of frequency delimiters describing frequency bands to be included in watermark computations; and

a signal encoding level;

wherein the method comprises the step of receiving human interactive input information used to describe limits on where, at what level, and at what frequencies the random binary information of the random key is to be applied to the stream of digitized samples in encoding the digital watermark;

wherein said human interactive input information comprises at least one of the following datum:

a list of time delimiters;

a list of frequency delimiters; and

a signal encoding level.

2. The method of claim 1 further comprising the step of selecting said stream of digitized samples from a list provided by a computer system.

3. The method of claim 2 further comprising the step of creating and displaying a graphical representation on the display device of the computer

DISH-Blue Spike-842
Exhibit 1004, Page 0720

system, wherein said graphical representation includes a time axis and a signal frequency axis.

4. The method of claim 2 further comprising the step of creating and displaying a graphical representation on the display device of the computer system, wherein said graphical representation includes a time axis and a signal amplitude axis.

5. The method of claim 3 or 4, further comprising the step of updating the graphical display to reflect receipt of new human interactive input information.

6. The method of claim 5 further comprising the step of generating a random or pseudo random sequence of 1s and 0s.

7. The method of claim 6 further comprising the step of storing input information in association with the random sequence of 1s and 0s as a single record in a database of such records.

8. The method of claim 7 wherein the record is encrypted using a pass phrase.

9. The method of claim 1 where the stream of digitized samples contains a digital audio recording.

10. The method of claim 1 where the stream of digitized samples to be watermarked contains a digital video recording.

11. The method of claim 6 wherein the process of generating the random sequence comprises the steps of:

DISH-Blue Spike-842
Exhibit 1004, Page 0721

(a) collecting a series of random bits derived from keyboard latency intervals in random typing;

(b) processing the initial series of random bits through a secure one-way hash function;

(c) using the results of one-way hash function to seed a block encryption cipher loop;

(d) cycling through the block encryption loop, and extracting the least significant bit of each result after cycle; and

(e) concatenating the block encryption output bits into the random key sequence

12. A method of encoding and decoding a digital watermark where the encoder and decoder are separate software applications or hardware devices.

13. The method of claim 12 wherein the decoder functionality is embedded in a software search engine, word-wide web-crawler file scanning engine, intelligent agent, or a virus.

14. The method of claim 12 wherein the decoder can access only a limited number of watermark channels, corresponding to public watermark keys, or any keys otherwise made available to said decoder.

15. The method of claim 12 wherein the decoder is capable of detecting the presence of a valid watermark but not of accessing the information in the watermark.

16. The method of claim 12 wherein the encoder places a separate signal, which does not interfere with the watermark, into a content stream, where said separate signal can indicate

DISH-Blue Spike-842
Exhibit 1004, Page 0722

watermark synchronization information, which helps locate watermarks in the content; and

the presence of a valid watermark in the content.

17. A method of using digital watermarks to convey information which is to be used for a content metering service, wherein said watermarks contain at least one of the following pieces of information:

title identification;

unit measure;

unit price;

percentage transfer threshold at which liability is incurred to purchaser;

percent of content transferred;

authorized purchaser identification;

seller account identification;

payment means identification;

digitally signed information from sender indicating percent of content transferred; and

digitally signed information from receiver indicating percent of content received.

18. A method of encoding digital watermarks which contain information pertaining to distribution restrictions and a location of an addressable directory containing related content, where said watermarks contain at least one of the following pieces of information:

geographical constraints on distribution (state, country, etc);

logical constraints on distribution;

Universal Resource Locator (URL);

telephone number;

Internet Protocol address;

Internet domain name;

email address; and

DISH-Blue Spike-842
Exhibit 1004, Page 0723

file name.

19. A method of encoding multiple digital watermarks into a single content stream wherein each watermark is encoded with a separate key.

20. The method of claim 18 wherein watermark information from each watermark is interleaved in the time domain.

21. A method of claim 18 wherein watermark information from each watermark is placed into specific frequency bands, or interleaved in the frequency domain.

22. A method of associating with a pseudo-random key, a list of component function references, which dictate what component functions are applied to the encoding and decoding of a digital watermark using the key in question.

23. A method of providing synchronization of a decoder to watermark which consists of the following steps:

a) recording a feature of sample stream, or a marker extracted from the sample stream immediately preceding the start of an encoded watermark;

b) recording the order in which a list of markers was encountered in the sample stream;

c) storing a list of such markers and the order of their appearance in a file for use by the decoder;

d) optionally, associating the stored information of step c) with a watermark key or watermark receipt or content title;

e) in the decoder, selecting a marker from the file in step c) such that the selected marker is not previous

DISH-Blue Spike-842
Exhibit 1004, Page 0724

in order to any other marker previously selected in decoding the sample stream in question;

f) attempting to find a feature or marker in the portion of the sample stream currently under processing;

g) at such time as the currently selected marker is deemed unlikely to be found, discarding it and proceeding to step e);

h) at such time as marker is found, decoding the watermark, then proceeding to step e) unless the sample stream is exhausted.

DISH-Blue Spike-842
Exhibit 1004, Page 0725

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00652

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/00
US CL :380/20
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/20, 54

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US, A, 5,530,759 (BRAUDAWAY ET AL) 25 June 1996, see Figs. 1-2.	1-11, 22

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
06 MAY 1997	09 JUN 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer SALVATORE CANGIALOSI
Facsimile No. (703) 305-3230	Telephone No. (703) 305-1837

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00652

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-11 and 22

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

DISH-Blue Spike-842
Exhibit 1004, Page 0727

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00652

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

Group I, Claims 1-11, 22, drawn to an method of generating an encrypted digital watermark.

Group II, Claims 12-21 and 23 method of making and using a digital watermark.

The inventions listed as Groups I-II do not relate to a single inventive concept under PCT Rule 13.1 because under PCT Rule 13.2, they lack the same or corresponding technical features for the following Reasons: The invention of Group I lack the separate software, hardware devices or content monitoring. The invention of Group II lack the pseudo-Random key.

DISH-Blue Spike-842
Exhibit 1004, Page 0728

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G09C 5/00, H04L 9/00	A1	**(11) International Publication Number:** WO 98/02864 **(43) International Publication Date:** 22 January 1998 (22.01.98)

(21) International Application Number: PCT/US97/11455

(22) International Filing Date: 2 July 1997 (02.07.97)

(30) Priority Data:
08/677,435 2 July 1996 (02.07.96) US

(71) Applicant: THE DICE COMPANY [US/US]; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US).

(72) Inventors: MOSKOWITZ, Scott, A.; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US). COOPERMAN, Marc, S.; 2929 Ramona, Palo Alto, CA 94306 (US).

(74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).

(81) Designated States: AU, BR, CN, JP, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: OPTIMIZATION METHODS FOR THE INSERTION, PROTECTION AND DETECTION OF DIGITAL WATERMARKS IN DIGITIZED DATA

(57) Abstract

The implementations of digital watermarks can be optimally suited to particular transmission, distribution and storage mediums given the nature of digitally-sampled audio, video and other multimedia works. Watermark application parameters can be adapted to the individual characteristics of a given digital sample stream. Watermark information can be either carried in individual samples or in relationships between multiple samples, such as in a waveform shape. More optimal models may be obtained to design watermark systems that are tamper-resistant given the number and breadth of existent digitized sample options with different frequency and time components. The highest quality of a given content signal may be maintained as it is mastered, with the watermark suitably hidden, taking into account usage of digital filters and error correction. The quality of the underlying content signals can be used to identify and highlight advantageous locations for the insertion of digital watermarks. The watermark is integrated as closely as possible to the content signal, at a maximum level to force degradation of the content signal when attempts are made to remove the watermarks.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

OPTIMIZATION METHODS FOR THE INSERTION, PROTECTION AND DETECTION OF DIGITAL WATERMARKS IN DIGITIZED DATA

RELATED APPLICATIONS

This application is related to patent applications entitled "Steganographic Method and Device", Serial No. 08/489,172 filed on June 7, 1995; "Method for Human-Assisted Random Key Generation and Application for Digital Watermark System", Serial No. 08/587,944 filed on January 17, 1996; "Method for Stega-Cipher Protection of Computer Code", Serial No. 08/587,943 filed on January 17, 1996; "Digital Information Commodities Exchange", Serial No. 08/365,454 filed on December 28, 1994, which is a continuation of Serial No. 08/083,593 filed on June 30, 1993; and "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management", Serial No. 08/674,726 filed on July 2, 1996. These related applications are all incorporated herein by reference.

This application is also related to U.S. Patent No. 5,428,606, "Digital Information Commodities Exchange", issued on June 27, 1995, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

The present invention relates to digital watermarks.

Digital watermarks exist at a convergence point where creators and publishers of digitized multimedia content demand localized, secured

identification and authentication of that content. Because existence of piracy is clearly a disincentive to the digital distribution of copyrighted works, establishment of responsibility for copies and derivative copies of such works is invaluable. In considering the various forms of multimedia content, whether "master," stereo, NTSC video, audio tape or compact disc, tolerance of quality degradation will vary with individuals and affect the underlying commercial and aesthetic value of the content. It is desirable to tie copyrights, ownership rights, purchaser information or some combination of these and related data to the content in such a manner that the content must undergo damage, and therefore a reduction in value, with subsequent, unauthorized distribution of the content, whether it be commercial or otherwise.

Legal recognition and attitude shifts, which recognize the importance of digital watermarks as a necessary component of commercially distributed content (audio, video, game, etc.), will further the development of acceptable parameters for the exchange of such content by the various parties engaged in the commercial distribution of digital content. These parties may include artists, engineers, studios, INTERNET access providers, publishers, agents, on-line service providers, aggregators of content for various forms of delivery, on-line retailers, individuals and parties that participate in the transfer of funds to arbitrate the actual delivery of content to intended parties.

Since the characteristics of digital recordings vary widely, it is a worthwhile goal to provide tools to describe an optimized envelope of parameters for inserting, protecting and detecting digital watermarks in a given digitized sample (audio, video, virtual reality, etc.) stream. The optimization techniques described hereinafter make unauthorized removal of digital watermarks containing these parameters a significantly costly operation in terms of the absolute given projected economic gain from undetected commercial distribution. The optimization techniques, at the least, require significant damage to the content signal, as to make the

DISH-Blue Spike-842
Exhibit 1004, Page 0732

unauthorized copy commercially worthless, if the digital watermark is removed, absent the use of extremely expensive tools.

Presumably, the commercial value of some works will dictate some level of piracy not detectable in practice and deemed "reasonable" by rights holders given the overall economic return. For example, there will always be fake $100 bills, LEVI jeans, and GUCCI bags, given the sizes of the overall markets and potential economic returns for pirates in these markets--as there also will be unauthorized copies of works of music, operating systems (Windows95, etc.), video and future multimedia goods.

However, what differentiates the "digital marketplace" from the physical marketplace is the absence of any scheme that establishes responsibility and trust in the authenticity of goods. For physical products, corporations and governments mark the goods and monitor manufacturing capacity and sales to estimate loss from piracy. There also exist reinforcing mechanisms, including legal, electronic, and informational campaigns to better educate consumers.

SUMMARY OF THE INVENTION

The present invention relates to implementations of digital watermarks that are optimally suited to particular transmission, distribution and storage mediums given the nature of digitally-sampled audio, video, and other multimedia works.

The present invention also relates to adapting watermark application parameters to the individual characteristics of a given digital sample stream.

The present invention additionally relates to the implementation of digital watermarks that are feature-based. That is, a system where watermark information is not carried in individual samples, but is carried in the relationships between multiple samples, such as in a waveform shape. The present invention envisions natural extensions for digital watermarks that may also separate frequencies (color or audio), channels in 3D while utilizing discreteness in feature-based encoding only known to those with

pseudo-random keys (i.e., cryptographic keys) or possibly tools to access such information, which may one day exist on a quantum level.

The present invention additionally relates to a method for obtaining more optimal models to design watermark systems that are tamper-resistant given the number and breadth of existent digitized-sample options with differing frequency and time components (audio, video, pictures, multimedia, virtual reality, etc.).

To accomplish these goals, the present invention maintains the highest quality of a given content signal as it was mastered, with its watermarks suitably hidden, taking into account usage of digital filters and error correction presently concerned solely with the quality of content signals.

The present invention additionally preserves quality of underlying content signals, while using methods for quantifying this quality to identify and highlight advantageous locations for the insertion of digital watermarks.

The present invention integrates the watermark, an information signal, as closely as possible to the content signal, at a maximal level, to force degradation of the content signal when attempts are made to remove the watermarks.

The present invention relates to a method for amplitude independent encoding of digital watermark information in a signal including steps of determining in the signal a sample window having a minimum and a maximum, determining a quantization interval of the sample window, normalizing the sample window, normalizing the sample window to provide normalized samples, analyzing the normalized samples, comparing the normalized samples to message bits, adjusting the quantization level of the sample window to correspond to the message bit when a bit conflicts with the quantization level and de-normalizing the analyzed samples.

The present invention also relates to a method for amplitude independent decoding of digital watermark information in a signal including steps of determining in the signal a sample window having a minimum and a

DISH-Blue Spike-842
Exhibit 1004, Page 0734

maximum, determining a quantization interval of the sample window, normalizing the sample window to provide samples, and analyzing the quantization level of the samples to determine a message bit value.

The present invention additionally relates to a method of encoding and decoding watermarks in a signal where, rather than individual samples, insertion and detection of abstract signal features to carry watermark information in the signal is done.

The present invention also relates to a method for pre-analyzing a digital signal for encoding digital watermarks using an optimal digital filter in which it is determined what noise elements in the digital signal will be removed by the optimal digital filter based on response characteristics of the filter.

The present invention also relates to a method of error coding watermark message certificates using cross-interleaved codes which use error codes of high redundancy, including codes with Hamming distances of greater than or equal to "n", wherein "n" is a number of bits in a message block.

The present invention additionally relates to a method of pre-processing a watermark message certificate including a step of determining an absolute bit length of the watermark message as it will be encoded.

The present invention additionally relates to a method of generating watermark pseudo-random key bits using a non-linear (chaotic) generator or to a method of mapping pseudo-random key and processing state information to affect an encode/decode map using a non-linear (chaotic) generator.

The present invention additionally relates to a method of guaranteeing watermark certificate uniqueness including a step of attaching a time stamp or user identification dependent hash or message digest of watermark certificate data to the certificate.

The present invention also relates to a method of generating and quantizing a local noise signal to contain watermark information where the

noise signal is a function of at least one variable which depends on key and processing state information.

The present invention also relates to a method of dithering watermark quantizations such that the dither changes an absolute quantization value, but does not change a quantization level or information carried in the quantization.

The present invention further relates to a method of encoding watermarks including inverting at least one watermark bit stream and encoding a watermark including the inverted watermark bit stream.

The present invention also relates to a method of decoding watermarks by considering an original watermark synchronization marker, an inverted watermark synchronization marker, and inverted watermarks, and decoding based on those considerations.

The present invention also relates to a method of encoding and decoding watermarks in a signal using a spread spectrum technique to encode or decode where information is encoded or decoded at audible levels and randomized over both frequency and time.

The present invention additionally relates to a method of analyzing composite digitized signals for watermarks including obtaining a composite signal, obtaining an unwatermarked sample signal, time aligning the unwatermarked sample signal to the composite signal, gain adjusting the time aligned unwatermarked sample signal to the composite signal, estimating a pre-composite signal using the composite signal and the gain adjusted unwatermarked sample signal, estimating a watermarked sample signal by subtracting the estimated pre-composite signal for the composite signal, and scanning the estimated watermark sample signal for watermarks.

The present invention additionally relates to a method for varying watermark encode/decode algorithms automatically during the encoding or decoding of a watermark including steps of (a) assigning a list of desired CODECs to a list of corresponding signal characteristics which indicate use

of particular CODECs, (b) during encoding/decoding, analyzing characteristics of the current sample frame in the signal stream, prior to delivering the frame to CODEC, (c) looking up the corresponding CODEC from the list of CODECs in step (a) which matches the observed signal characteristics from step (b), (d) loading and/or preparing the desired CODEC, (e) passing the sample frame to the CODEC selected in step (c), and f) receiving the output samples from step (e).

The present invention also relates to a method for varying watermark encode/decode algorithms automatically during the encoding or decoding of a watermark, including steps of (a) assigning a list of desired CODECs to a list of index values which correspond to values computed to values computed as a function of the pseudo-random watermark key and the state of the processing framework, (b) during encoding/decoding, computing the pseudo-random key index value for the current sample frame in the signal stream, prior to delivering the frame to a CODEC, (c) looking up the corresponding CODEC from the list of CODECs in step (a) which matches the index value from step (b), (d) loading and/or preparing the desired CODEC, (e) passing the sample frame to the CODEC selected in step (c), and (f) receiving the output samples from step (e).

DETAILED DESCRIPTION

The present invention relates to implementations of digital watermarks that are optimally suited to particular transmission, distribution and storage mediums given the nature of digitally sampled audio, video, and other multimedia works.

The present invention also relates to adapting watermark application parameters to the individual characteristics of a given digital sample stream.

The present invention additionally relates to the implementation of digital watermarks that are feature-based. That is, a system where watermark information is not carried in individual samples, but is carried in the relationships between multiple samples, such as in a waveform shape.

DISH-Blue Spike-842
Exhibit 1004, Page 0737

For example, in the same manner a US $100 bill has copy protection features including ink type, paper stock, fiber, angles of artwork that distort in photocopier machines, inserted magnetic strips, and composite art, the present invention envisions natural extensions for digital watermarks that may also separate frequencies (color or audio), channels in 3D while utilizing discreteness in feature-based encoding only known to those with pseudo-random keys (i.e., cryptographic keys) or possibly tools to access such information, which may one day exist on a quantum level.

There are a number of hardware and software approaches in the prior art that attempt to provide protection of multimedia content, including encryption, cryptographic containers, cryptographic envelopes or "cryptolopes", and trusted systems in general. None of these systems places control of copy protection in the hands of the content creator as the content is created, nor provides an economically feasible model for exchanging the content to be exchanged with identification data embedded within the content.

Yet, given the existence of over 100 million personal computers and many more non-copy-protected consumer electronic goods, copy protection seems to belong within the signals. After all, the playing (i.e., using) of the content establishes its commercial value.

Generally, encryption and cryptographic containers serve copyright holders as a means to protect data in transit between a publisher or distributor and the purchaser of the data (i.e., a means of securing the delivery of copyrighted material from one location to another by using variations of public key cryptography or other more centralized cryptosystems).

Cryptolopes are suited specifically for copyrighted text that is time-sensitive, such as newspapers, where intellectual property rights and origin data are made a permanent part of the file. For information on public-key cryptosystems see U.S. Patent No. 4,200,770 to Hellman et al., U.S. Patent No. 4,218,582 to Hellman et al., U.S. Patent No. 4,405,829 to Rivest et al.,

DISH-Blue Spike-842
Exhibit 1004, Page 0738

and U.S. Patent No. 4,424,414 to Hellman et al. Systems are proposed by IBM and Electronic Publishing Resources to accomplish cryptographic container security.

Digitally-sampled copyrighted material, that is binary data on a fundamental level, is a special case because of its long term value coupled with the ease and perfectness of copying and transmission by general purpose computing and telecommunications devices. In particular, in digitally-sampled material, there is no loss of quality in copies and no identifiable differences between one copy and any other subsequent copy. For creators of content, distribution costs may be minimized with electronic transmission of copyrighted works. Unfortunately, seeking some form of informational or commercial return via electronic exchange is ill-advised absent the use of digital watermarks to establish responsibility for specific copies and unauthorized copying. Absent digital watermarks, the unlikely instance of a market of trusted parties who report any distribution or exchange of unauthorized copies of the protected work must be relied upon for enforcement. Simply, content creators still cannot independently verify watermarks should they choose to do so.

For a discussion of systems that are oriented around content-based addresses and directories, see U.S. Patent No. 5,428,606 to Moskowitz.

In combining steganographic methods for insertion of information identifying the title, copyright holder, pricing, distribution path, licensed owner of a particular copy, or a myriad of other related information, with pseudo-random keys (which map insertion location of the information) similar to those used in cryptographic applications, randomly placed signals (digital watermarks) can be encoded as random noise in a content signal. Optimal planning of digital watermark insertion can be based on the inversion of optimal digital filters to establish or map areas comprising a given content signal insertion envelope. Taken further, planning operations will vary for different digitized content: audio, video, multimedia, virtual reality, etc. Optimization techniques for processes are described in the

DISH-Blue Spike-842
Exhibit 1004, Page 0739

copending related applications entitled "Steganographic Method and Device" and "Method for Human Assisted Random Key Generation and Application for Digital Watermark System".

Optimization processes must take into consideration the general art of digitization systems where sampling and quantizing are fundamental physical parameters. For instance, discrete time sampling has a natural limit if packets of time are used, estimated at $1x10^{-42}$ second. This provides a natural limit to the sampling operation. Also, since noise is preferable to distortion, quantizing will vary given different storage mediums (magnetic, optical, etc.) or transmission mediums (copper, fiber optic, satellite, etc.) for given digitized samples (audio, video, etc.). Reducing random bit error, quantization error, burst error, and the like is done for the singular goal of preserving quality in a given digitized sample. Theoretical perfect error correction is not efficient, given the requirement of a huge allocation of redundant data to detect and correct errors. In the absence of such overhead, all error correction is still based on data redundancy and requires the following operations: error detection to check data validity, error correction to replace erroneous data, and error concealment to hide large errors or substitute data for insufficient data correction. Even with perfect error correction, the goal of a workable digital watermark system for the protection of copyrights would be to distribute copies that are less than perfect but not perceivably different from the original. Ironically, in the present distribution of multimedia, this is the approach taken by content creators when faced with such distribution mechanisms as the INTERNET. As an example, for audio clips commercially exchanged on the World Wide Web (WWW), a part of the INTERNET, 8 bit sampled audio or audio downsampled from 44.1 kHz (CD-quality), to 22 kHz and lower. Digital filters, however, are not ideal because of trade-offs between attenuation and time-domain response, but provide the engineer or similarly-trained individual with a set of decisions to make about maximizing content quality with minimum data overhead and consideration of the ultimate delivery

DISH-Blue Spike-842
Exhibit 1004, Page 0740

mechanism for the content (CDs, cable television, satellite, audio tape, stereo amplifier, etc.).

For audio signals and more generally for other frequency-based content, such as video, one method of using digital filters is to include the use of an input filter to prevent frequency aliasing higher than the so-called Nyquist frequencies. The Nyquist theorem specifies that the sampling frequency must be at least twice the highest signal frequency of the sampled information (e.g., for the case of audio, human perception of audio frequencies is in a range between 20 Hz and 20 kHz). Without an input filter, aliases can still occur leaving an aliased signal in the original bandwidth that cannot be removed.

Even with anti-aliasing filters, quantization error can still cause low level aliasing which may be removed with a dither technique. Dither is a method of adding random noise to the signal, and is used to de-correlate quantization error from the signal while reducing the audibility of the remaining noise. Distortion may be removed, but at the cost of adding more noise to the filtered output signal. An important effect is the subsequent randomization of the quantization error while still leaving an envelope of an unremovable signaling band of noise. Thus, dither is done at low signal levels, effecting only the least significant bits of the samples. Conversely, digital watermarks, which are essentially randomly-mapped noise, are intended to be inserted into samples of digitized content in a manner such as to maximize encoding levels while minimizing any perceivable artifacts that would indicate their presence or allow for removal by filters, and without destroying the content signal. Further, digital watermarks should be inserted with processes that necessitate random searching in the content signal for watermarks if an attacker lacks the keys. Attempts to over-encode noise into known watermarked signal locations to eliminate the information signal can be made difficult or impossible without damaging the content signal by relying on temporal encoding and randomization in the generation of keys during digital watermark insertion. As a result, although the

watermark occupies only a small percentage of the signal, an attacker is forced to over-encode the entire signal at the highest encoding level, which creates audible artifacts.

The present invention relates to methods for obtaining more optimal models to design watermark systems that are tamper-resistant given the number and breadth of existent digitized sample options with differing frequency and time components (audio, video, pictures, multimedia, virtual reality, etc.).

To accomplish these goals, the present invention maintains the highest quality of a given content signal as it was mastered, with its watermarks suitably hidden, taking into account usage of digital filters and error correction presently concerned solely with the quality of content signals.

Additionally, where a watermark location is determined in a random or pseudo-random operation dependent on the creation of a pseudo-random key, as described in copending related application entitled "Steganographic Method and Device" assigned to the present assignee, and unlike other forms of manipulating digitized sample streams to improve quality or encode known frequency ranges, an engineer seeking to provide high levels of protection of copyrights, ownership, etc. is concerned with the size of a given key, the size of the watermark message and the most suitable area and method of insertion. Robustness is improved through highly redundant error correction codes and interleaving, including codes known generally as q-ary Bose-Chaudhuri-Hocquenghem (BCH) codes, a subset of Hamming coding operations, and codes combining error correction and interleaving, such as the Cross-Interleave Reed-Solomon Code. Using such codes to store watermark information in the signal increases the number of changes required to obliterate a given watermark. Preprocessing the certificate by considering error correction and the introduction of random data to make watermark discovery more difficult, prior to watermarking, will help determine sufficient key size. More generally, absolute key size can be

determined through preprocessing the message and the actual digital watermark (a file including information regarding the copyright owner, publisher, or some other party in the chain of exchange of the content) to compute the absolute encoded bit stream and limiting or adjusting the key size parameter to optimize the usage of key bits. The number of bits in the primary key should match or exceed the number of bits in the watermark message, to prevent redundant usage of key bits. Optimally, the number of bits in the primary key should exactly match the watermark size, since any extra bits are wasted computation.

Insertion of informational signals into content signals and ranges from applications that originate in spread spectrum techniques have been contemplated. More detailed discussions are included in copending related applications entitled "Steganographic Method and Device" and entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System".

The following discussion illustrates some previously disclosed systems and their weaknesses.

Typically, previously disclosed systems lack emphasis or implementation of any pseudo-random operations to determine the insertion location, or map, of information signals relating to the watermarks. Instead, previous implementations provide "copy protect" flags in obvious, apparent and easily removable locations. Further, previous implementations do not emphasize the alteration of the content signal upon removal of the copy protection.

Standards for digital audio tape (DAT) prescribe insertion of data such as ISRC (Industry Standard Recording Codes) codes, title, and time in sub-code according to the Serial Copy Management System (SCMS) to prevent multiple copying of the content. One time copying is permitted, however, and systems with AES3 connectors, which essentially override copy protection in the sub-code as implemented by SCMS, actually have no copy limitations. The present invention provides improvement over this

DISH-Blue Spike-842
Exhibit 1004, Page 0743

implementation with regard to the ability of unscrupulous users to load digital data into unprotected systems, such general computing devices, that may store the audio clip in a generalized file format to be distributed over an on-line system for further duplication. The security of SCMS (Serial Copy Management System) can only exist as far as the support of similarly-oriented hardware and the lack of attempts by those skilled in the art to simply remove the subcode data in question.

Previous methods seek to protect content, but shortcomings are apparent. U.S. Patent No. 5,319,735 to Preuss et al. discusses a spread spectrum method that would allow for over-encoding of the described, thus known, frequency range and is severely limited in the amount of data that can be encoded-- 4.3 8-bit symbols per second. However, with the Preuss et al. method, randomization attacks will not result in audible artifacts in the carrier signal, or degradation of the content as the information signal is in the subaudible range. It is important to note the difference in application between spread spectrum in military field use for protection of real-time radio signals, and encoding information into static audio files. In the protection of real-time communications, spread spectrum has anti-jam features, since information is sent over several channels at once. Therefore, in order to jam the signal, one has to jam all channels, including their own. In a static audio file, however, an attacker has practically unlimited time and processing power to randomize each sub-channel in the signaling band without penalty to themselves, so the anti-jam advantages of spread spectrum do not extend to this domain.

In a completely different implementation, U.S. Patent No. 5,379,345 to Greenberg seeks enforcement of broadcast contracts using a spread spectrum modulator to insert signals that are then confirmed by a spread spectrum-capable receiver to establish the timing and length that a given, marked advertisement is played. This information is measured against a specific master of the underlying broadcast material. The Greenberg patent does not ensure that real-time downloads of copyrighted content can be

marked with identification information unless all download access points (PCs, modems, etc.), and upload points for that matter, have spread spectrum devices for monitoring.

Other methods include techniques similar to those disclosed in related copending patent applications mentioned above by the present assignee, but lack the pseudo-random dimension of those patent applications for securing the location of the signals inserted into the content. One implementation conducted by Michael Gerzon and Peter Craven, and described by Ken Pohlmann in the 3rd edition of Principles of Digital Audio, illustrates a technology called "buried data technique," but does not address the importance of randomness in establishing the insertion locations of the informational signals in a given content signal, as no pseudo-random methods are used as a basis for insertion. The overriding concern of the "buried data techniques" appears to be to provide for a "known channel" to be inserted in such a manner as to leave little or no perceivable artifacts in the content signal while prescribing the exact location of the information (i.e., replacing the least significant bits (LSB) in a given information signal). In Gerzon and Craven's example, a 20-bit signal gives way to 4-bits of LSBs for adding about 27 dB of noise to the music. Per channel data insertion reached 176.4 kilobits per second per channel, or 352.8 kbps with stereo channels. Similarly attempted data insertion by the present inventors using random data insertion yielded similar rates. The described techniques may be invaluable to manufacturers seeking to support improvements in audio, video and multimedia quality improvements. These include multiple audio channel support, surround sound, compressed information on dynamic range, or any combination of these and similar data to improve quality. Unfortunately, this does little or nothing to protect the interests of copyright holders from unscrupulous pirates, as they attempt to create unmarked, perfect copies of copyrighted works.

The present invention also relates to copending patent applications

DISH-Blue Spike-842
Exhibit 1004, Page 0745

entitled "Staganographicc Method and Device"; "Method for Human-Assisted Random Key Generation and Application for Digital Watermark System"; and "Method for Stega-Cipher Protection of Computer Code" as mentioned above, specifically addressing the weakness of inserting informational signals or digital watermarks into known locations or known frequency ranges, which are sub-audible. The present invention seeks to improve on the methods disclosed in these patent applications and other methods by describing specific optimization techniques at the disposal of those skilled in the art. These techniques provide an a la carte method for rethinking error correction, interleaving, digital and analog filters, noise shaping, nonlinear random location mapping in digitized samples, hashing, or making unique individual watermarks, localized noise signal mimic encoding to defeat noise filtering over the entire sample stream, super audible spread spectrum techniques, watermark inversion, preanalyzing watermark key noise signatures, and derivative analysis of suspect samples against original masters to evaluate the existence of watermarks with statistical techniques.

The goal of a digital watermark system is to insert a given information signal or signals in such a manner as to leave few or no artifacts in the underlying content signal, while maximizing its encoding level and location sensitivity in the signal to force damage to the content signal when removal is attempted. The present invention establishes methods for estimating and utilizing parameters, given principles of the digitization of multimedia content (audio, video, virtual reality, etc.), to create an optimized "envelope" for insertion of watermarks, and thus establish secured responsibility for digitally sampled content. The pseudo-random key that is generated is the only map to access the information signal while not compromising the quality of the content. A digital watermark naturally resists attempts at removal because it exists as purely random or pseudo-random noise in a given digitized sample. At the same time, inversion techniques and mimicking operations, as well as encoding signal features instead of given

DISH-Blue Spike-842
Exhibit 1004, Page 0746

samples, can make the removal of each and every unique encoded watermark in a given content signal economically infeasible (given the potential commercial returns of the life of a given copyright) or impossible without significantly degrading the quality of the underlying, "protected" signal. Lacking this aesthetic quality, the marketability or commercial value of the copy is correspondingly reduced.

The present invention preserves quality of underlying content signals, while using methods for quantifying this quality to identify and highlight advantageous locations for the insertion of digital watermarks.

The present invention integrates the watermark, an information signal, as closely as possible to the content signal, at a maximal level, to force degradation of the content signal when attempts are made to remove the watermarks.

General methods for watermarking digitized content, as well as computer code, are described in copending related patent applications entitled "Steganographic Method and Device" and entitled "Method for Stega-Cipher Protection of Computer Code", both assigned to the present assignee. Recognizing the importance of perceptual encoding of watermarks by the authors and engineers who actually create content is addressed in copending related application entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System".

The present invention describes methods of random noise creation given the necessary consequence of improving signal quality with digitization techniques. Additionally, methods are described for optimizing projections of data redundancy and overhead in error correction methods to better define and generate parameters by which a watermarking system can successfully create random keys and watermark messages that subsequently cannot be located and erased without possession of the key that acts as the map for finding each encoded watermark. This description will provide the backdrop for establishing truly optimized watermark

DISH-Blue Spike-842
Exhibit 1004, Page 0747

insertion including: use of nonlinear (chaotic) generators; error correction and data redundancy analysis to establish a system for optimizing key and watermark message length; and more general issues regarding desired quality relating to the importance of subjecting watermarked content to different models when the content may be distributed or sold in a number of prerecorded media formats or transmitted via different electronic transmission systems; this includes the use of perceptual coding; particularized methods such as noise shaping; evaluating watermark noise signatures for predictability; localized noise function mimic encoding; encoding signal features; randomizing time to sample encoding of watermarks; and, finally, a statistical method for analyzing composite watermarked content against a master sample content to allow watermark recovery. All of these features can be incorporated into specialized digital signal processing microprocessors to apply watermarks to nongeneralized computing devices, such as set-top boxes, video recorders that require time stamping or authentication, digital video disc (DVD) machines and a multitude of other mechanisms that play or record copyrighted content.

The sampling theorem, known specifically as the Nyquist Theorem, proves that bandlimited signals can be sampled, stored, processed, transmitted, reconstructed, desampled or processed as discrete values. In order for the theorem to hold true, the sampling must be done at a frequency that is at least twice the frequency of the highest signal frequency to be captured and reproduced. Aliasing will occur as a form of signal fold over, if the signal contains components above the Nyquist frequency. To establish the highest possible quality in a digital signal, aliasing is prevented by low-pass filtering the input signal to a given digitization system by a low-pass or anti-aliasing filter. Any residue aliasing which may result in signal distortion, relates to another area of signal quality control, namely, quantization error removal.

Quantization is required in a digitization system. Because of the continuous nature of an analog signal (amplitude vs. time), a quantized

DISH-Blue Spike-842
Exhibit 1004, Page 0748

sample of the signal is an imperfect estimate of the signal sample used to encode it as a series of discrete integers. These numbers are merely estimates of the true value of the signal amplitude. The difference between the true analog value at a discrete time and the quantization value is the quantization error. The more bits allowed per sample, the greater the accuracy of estimation; however, errors still always will occur. It is the recurrent nature of quantization errors that provides an analogy with the location of digital watermarks.

Thus, methods for removal of quantization errors have relevance in methods for determining the most secure locations for placement of watermarks to prevent the removal of such watermarks.

The highest fidelity in digital reproduction of a signal occurs at points where the analog signal converges with a given quantization interval. Where there is no such convergence, in varying degrees, the quantization error will be represented by the following range:

+Q /2 and -Q/2, where Q is the quantization interval.

Indeed, describing maximization of the quantization error and its ratio with the maximum signal amplitude, as measured, will yield a signal-to-error ratio (S/E) which is closely related to the analog signal-to-noise ratio (S/N). To establish more precise boundaries for determining the S/E, with root mean square (rms) quantization error E_{rms}, and assuming a uniform probability density function 1/Q (amplitude), the following describes the error:

$E_{rms}=Q/(12)^{½}$

Signal to quantization error is expressed as:

$S/E=[S_{rms}/E_{rms}]^2=3/2(2^{2n})$

Finally, in decibels (dB) and comparing 16-bit and 15-bit quantization:

$S/E(dB)=10\log[3/2(2^{2n})]=10\log 3/2+2^n\log 2$

(or "$= 20\log[(3/2)^{½}(2^n)]$")

$=6.02n+1.76$

This explains the S/E ratio of 98 dB for 16-bit and 92 dB for 15-bit quantization. The 1.76 factor is established statistically as a result of peak-to-rms ratio of a sinusoidal waveform, but the factor will differ if the signal waveform differs. In complex audio signals, any distortion will exist as white noise across the audible range. Low amplitude signals may alternatively suffer from distortion.

Quantization distortion is directly related with the original signal and is thus contained in the output signal, it is not simply an error. This being the case, implementation of so-called quality control of the signal must use dither. As discussed above, dither is a method of adding random noise to the signal to de-correlate quantization error from the signal while reducing the audibility of the remaining noise. Distortion may be removed at the cost of adding more noise to the filtered output signal. An important effect is the subsequent randomization of the quantization error while still leaving an envelope of an unremovable signaling band of noise. Dither, done at low signal levels, effects only the least significant bits of the samples.

Use of linear and nonlinear quantization can effect the trade-off in the output signal and must be considered for a system of watermarks designed to determine acceptable quantization distortion to contain the digital watermark. For audio systems, block linear quantization implementations have been chosen. However, block floating point and floating point systems, nonuniform companding, adaptive delta modulation, adaptive differential pulse-code modulation, and perceptual coding schemes (which are oriented around the design of filters that closely match the actual perception of humans) appear to provide alternative method implementations that would cause higher perceptible noise artifacts if filtering for watermarks was undertaken by pirates. The choice of method is related to the information overhead desired.

According to one aspect of the present invention, the envelope described in the quantization equations above is suitable for preanalysis of a digitized sample to evaluate optimal locations for watermarks. The

DISH-Blue Spike-842
Exhibit 1004, Page 0750

present example is for audio, but corresponding applications for digitization of video would be apparent in the quantization of color frequencies.

The matter of dither complicates preanalysis of a sample evaluated for digital watermarks. Therefore, the present invention also defines the optimal envelope more closely given the three types of dither (this example is for audio, others exist for video): triangular probability density function (pdf), Gaussian pdf, and rectangular pdf. Again, to establish better boundaries for the random or pseudo-random insertion of a watermark to exist in a region of a content signal that would represent an area for hiding watermarks in a manner most likely to cause damage to the content signal if unauthorized searches or removal are undertaken. Dither makes removal of quantization error more economical through lower data overhead in a system by shifting the signal range to decorrelate errors from the underlying signal. When dither is used, the dither noise and signal are quantized together to randomize the error. Dither which is subtractive requires removing the dither signal after requantization and creates total error statistical independence. It would also provide further parameters for digital watermark insertion given the ultimate removal of the dither signal before finalizing the production of the content signal. With nonsubtractive dither, the dither signal is permanently left in the content signal. Errors would not be independent between samples. For this reason, further analysis with the three types of dither should reveal an acceptable dither signal without materially affecting the signal quality.

Some proposed systems for implementing copyright protection into digitally-sampled content, such as that proposed by Digimarc Corporation, predicate the natural occurrence of artifacts that cannot be removed. Methods for creating a digital signature in the minimized error that is evident, as demonstrated by explanations of dither, point out another significant improvement over the art in the system described in the present invention and its antecedents. Every attempt is made to raise the error level of error from LSBs to a level at which erasure necessarily leads to the

degradation of the "protected" content signal. Furthermore, with such a system, pirates are forced to make guesses, and then changes, at a high enough encoding level over a maximum amount of the content signal so as to cause signal degradation, because guessing naturally introduces error. Thus, dither affects the present invention's envelope by establishing a minimum encoding level. Any encoding done below the dither level might be erased by the dither.

One embodiment of the present invention may be viewed as the provision of a random-super-level non-subtractive dither which contains information (the digital watermark).

To facilitate understanding of how this does not cause audible artifacts, consider the meaning of such encoding in terms of the S/E ratio. In a normal 16-bit signal, there is a 98 dB S/E according to the equation S/E = 6.02n + 1.76. Consider that the encoding of watermark information looks like any other error, except it moves beyond the quantization level, out of the LSBs. If the error is of a magnitude expressed in, say, 8 bits, then at that moment, the signal effectively drops to 8 bits (16-8). This corresponds to a momentary drop in S/E, referred to herein as the momentary S/E. Yet, these errors are relatively few and far between and therefore, since the signal is otherwise comprised of higher-bit samples, a "Perceived S/E" may be derived which is simply the weighted average of the samples using the "Pure S/E" (the samples without watermark information) and those with the Momentary S/E. As a direct consequence, it may be observed that the more sparse the watermark map, the fewer errors introduced in a given range, and the higher the perceived S/E. It also helps that the error is random, and so over time, appears as white noise, which is relatively unobtrusive. In general, it is observed that as long as introduced errors leave resulting samples within an envelope in the sample window described by minimum and maximum values, before error introduction, and the map is sufficiently sparse, the effects are not perceived.

In addition, it is possible to obtain an even higher Perceived S/E by allowing the range of introduced errors to vary between a minimum and maximum amount. This makes the weighted average S/E higher by reducing the average introduced error level. Yet, someone trying to erase a watermark, assuming they knew the maximum level, would have to erase at that level throughout the data, since they would not know how the introduced level varies randomly, and would want to erase all watermarks.

A watermarking cipher could perform this operation and may also introduce the further step of local dither (or other noise) significantly above the quantization amplitude on a window by window basis randomly, to restrict total correlation between the watermark signal and the probability that it remains independent between samples, as with subtractive dither implementations that are mostly concerned with the ultimate removal of the dither signal with requantization. This ability could be used to accomplish signal doping, which adds a degree of random errors that do not contain watermark information so as to prevent differential analysis of multiple watermarked copies. Alternatively, it could be used to mimic a specific noise function in a segment of the signal in order to defeat attempts to filter a particular type of noise over the entire signal. By varying this function between watermarks, it may be guaranteed that any particular filter is of no use over the whole signal. By applying several filters in series, it seems intuitive that the net results would be significantly different from the original signal.

The discussion may be more appropriately introduced with perceptual coding techniques, but a watermarking system could also defeat some detection and correction with dither by inserting watermarks into signal features, instead of signal samples. This would be equivalent to looking for signal characteristics, independent of the overall sample as it exists as a composite of a number of signals. Basically, instead of encoding on a bit per sample basis, one might spread bits over several samples. The point of doing this is that filtering and convolution operations, like "flanging", which

DISH-Blue Spike-842
Exhibit 1004, Page 0753

definitely change individual samples on a large scale, might leave intact enough of a recognizable overall signal structure (the relationship between multiple samples) to preserve the watermark information. This may be done by measuring, generalizing, and altering features determined by the relationships between samples or frequency bands. Because quantization is strictly an art of approximation, signal-to-error ratios, and thus the dynamic range of a given system are determined.

The choice of eliminating quantization distortion at the expense of leaving artifacts (not perceptible) is a permanent trade-off evident in all digitization systems which are necessarily based on approximation (the design goal of the present invention in preanalyzing a signal to mask the digital watermarks make imperceptibility possible). The high fidelity of duplication and thus subsequent ability to digitally or electronically transmit the finished content (signal) is favored by consumers and artists alike. Moreover, where there continues to be a question of approximating in quantization-- digital watermark systems will have a natural partner in seeking optimized envelopes in the multitude and variety of created digitized content.

Another aspect of optimizing the insertion of digital watermarks regards error correction. Highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks. A detailed description follows from the nature of a digitization system-- binary data can be corrected or concealed when errors exist. Random bit errors and burst errors differ in their occurrence:

Random bit errors are error bits occurring in a random manner, whereas burst errors may exist over large sequences of the binary data comprising a digitized signal. Outside the scope of the present invention are errors caused by physical objects, such as dust and fingerprints, that contribute to the creation of dropouts are different from the errors addressed herein.

DISH-Blue Spike-842
Exhibit 1004, Page 0754

Measuring error with bit-error ratio (BER), block error ratio (BLER) and burst-error length (BERL), however, provides the basis of error correction. Redundancy of data is a focus of the present invention. This data necessarily relies on existing data, the underlying content. To efficiently describe optimal parameters for generating a cryptographic key and the digital watermark message discussion of error correction and error concealment techniques is important.

Forms of error detection include one-bit parity, relying on the mathematical ability to cast out numbers, for binary systems including digitization systems, such as 2. Remainders given odd or even results (parity) that are probablistically determined to be errors in the data. For more appropriate error detection algorithms, such as Cyclic Redundancy Check Code (CRCC), which are suited for the detection of commonly occurring burst error. Pohlmann (Principles of Digital Audio) notes the high accuracy of CRCC (99.99%) and the truth of the following statements given a k-bit data word with m bits of CRCC, a code word of n bits is formed (m=n-k):

- burst errors less than or equal to m bits are always predictable.
- the detection probability of burst errors of m+1 bits = $1-2^{-m+1}$.
- the detection probability of burst errors longer than m+1 bits = $1-2^{-m}$
- random errors up to 3 consecutive bits long can be detected.

The medium of content delivery, however, provides the ultimate floor for CRCC design and the remainder of the error correction system.

Error correction techniques can be broken into three categories: methods for algebraic block codes, probablistic methods for convolutional codes, and cross-interleave code where block codes are used in a convolution structure. As previously discussed, the general class of codes that assist in pointing out the location of error are known generally as Hamming codes, versus CRCC which is a linear block code.

DISH-Blue Spike-842
Exhibit 1004, Page 0755

What is important for establishing parameters for determining optimized error coding in systems such as digital audio are more specifically known as Reed-Solomon Codes which are effective methods for correcting burst errors. Certain embodiments of the present invention presuppose the necessity of highly redundant error codes and interleaving, such as that done in Cross Interleave Reed-Solomon Code, to counter burst errors typically resulting from randomization attacks. More generally, certain embodiments of the present invention include the use of Hamming Codes of (n,n) to provide n-1 bit error detection and n-2 bit error correction. Further, a Hamming distance of n (or greater than n) is significant because of the nature of randomization attacks. Such an attack seeks to randomize the bits of the watermark message. A bit can be either 0 or 1, so any random change has a 50% chance of actually changing a bit from what it was (50% is indicative of perfect randomness). Therefore, one must assume that a good attack will change approximately half the bits (50%). A Hamming distance of n or greater, affords redundancy on a close par with such randomization. In other words, even if half the bits are changed, it would still be possible to recover the message.

Because interleaving and parity makes data robust for error avoidance, certain embodiments of the present invention seek to perform time interleaving to randomly boost momentary S/E ratio and give a better estimate of not removing keys and watermarks that may be subsequently determined to be "errors."

Given a particular digital content signal, parity, interleaving, delay, and cross-interleaving, used for error correction, should be taken into account when preprocessing information to compute absolute size requirements of the encoded bit stream and limiting or adjusting key size parameters to optimize and perhaps further randomize usage of key bits. In addition, these techniques minimize the impact of errors and are thus valuable in creating robust watermarks.

DISH-Blue Spike-842
Exhibit 1004, Page 0756

Uncorrected errors can be concealed in digital systems. Concealment offers a different dynamic to establish insertion parameters for the present invention. Error concealment techniques exist because it is generally more economical to hide some errors instead of requiring overly expensive encoders and decoders and huge information overheads in digitization systems. Muting, interpolation, and methods for signal restoration (removal of noise) relate to methods suggested by the present invention to invert some percentage or number of watermarks so as to ensure that at least some or as many as half of the watermarks must still remain in the content signal to effectively eliminate the other half. Given that a recording contains noise, whether due to watermarks or not, a restoration which "removes" such noise is likely to result in the changing of some bit of the watermark message. Therefore, by inverting every other watermark, it is possible to insure that the very act of such corrections inverts enough watermark bits to create an inverse watermark. This inversion presupposes that the optimized watermark insertion is not truly optimal, given the will of a determined pirate to remove watermarks from particularly valuable content. Ultimately, the inability to resell or openly trade unwatermarked content will help enforce, as well as dictate, the necessity of watermarked content for legal transactions.

The mechanisms discussed above reach physical limits as the intent of signal filtering and error correction are ultimately determined to be effective by humans-- decidedly analog creatures. All output devices are thus also analog for playback.

The present invention allows for a preprocessed and preanalyzed signal stream and watermark data to be computed to describe an optimized envelope for the insertion of digital watermarks and creation of a pseudo-random key, for a given digitized sample stream. Randomizing the time variable in evaluating discrete sample frames of the content signal to introduce another aspect of randomization could further the successful insertion of a watermark. More importantly, aspects of perceptual coding

DISH-Blue Spike-842
Exhibit 1004, Page 0757

are suitable for methods of digital watermarks or super-audible spread spectrum techniques that improve on the art described by the Preuss et al. patent described above.

The basis for a perceptual coding system, for audio, is psychoacoustics and the analysis of only what the human ear is able to perceive. Similar analysis is conducted for video systems, and some may argue abused, with such approaches as "subliminal seduction" in advertising campaigns. Using the human for design goals is vastly different than describing mathematical or theoretical parameters for watermarks. On some level of digital watermark technology, the two approaches may actually complement each other and provide for a truly optimized model.

The following example applies to audio applications. However, this example and other examples provided herein are relevant to video systems as well as audio systems. Where a human ear can discern between energy inside and outside the "critical band," (described by Harvey Fletcher) masking can be achieved. This is particularly important as quantization noise can be made imperceptible with perceptual coders given the maintenance of a sampling frequency, decreased word length (data) based on signaling conditions. This is contrasted with the necessary decrease of 6 dB/bit with decreases in the sampling frequency as described above in the explanation of the Nyquist Theorem. Indeed, data quantity can be reduced by 75%. This is an extremely important variable to feed into the preprocessor that evaluates the signal in advance of "imprinting" the digital watermark.

In multichannel systems, such as MPEG-1, AC-3 and other compression schemes, the data requirement (bits) is proportional to the square root of the number of channels. What is accomplished is masking that is nonexistent perceptually, only acoustically.

Taken to another level for digital watermarking, which is necessary for content that may be compressed and decompressed, forward adaptive

DISH-Blue Spike-842
Exhibit 1004, Page 0758

allocation of bits and backward adaptive allocation provide for encoding signals into content signals in a manner such that information can be conveyed in the transmission of a given content signal that is subsequently decoded to convey the relatively same audible signal to a signal that carries all of its bits-- e.g., no perceptual differences between two signals that differ in bit size. This coding technique must also be preanalyzed to determine the most likely sample bits, or signal components, that will exist in the smaller sized signal. This is also clearly a means to remove digital watermarks placed into LSBs, especially when they do not contribute theoretically perceptible value to the analyzed signal. Further methods for data reduction coding are similarly important for preanalyzing a given content signal prior to watermarking. Frequency domain coders such as subband and transform bands can achieve data reduction of ratios between 4:1 and 12:1. The coders adaptively quantize samples in each subband based on the masking threshold in that subband (See Pohlmann, Principles of Digital Audio). Transform coders, however, convert time domain samples into the frequency domain for accomplishing lossless compression. Hybrid coders combine both subband and transform coding, again with the ultimate goal of reducing the overall amount of data in a given content signal without loss of perceptible quality.

With digital watermarks, descriptive analysis of an information signal is important to preanalyze a given watermark's noise signature. Analysis of this signature versus the preanalysis of the target content signal for optimized insertion location and key/message length, are potentially important components to the overall implementation of a secure watermark. It is important that the noise signature of a digital watermark be unpredictable without the pseudo-random key used to encode it. Noise shaping, thus, has important applications in the implementation of the present invention. In fact, adaptive dither signals can be designed to correlate with a signal so as to mask the additional noise-- in this case a digital watermark. This relates to the above discussion of buried data

DISH-Blue Spike-842
Exhibit 1004, Page 0759

techniques and becomes independently important for digital watermark systems. Each instance of a watermark, where many are added to a given content signal given the size of the content and the size of the watermark message, can be "noise shaped" and the binary description of the watermark signature may be made unique by "hashing" the data that comprises the watermark. Generally, hashing the watermark certificate prior to insertion is recommended to establish differences between the data in each and every watermark "file."

Additionally, the present invention provides a framework in which to analyze a composite content signal that is suspected to contain a watermarked sample of a copyrighted work, against an unwatermarked original master of the same sample to determine if the composite content actually contains a copy of a previously watermarked content signal. Such an analysis may be accomplished in the following scenario:

- Assume the composite signal contains a watermark from the sample.

- Assume the provision of the suspect composite signal $C_w(t)$ (w subscript denotes a possible watermark) and the unwatermarked original sample $S_{uw}(t)$. These are the only two recordings the analyzer is likely to have access to.

Now, it is necessary to recover a watermarked sample $S_w(t)$.

The methods of digital signal processing allow for the computation of an optimal estimate of a signal. The signal to be estimated is the composite minus the watermarked sample, or $C"_w(t) = C_w(t) - S_w(t)$. The analyzer, however, cannot determine a value of $S_w(t)$, since it does not know which of the many possible $S_w(t)$ signals was used in the composite. However, a close estimate may be obtained by using $S_{uw}(t)$, since watermarking makes relatively minor changes to a signal.

So, $C"_w(t)$ (an estimate of $C'_w(t)$ given $C_w(t)$ and $S_{uw}(t)$) may be obtained. Once $C"_w(t)$ is calculated, it is simply subtracted from $C_w(t)$. This yields $S'_w(t) = C_w(t) - C"_w(t)$. If the watermark is robust enough, and the estimate good enough,

DISH-Blue Spike-842
Exhibit 1004, Page 0760

then $S'_w(t)$, which is approximately equal to $S_w(t)$, can be processed to extract the watermark. It is simply a matter of attempting watermark decoding against a set of likely encoding key candidates.

Note that although a watermark is initially suspected to be present in the composite, and the process as if it is, the specifics of the watermark are not known, and a watermark is never introduced into the calculations, so a watermark is extracted, it is valid, since it was not introduced by the signal processing operations.

The usefulness of this type of operation is demonstrated in the following scenario:

People are interested in simply proving that their copyrighted sample was dubbed into another recording, not the specifics of ownership of the sample used in the dubbing. So, this implies that only a single, or limited number of watermark keys would be used to mark samples, and hence, the decode key candidates are limited, since the same key would be used to encode simple copyright information which never varies from copy to copy.

There are some problems to solve to accomplish this sort of processing. The sample in question is generally of shorter duration than the composite, and its amplitude may be different from the original. Analysis techniques could use a combination of human-assisted alignment in the time domain, where graphical frequency analysis can indicate the temporal location of a signal which closely matches that of the original sample. In addition, automatic time warping algorithms which time align separate signals, on the assumption they are similar could also be used to solve temporal problems. Finally, once temporal alignment is accomplished, automatic amplitude adjustment could be performed on the original sample to provide an optimal match between the composite section containing the sample and the original sample.

It may be desirable to dynamically vary the encoding/decoding algorithm during the course of encoding/decoding a signal stream with a given watermark. There are two reasons for dynamically varying the encoding/decoding algorithm.

DISH-Blue Spike-842
Exhibit 1004, Page 0761

The first reason for dynamically varying the encoding/decoding algorithm is that the characteristics of the signal stream may change between one locality in the stream and another locality in the stream in a way that significantly changes the effects that a given encoding algorithm may have on the perception of that section of the stream on playback. In other words, one may want the encoding algorithm, and by implication, the decoding algorithm, to adapt to changes in the signal stream characteristics that cause relative changes in the effects of the encoding algorithm, so that the encoding process as a whole causes fewer artifacts, while maintaining a certain level of security or encoding a given amount of information.

The second reason for dynamically varying the encoding/decoding algorithm is simply to make more difficult attempts at decoding watermarks without keys. It is obviously a more difficult job to attempt such attacks if the encoding algorithm has been varied. This would require the attacker to guess the correct order in which to use various decoding algorithms.

In addition, other reasons for varying the encoding/decoding algorithms may arise in the future.

Two methods for varying of the encoding/decoding algorithms according to embodiments of the present invention are described herein. The first method corresponded to adaptation to changing signal characteristics. This method requires a continuous analysis of the sample windows comprising the signal stream as passed to the framework. Based on these characteristics, which are mathematically well-defined functions of the sample stream (such as RMS energy, RMS/peak ratio, RMS difference between samples - which could reflect a measure of distortion), a new CODEC module, from among a list of pre-defined CODECs, and the algorithms implemented in them, can be applied to the window in question. For the purpose of this discussion, windows are assumed to be equivalent to frames. And, in a frame-based system, this is a straightforward application of the architecture to provide automated variance of algorithms to encode and decode a single watermark.

DISH-Blue Spike-842
Exhibit 1004, Page 0762

The second method for varying of the encoding/decoding algorithms corresponds to increased security. This method is easier, since it does not require the relatively computationally-expensive process of further analyzing the samples in a frame passed to the Framework. In this method, the Framework selects a new CODEC, from among a list of pre-defined CODECs, to which to pass the sample frame as a function of the pseudo-random key employed to encode/decode the watermark. Again, this is a straightforward application of framework architecture which provides automated variance of algorithms to encode and decode a single watermark versus limitations evident in the analysis of a single random noise signal inserted over the entire content signal as proposed by Digimarc, NEC, Thorn EMI and IBM under the general guise of spread spectrum, embedded signalling schemes.

It is important to note that the modular framework architecture, in which various modules including CODECs are linked to keys, provides a basic method by which the user can manually accomplish such algorithmic variations for independent watermarks. The main difference detailed above is that an automated method to accomplish this can be used within single watermarks.

Automated analysis of composited copyrighted material offers obvious advantages over subjective "human listening" and "human viewing" methods currently used in copyright infringement cases pursued in the courts.

DISH-Blue Spike-842
Exhibit 1004, Page 0763

What Is Claimed Is:

1. A method for amplitude independent encoding of digital watermark information in a signal, comprising steps of:

determining in said signal a sample window having a minimum and a maximum;

determining a quantization interval of said sample window, where said quantitization interval can be used to quantize normalized window samples;

normalizing the sample window to provide normalized samples, where normalized samples conform to a limited range of values, proportional to real sample values, and comprise a representation of the real sample values with a resolution higher than the real range of values, and where the normalized values can be divided by the quantization interval into distinct quantization levels;

analyzing the normalized samples to determine quantization levels;

comparing the message bits to the corresponding quantization level information from the analyzing step;

when a bit conflicts with the quantization level, adjusting the quantization level of said sample window to correspond to the message bit; and

de-normalizing the analyzed normalized samples.

2. The method according to claim 1, wherein watermark signal characteristics or a watermark certificate can be compressed.

3. A method for amplitude independent decoding of digital watermark information in a signal comprising steps of:

determining in said signal a sample window having a minimum and a maximum;

determining a quantization interval of said sample window, where said quantitization interval can be used to quantize normalized window samples;

DISH-Blue Spike-842
Exhibit 1004, Page 0764

normalizing the sample window to provide samples, where normalized samples conform to a limited range of values, proportional to real sample values, and comprise a representation of the real sample values with a resolution higher than the real range of values, and where the normalized values can be divided by the quantization interval into distinct quantization levels; and

analyzing the quantization level of said samples to determine a message bit value.

4. The method according to claim 3, wherein watermark signal characteristics or a watermark certificate can be compressed.

5. A method of encoding and decoding watermarks in a signal, comprising insertion and detection of abstract signal features in said signal to carry watermark information, wherein said abstract signal features are mathematical functions of the input sample window, and by extension, adjacent sample windows.

6. A method of pre-analyzing a digital signal for encoding digital watermarks using a digital filter comprising determining what changes in the digital signal will be affected by the digital filter.

7. The method according to claim 6, further comprising a step of encoding watermarks so as to either avoid frequency or time delimited areas of the signal which will be changed by the digital filter, or ensure that the watermark will survive the changes instroduced by the digital filter.

8. A method of error coding watermark message certificates using cross interleaved codes which use error codes of high redundancy, including codes with Hamming distances of greater than or equal to n, wherein is a number of bits in a message block.

DISH-Blue Spike-842
Exhibit 1004, Page 0765

9. A method of pre-processing a watermark message certificate comprising determining an exact length of the watermark message as it will be encoded.

10. The method according to claim 9, further comprising a step of generating a watermark key which will provide at least one unique bit for each bit comprising the watermark message.

11. A method of generating watermark pseudo-random key bits using a non-linear generator.

12. A method of generating watermark pseudo-random key bits using a chaotic generator.

13. A method of mapping pseudo-random key and processing state information to effect an encode / decode map using a non-linear generator.

14. A method of mapping pseudo-random key and processing state information to effect an encode / decode map using a chaotic generator.

15. A method of guaranteeing watermark certificate uniqueness comprising attaching a timestamp or user identification dependent hash or message digest of watermark certificate data to the certificate.

16. A method of generating and modulating a local noise signal to contain watermark information, wherein the noise signal is a function of at least one variable which depends on key and processing state information.

DISH-Blue Spike-842
Exhibit 1004, Page 0766

17. A method of dithering watermark quantizations such that the dither changes an absolute quantization value, but does not change a quantization level or information carried in the quantization.

18. A method of encoding watermarks comprising steps of:

inverting at least one instance of the watermark bit stream; and

encoding at least one instance of the watermark using said inverted instance of the watermark bit stream.

19. A method of decoding watermarks comprising steps of:

considering an original watermark synchronization marker, an inverted watermark synchronization marker, and inverted watermarks; and

decoding based on the considering step.

20. A method of encoding and decoding watermarks in a signal using a spread spectrum technique to encode or decode where information is encoded or decoded at audible levels and the encoding and decoding methods are pseudo-random over frequency.

21. A method of encoding and decoding watermarks in a signal using a spread spectrum technique to encode or decode where information is encoded or decoded at audible levels and the encoding and decoding methods are pseudo-random over time.

22. The method of claim 21, wherein the information is encoded or decoded at audible levels and the encoding and decoding methods are pseudo-random, over both frequency and time.

23. A method of analyzing composite digitized signals for watermarks comprising steps of:

DISH-Blue Spike-842
Exhibit 1004, Page 0767

obtaining a composite signal;

obtaining an unwatermarked sample signal;

time aligning the unwatermarked sample signal to the composite signal;

gain adjusting the time aligned unwatermarked sample signal to a corresponding segment of the composite signal, determined in the time aligning step;

estimating a pre-composite signal using the composite signal and the gain adjusted unwatermarked sample signal;

estimating a watermarked sample signal by subtracting the estimated pre-composite signal from the composite signal; and

scanning the estimated watermarked sample signal for watermarks.

24. A method for varying watermark encode/decode algorithms automatically during the encoding or decoding of a watermark comprising steps of:

a) assigning a list of desired CODECs to a list of corresponding signal characteristics which indicate use of particular CODECs;

b) during encoding/decoding, analyzing characteristics of the current sample frame in the signal stream, prior to delivering the frame to a CODEC;

c) looking up the corresponding CODEC from the list of CODECs in step (a) which matches the observed signal characteristics from step (b);

d) loading and/or preparing the desired CODEC;

e) passing the sample frame to the CODEC selected in step (c); and

f) receiving the output samples from step (e).

25. The method according to claim 24, wherein watermark signal characteristics or a watermark certificate can be compressed.

DISH-Blue Spike-842
Exhibit 1004, Page 0768

26. A method for varying watermark encode/decode algorithms automatically during the encoding or decoding of a watermark comprising steps of:

a) assigning a list of desired CODECs to a list of index values which correspond to values computed as a function of the pseudo-random watermark key and the state of the processing framework;

b) during encoding/decoding, computing the pseudo-random key index value for the current sample frame in the signal stream, prior to delivering the frame to a CODEC;

c) looking up the corresponding CODEC from the list of CODECs in step (a) which matches the index value from step (b);

d) loading and/or preparing the desired CODEC;

e) passing the sample frame to the CODEC selected in step (c); and

f) receiving the output samples from step (e).

27. The method according to claim 26, wherein watermark signal characteristics or a watermark certificate can be compressed.

DISH-Blue Spike-842
Exhibit 1004, Page 0769

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/11455

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :G09C 5/00 H04L 9/00
US CL :380/54, 3, 4, 23, 55; 283/73, 113, 17
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/54, 3, 4, 23, 55, 49, 51, 59; 283/73, 113, 17

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, E	US 5,664,018 A (LEIGHTON) 02 SEPTEMBER 1997	1-27
A, P	US, 5,636,292 A (RHOADS) 03 JUNE 1997	1-27
A, P	US 5,617,119 A (BRIGGS ET AL.) 01 APRIL 1997	1-27
A, P	US 5,568,570 A (RABBANI) 22 OCTOBER 1996	1-27
A, P	US 5,530,759 A (BRAUDAWAY, ET AL.) 25 JUNE 1996	1-27
A	US 5,493,677 A (BALOGH, ET AL.) 20 FEBRUARY 1996	1-27

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
23 OCTOBER 1997

Date of mailing of the international search report
23 DEC 1997

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
DAVID CAIN
Telephone No. (703) 305-1836

Form PCT/ISA/210 (second sheet)(July 1992)*

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04N 1/32 — A1

(11) International Publication Number: WO 99/52271

(43) International Publication Date: 14 October 1999 (14.10.99)

(21) International Application Number: PCT/US99/07262

(22) International Filing Date: 2 April 1999 (02.04.99)

(30) Priority Data:
09/053,628 2 April 1998 (02.04.98) US

(71)(72) Applicant and Inventor: MOSKOWITZ, Scott, A. [US/US]; 16711 Collins Avenue #2505, Miami, FL 33160 (US).

(74) Agents: CHAPMAN, Floyd, B. et al.; Baker & Botts, L.L.P., The Warner, 1299 Pennsylvania Avenue, N.W., Washington, DC 20004 (US).

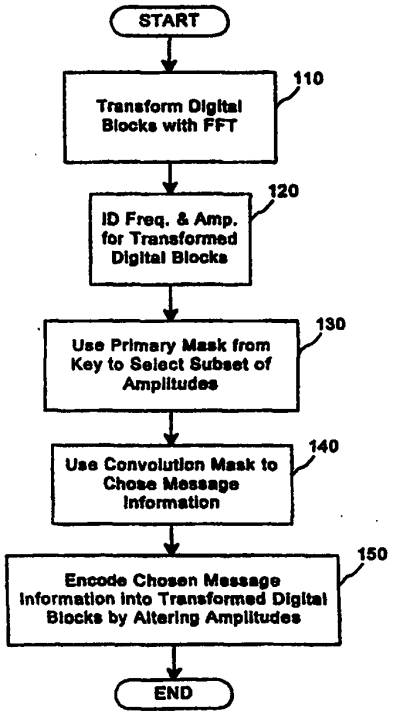
(81) Designated States: JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: MULTIPLE TRANSFORM UTILIZATION AND APPLICATIONS FOR SECURE DIGITAL WATERMARKING

(57) Abstract

Multiple transform utilization and applications for secure digital watermarking. In one embodiment of the present invention, digital blocks in digital information to be protected are transformed into the frequency domain using a fast Fourier transform. A plurality of frequencies and associated amplitudes are identified for each of the transformed digital blocks and a subset of the identified amplitudes is selected for each of the digital blocks using a primary mask from a key. Message information is selected from a message using a transformation table generated with a convolution mask. The chosen message information is encoded into each of the transformed digital blocks by altering the selected amplitudes based on the selected message information.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

MULTIPLE TRANSFORM UTILIZATION AND APPLICATIONS FOR SECURE DIGITAL WATERMARKING

BACKGROUND

Field of the Invention

The invention relates to the protection of digital information. More particularly, the invention relates to multiple transform utilization and applications for secure digital watermarking.

Cross-Reference To Related Applications

This application claims the benefit of U.S. patent application Serial No. 08/587,943, filed January 17, 1996, entitled "Method for Stega-Cipher Protection of Computer Code," the entire disclosure of which is hereby incorporated by reference.

Description of the Background

Increasingly, commercially valuable information is being created and stored in "digital" form. For example, music, photographs and video can all be stored and transmitted as a series of numbers, such as 1's and 0's. Digital techniques let the original information be recreated in a very accurate manner. Unfortunately, digital techniques also let the information be easily copied without the owner's permission.

Digital watermarks exist at a convergence point where creators and publishers of digitized multimedia content demand local, secure identification and authentication of content. Because piracy discourages the distribution of valuable digital information, establishing responsibility for copies and derivative copies of such works is important. The goal of a digital watermark system is to insert a given information signal or signals in such a manner as to leave little or no artifacts, with one standard being perceptibility, in the underlying content signal, while maximizing its encoding level and "location sensitivity" in the signal to force damage to the content signal when removal is attempted. In considering the various forms of multimedia content, whether "master," stereo, National Television Standards Committee (NTSC) video, audio tape or compact disc, tolerance of quality will vary with individuals and affect the underlying commercial and aesthetic value of the content. It is desirable to tie copyrights, ownership rights, purchaser information or some combination of these and related data into the content in such a manner that the content undergoes damage, and therefore

reduction of its value, with subsequent unauthorized distribution, commercial or otherwise. Digital watermarks address many of these concerns and research in the field has provided a rich basis for extremely robust and secure implementations.

Of particular concern is the balance between the value of a digitized "piece" of content and the cost of providing worthwhile "protection" of that content. In a parallel to real world economic behavior, the perceived security of a commercial bank does not cause people to immediately deposit cash because of the expense and time required to perform a bank deposit. For most individuals, possession of a US$100 bill does not require any protection beyond putting it into a wallet. The existence of the World Wide Web, or "Web," does not implicitly indicate that value has been created for media which can be digitized, such as audio, still images and other media. The Web is simply a medium for information exchange, not a determinant for the commercial value of content. The Web's use to exchange media does, however, provide information that helps determine this value, which is why responsibility over digitized content is desirable. Note that digital watermarks are a tool in this process, but they no not replace other mechanisms for establishing more public issues of ownership, such as copyrights. Digital watermarks, for example, do not replace the "historical average" approach to value content. That is, a market of individuals willing to make a purchase based solely on the perceived value of the content. By way of example, a picture distributed over the Internet, or any other electronic exchange, does not necessarily increase the underlying value of the picture, but the opportunity to reach a greater audience by this form of "broadcast" may be a desirable mechanism to create "potentially" greater market-based valuations. That decision rests solely with the rights holder in question.

Indeed, in many cases, depending on the time value of the content, value may actually be reduced if access is not properly controlled. With a magazine sold on a monthly basis, it is difficult to assess the value of pictures in the magazine beyond the time the magazine is sold. Compact disc valuations similarly have time-based variables, as well as tangible variables such as packaging versus the package-less electronic exchange of the digitized audio signals. The Internet only provides a means to more quickly reach consumers and does not replace the otherwise "market-based"

value. Digital watermarks, properly implemented, add a necessary layer of ownership determination which will greatly assist in determining and assessing value when they are "provably secure." The present invention improves digital watermarking technology while offering a means to properly "tamper proof" digitized content in a manner analogous to methods for establishing authenticity of real world goods.

A general weakness in digital watermark technology relates directly to the way watermarks are implemented. Too many approaches leave detection and decode control with the implementing party of the digital watermark, not the creator of the work to be protected. This fundamental aspect of various watermark technologies removes proper economic incentives for improvement of the technology when third parties successfully exploit the implementation. One specific form of exploitation obscures subsequent watermark detection. Others regard successful over encoding using the same watermarking process at a subsequent time.

A set of secure digital watermark implementations address this fundamental control issue, forming the basis of "key-based" approaches. These are covered by the following patents and pending applications, the entire disclosures of which are hereby incorporated by reference: US Patent No. 5,613, 004 entitled "Steganographic Method and Device" and its derivative US patent application Serial No. 08/775,216, US patent application Serial No. 08/587,944 entitled "Human Assisted Random Key Generation and Application for Digital Watermark System," US Patent Application Serial No. 08/587,943 entitled "Method for Stega-Cipher Protection of Computer Code," US patent application Serial No. 08/677,435 entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data," and US Patent Application Serial No. 08/772,222 entitled "Z-Transform Implementation of Digital Watermarks." Public key crypto-systems are described in US Patents No. 4,200,770, 4,218,582, 4,405,829 and 4,424,414, the entire disclosures of which are also hereby incorporated by reference.

By way of improving these digital watermark security methods, utilization of multiple transforms, manipulation of signal characteristics and the requisite relationship to the mask set or "key" used for encoding and decoding operations are envisioned, as

are optimized combinations of these methods. While encoding a watermark may ultimately differ only slightly in terms of the transforms used in the encoding algorithm, the greater issues of an open, distributed architecture requires more robust approaches to survive attempts at erasure, or even means for making detection of the watermark impossible. These "attacks," when computationally compared, may be diametrically related. For instance, cropping and scaling differ in signal processing orientation, and can result in the weakening of a particular watermarking approach but not all watermarking approaches.

Currently available approaches that encode using either a block-based or entire data set transform necessarily encode data in either the spatial or frequency domains, but never both domains. A simultaneous crop and scale affects the spatial and frequency domains enough to obscure most available watermark systems. The ability to survive multiple manipulations is an obvious benefit to those seeking to ensure the security of their watermarked media. The present invention seeks to improve on key-based approaches to watermarking previously disclosed, while offering greater control of the subsequently watermarked content to rights owners and content creators.

Many currently available still image watermarking applications are fundamentally different from the key-based implementations. Such products include products offered by Digimarc and Signum, which seek to provide a robust watermark by encoding watermark messages that rely entirely on comparisons with the original image for decode operations. The subsequent result of the transform, a discrete cosine transform performed in blocks, is digital signed. The embedded watermarks lack any relationship to the perceptual qualities of the image, making inverse application of the publicly available decoders a very good first line of attack. Similarly, the encoding process may be applied by third parties, as demonstrated by some robustness tests, using one process to encode over the result of an image watermarked with another process. Nonrepudiation of the watermark is not possible, because Digimarc and Signum act as the repository of all registrations of the image's ownership.

Another line of attack is a low pass filter that removes some of the high frequency noise that has been added, making error-free detection difficult or impossible.

Finally, many tests of a simple JPEG transform indicate the watermarks may not survive as JPEG is based on the same transforms as the encoding transforms used by the watermarking process. Other notable implementations, such as that offered by Signafy (developed by NEC researchers), appear to encode watermark messages by performing a transform of the entire image. The goal of this process is to more consistently identify "candidate" watermark bits or regions of the image to encode in perceptually significant regions of the signal. Even so, Signafy relies on the original unwatermarked image to accomplish decoding.

All of these methods still rely on the original unwatermarked image to ensure relatively error-free detection of the watermarks. The steganographic method seeks to provide watermark security without an original unwatermarked copy of the media for decode operations, as well as providing users cryptographic security with ciphered symmetric keys. That is, the same key is used for encode and decode operations. Public key pairs, where each user has a public/private key pair to perform asymmetric encode and decode operations, can also be used. Discussions of public key encryption and the benefits related to encryption are well documented. The growing availability of a public key infrastructure also indicates recognition of provable security. With such key-based implementations of watermarking, security can be off-loaded to the key, providing for a layered approach to security and authentication of the watermark message as well as the watermarked content.

It is known that attacks on the survivability of other implementations are readily available. Interesting network-based attacks on the watermark message are also known which fool the central registration server into assuming an image is owned by someone other than the registered owner. This also substantiates the concern that centralized watermarking technologies are not robust enough to provide proper assurances as to the ownership of a given digitized copy of an multimedia work.

Because the computational requirements of performing multiple transforms may not be prohibitive for certain media types, such as still images and audio, the present invention seeks to provide a means to securely watermark media without the need for an original unwatermarked copy to perform decoding. These transforms may be

performed in a manner not plainly evident to observers or the owner of the content, who may assume the watermark is still detectable. Additionally, where a particular media type is commonly compressed (JPEG, MPEG, etc.), multiple transforms may be used to properly set the mask sets, prior to the watermarking process, to alert a user to survivability prior to the release of a watermarked, and thus perceived, "safe" copy to unknown parties. The result of the present invention is a more realistic approach to watermarking taking the media type, as well as the provable security of the keys into consideration. A more trusted model for electronic commerce is therefore possible.

The creation of an optimized "envelope" for insertion of watermarks to establish secured responsibility for digitally-sampled content provides the basis of much watermark security but is also a complementary goal of the present invention. The predetermined or random key that is generated is not only an essential map to access the hidden information signal, but is also the a subset of the original signal making direct comparisons with the original signal unnecessary. This increases the overall security of the digital watermark.

Survival of simultaneous cropping and scaling is a difficult task with image and audio watermarking, where such transformations are common with the inadvertent use of images and audio, and with intentional attacks on the watermark. The corresponding effects in audio are far more obvious, although watermarks which are strictly "frequency-based," such as variations of spread spectrum, suffer from alignment issues in audio samples which have been "cropped," or clipped from the original length of the piece. Scaling is far more noticeable to the human auditory system, though slight changes may affect frequency-only-type watermarks while not being apparent to a consumer. The far greater threat to available audio watermark applications, most of which are variations of frequency-based embedded signaling, are generally time-based transformations, including time-based compression and expansion of the audio signal. Signafy is an example of spread spectrum-based watermarking, as are applications by Solana Technology, CRL, BBN, MIT, etc. "Spatial domain" approaches are more appropriate designations for the technologies deployed by Digimarc, Signum, ARIS, Arbitron, etc. Interestingly, a time-based approached when considered for images is

basically a "spatial-based" approach. The pixels are "convolutional." The difference being that the "spread spectrum-ed" area of the frequencies is "too" well-defined and thus susceptible to over-encoding of random noise at the same sub-bands as that of the embedded signal.

Giovanni uses a block-based approach for the actual watermark. However, it is accompanied by image-recognition capable of restoring a scaled image to its original scale. This "de-scaling" is applied before the image is decoded. Other systems used a "differencing" of the original image with the watermarked image to "de-scale." It is clear that de-scaling is inherently important to the survival of any image, audio or video watermark. What is not clear is that the differencing operation is acceptable from a security standpoint. Moreover, differencing that must be carried out by the watermarking "authority," instead of the user or creator of the image, causes the rights owner to lose control over the original unwatermarked content. Aside from utilizing the mask set within the encoding/decoding key/key pair, the original signal must be used. The original is necessary to perform detection and decoding, although with the attacks described above it is not possible to clearly establish ownership over the watermarked content.

In view of the foregoing, it can be appreciated that a substantial need exists for multiple transform utilization and applications for secure digital watermarking that solve the problems discussed above.

Summary of the Invention

The disadvantages of the art are alleviated to a great extent by multiple transform utilization and applications for secure digital watermarking. In one embodiment of the present invention, digital blocks in digital information to be protected are transformed into the frequency domain using a fast Fourier transform. A plurality of frequencies and associated amplitudes are identified for each of the transformed digital blocks and a subset of the identified amplitudes is selected for each of the digital blocks using a primary mask from a key. Message information is selected from a message using a transformation table generated with a convolution mask. The

chosen message information is encoded into each of the transformed digital blocks by altering the selected amplitudes based on the selected message information.

With these and other advantages and features of the invention that will become hereinafter apparent, the nature of the invention may be more clearly understood by reference to the following detailed description of the invention, the appended claims and to the several drawings attached herein.

Brief Description of the Drawings

FIG. 1 is a block flow diagram of a method for encoding digital information according to an embodiment of the present invention.

FIG. 2 is a block flow diagram of a method for descaling digital information according to an embodiment of the present invention.

FIG. 3 is a block flow diagram of a method for decoding digital information according to an embodiment of the present invention.

Detailed Description

In accordance with an embodiment of the present invention, multiple transforms are used with respect to secure digital watermarking. There are two approaches to watermarking using frequency-domain or spatial domain transformations: using small blocks or using the entire data-set. For time-based media, such as audio or video, it is only practical to work in small pieces, since the entire file can be many megabytes in size. For still images, however, the files are usually much smaller and can be transformed in a single operation. The two approaches each have their own strengths. Block-based methods are resistant to cropping. Cropping is the cutting out or removal of portions of the signal. Since the data is stored in small pieces, a crop merely means the loss of a few pieces. As long as enough blocks remain to decode a single, complete watermark, the crop does not remove the mark. Block-based systems, however, are susceptible to scaling. Scaling, such as affine scaling or "shrinking," leads to a loss of the high frequencies of the signal. If the block size is 32 samples and the data is scaled by 200%, the relevant data now covers 64 samples. However, the decoder still thinks that the data is in 32 samples, and therefore only uses half the space necessary to properly read the watermark. Whole-set approaches have the opposite behavior. They

are very good at surviving scaling, since they approach the data as a whole, and generally scale the data to a particular size before encoding. Even a small crop, however, can throw off the alignment of the transform and obscure the watermark.

With the present invention, and by incorporation of previously disclosed material, it is now possible to authenticate an image or song or video with the encoding key/key pair, eliminating false positive matches with cryptography and providing for the communication of a copyright through registration with third party authorities, instead of the original unwatermarked copy.

The present invention provides an obvious improvement over the prior art while improving on previous disclosures by offsetting coordinate values of the original signal onto the key, which are then subsequently used to perform decode or detection operations by the user or authorized "key-holder." This offsetting is necessary with content which may have a watermark "payload," the amount of data that may successfully be encoded, based on Shannon's noisy channel coding theorem, that prevents enough invisible "saturation" of the signal with watermark messages to afford the owner the ability to detect a single message. An example, it is entirely possible that some images may only have enough of a payload to carry a single 100 bit message, or 12 ASCII characters. In audio implementations tested by the present inventor, 1000 bits per second are inaudibly encoded in a 16 bit 44.1 kHz audio signal. Most electronically available images do not have enough data to afford similar "payload" rates. Thus the premise that simultaneous cropping and scaling survival is more difficult for images than a comparable commercially available audio or video track. The added security benefit is that the more limited randomizer of a watermarking system based on spread spectrum or frequency-only applications, the random value of the watermark data "hopping "over a limited signaling band, is that the key is also an independent source of ciphered or random data used to more effectively encode in a random manner. The key may actually have random values larger than the watermark message itself, measured in bits. The watermark decoder is assured that the image is in its original scale, and can decide whether it has been cropped based on its "de-scaled" dimensions.

The benefits of a system requiring keys for watermarking content and validating the distribution of said content is obvious. Different keys may be used to encode different information while secure one way hash functions, digital signatures, or even one-time pads may be incorporated in the key to secure the embedded signal and afford nonrepudiation and validation of the watermarked image and "its" key/key pair. Subsequently, these same keys may be used to later validate the embedded digital signature only, or fully decode the digital watermark message. Publishers can easily stipulate that content not only be digitally watermarked, but that distributors must check the validity of the watermarks by performing digital signature checks with keys that lack any other functionality.

Some discussion of secure digital watermarking has begun to appear. Leighton describes a means to prevent collusion attacks in digital watermarks in US Patent No. 5,664,018. Leighton, however, may not actually provide the security described. For example, in particularly instances where the watermarking technique is linear, the "insertion envelope" or "watermarking space" is well-defined and thus susceptible to attacks less sophisticated than collusion by unauthorized parties. Over encoding at the watermarking encoding level is but one simple attack in such linear implementations. Another consideration ignored by Leighton is that commercially-valuable content in many cases may already exist in a unwatermarked form somewhere, easily accessible to potential pirates, gutting the need for any type of collusive activity. Such examples as compact disc or digitally broadcast video abound. Digitally signing the embedded signal with preprocessing of watermark data is more likely to prevent successful collusion. Depending on the media to be watermarked, highly granular watermarking algorithms are far more likely to successfully encode at a level below anything observable given quantization artifacts, common in all digitally-sampled media, than expectations that a baseline watermark has any functionality.

Furthermore, a "baseline" watermark as disclosed is quite subjective. It is simply described elsewhere in the art as the "perceptually significant" regions of a signal: so making a watermarking function less linear or inverting the insertion of watermarks would seem to provide the same benefit without the additional work

required to create a "baseline" watermark. Indeed, watermarking algorithms should already be capable of defining a target insertion envelope or region without additional steps. Further, earlier disclosed applications by the present invention's inventor describe watermarking techniques that can be set to encode fewer bits than the available watermarking region's "bit-space" or encoding unrelated random noise in addition to watermark data to confuse possible collusive or other attempts at erasure. The region of "candidate bits" can be defined by any number of compression schemes or transformations, and the need to encode all of the bits is simply unnecessary. What is evident is that Leighton does not allow for initial prevention of attacks on an embedded watermark as the content is visibly or audibly unchanged. Moreover, encoding all of the bits may actually act as a security weakness to those who can replicate the regions with a knowledge of the encoding scheme. Again, security must also be offset outside of the actual watermark message to provide a truly robust and secure watermark implementation.

In contrast, the present invention may be implemented with a variety of cryptographic protocols to increase both confidence and security in the underlying system. A predetermined key is described as a set of masks. These masks may include primary, convolution and message delimiters but may extend into additional domains such as digital signatures of the message. In previous disclosures, the functionality of these masks is defined solely for mapping. Public and private keys may be used as key pairs to further increase the unlikeliness that a key may be compromised. Prior to encoding, the masks described above are generated by a cryptographically secure random generation process. A block cipher, such as DES, in combination with a sufficiently random seed value emulates a cryptographically secure random bit generator. These keys will be saved along with information matching them to the sample stream in question in a database for use in descrambling and subsequent detection or decode operation.

These same cryptographic protocols can be combined with embodiments of the present invention in administering streamed content that requires authorized keys to correctly display or play said streamed content in an unscrambled manner. As with

digital watermarking, symmetric or asymmetric public key pairs may be used in a variety of implementations. Additionally, the need for certification authorities to maintain authentic key-pairs becomes a consideration for greater security beyond symmetric key implementations, where transmission security is a concern.

The following describes a sample embodiment of a system that protects digital information according to the present invention. Referring now in detail to the drawings wherein like parts are designated by like reference numerals throughout, there is illustrated in FIG. 1 a block flow diagram of a method for encoding digital information according to an embodiment of the present invention. An image is processed by "blocks," each block being, for example, a 32 x 32 pixel region in a single color channel. At step 110, each block is transformed into the frequency domain using a spectral transform or a Fast Fourier Transform (FFT). The largest 32 amplitudes are identified and a subset of these 32 are selected using the primary mask from the key at steps 120 and 130. One message bit is then encoded into each block at steps 140 and 150. The bit is chosen from the message using a transformation table generated using the convolution mask. If the bit is true, the selected amplitudes are reduced by a user defined strength fraction. If the bit is false, the amplitudes are unchanged.

Each of the selected amplitudes and frequencies are stored in the key. After all of the image has been processed, a diagonal stripe of pixels is saved in the key. This stripe can, for example, start in the upper left corner and proceed at a 45 degree angle through the image. The original dimensions of the image are also stored in the key.

FIG. 2 is a block flow diagram of a method for descaling digital information according to an embodiment of the present invention. When an image is chosen to be decoded, it first is checked to determine if it has been cropped and/or scaled. If so, the image is scaled to the original dimensions at step 210. The resulting "stripe," or diagonal line of pixels, is fit against the stripe stored in the key at step 220. If the fit is better than the previous best fit, the scale is saved at steps 230 and 240. If desired, the image can be padded with, for example, a single row or column of zero pixels at step 260 and the process can be repeated to see if the fit improves.

If a perfect fit is found at step 250, the process concludes. If no perfect fit is found, the process continues up to a crop "radius" set by the user. For example, if the crop radius is 4 the image can be padded up to 4 rows and/or 4 columns. The best fit is chosen and the image is restored to its original dimension, with any cropped area replaced by zeroes.

Once the in formation has been descaled, it can be decoded according to an embodiment of the present invention shown in FIG. 3. Decoding is the inverse process of encoding. The decoded amplitudes are compared with the ones stored in the key in order to determine the position of the encoded bit at steps 310 and 320. The message is assembled using the reverse transformation table at step 330. At step 340, the message is then hashed and the hash is compared with the hash of the original message. The original hash had been stored in the key during encoding. If the hashes match, the message is declared valid and presented to the user at step 350.

Although various embodiments are specifically illustrated and described herein, it will be appreciated that modifications and variations of the present invention are covered by the above teachings and within the purview of the appended claims without departing from the spirit and intended scope of the invention. Moreover, similar operations have been applied to audio and video content for time-based manipulations of the signal as well as amplitude and pitch operations. The ability to descale or otherwise quickly determine differencing without use of the unwatermarked original is inherently important for secure digital watermarking. It is also necessary to ensure nonrepudiation and third part authentication as digitized content is exchanged over networks.

What is claimed is:

1. A method for encoding a message into digital information, the digital information including a plurality of digital blocks, comprising the steps of:

transforming each of the digital blocks into the frequency domain using a spectral transform;

identifying a plurality of frequencies and associated amplitudes for each of the transformed digital blocks;

selecting a subset of the identified amplitudes for each of the digital blocks using a primary mask from a key;

choosing message information from the message using a transformation table generated with a convolution mask; and

encoding the chosen message information into each of said transformed digital blocks by altering the selected amplitudes based on the chosen message information.

2. The method of claim 1 wherein the transforming step comprises:

transforming each of the digital blocks into the frequency domain using a fast Fourier transform.

3. The method of claim 2, wherein the digital information contains pixels in a plurality of color channels forming an image, and each of the digital blocks represents a pixel region in one of the color channels.

4. The method of claim 1, wherein the digital information contains audio information.

5. The method of claim 2, wherein said step of identifying comprises:

identifying a predetermined number of amplitudes having the largest values for each of the transformed digital blocks.

6. The method of claim 2, wherein the chosen message information is a message bit and wherein said step of encoding comprises the step of:

encoding the chosen message bit into each of said transformed digital blocks by reducing the selected amplitudes using a strength fraction if the message bit is true, and not reducing the selected amplitudes if the message bit is false.

7. The method of claim 6, wherein the strength fraction is user defined.

8. The method of claim 2, further comprising the step of storing each of the selected amplitudes and associated frequencies in the key.

9. The method of claim 2, further comprising the step of storing a reference subset of the digital information into the key.

10. The method of claim 2, wherein the digital information contains pixels forming an image, further comprising the steps of:

saving a reference subset of the pixels in the key; and

storing original dimensions of the image in the key.

11. The method of claim 1, wherein the digital information contains audio information, further comprising the steps of:

saving a reference subset of audio information in the key; and

storing original dimensions of the audio signal in the key.

12. The method of claim 10, wherein the reference subset of pixels form a line of pixels in the image.

13. The method of claim 11, wherein the reference subset of audio information includes an amplitude setting.

14. The method of claim 8, wherein the image is a rectangle and the reference subset of pixels form a diagonal of the rectangle.

15. The method of claim 2, further comprising the step of:

requiring a predetermined key to decode the encoded message information.

16. The method of claim 2, further comprising the step of:

requiring a public key pair to decode the encoded message information.

17. The method of claim 2, further comprising the steps of:

calculating an original hash value for the message; and

storing the original hash value in the key.

18. A method for descaling digital information using a key, comprising the steps of:

determining original dimensions of the digital information from the key;

scaling the digital information to the original dimensions;

obtaining a reference subset of information from the key; and

comparing the reference subset with corresponding information in the scaled digital information.

19. The method of claim 18 wherein the digital information being descaled is a digital image and the step of obtaining a reference subset of information from the key comprises obtaining a reference subset of pixels from the key.

20. The method of claim 18 wherein the digital information being descaled is audio digital information and the step of obtaining a reference subset of information from the key comprises obtaining a reference subset of audio information from the key.

21. The method of claim 19, wherein said step of comparing determines a first fit value based on the comparison, and wherein the method further comprises the steps of:

padding the scaled digital image with an area of pad pixels; and

re-comparing the reference subset of pixels with corresponding pixels in the padded image to determine a second fit value.

22. The method of claim 20, wherein the area of pad pixels is a row of single pixels.

23. The method of claim 20, wherein the area of pad pixels is a column of single pixels.

24. The method of claim 20, wherein said steps of padding and re-comparing are performed a plurality of times.

25. The method of claim 20, further comprising the step of choosing a best fit value among the determined fit values and restoring the digital image to the original size, including any pad pixels associated with the best fit value.

26. A method of extracting a message from encoded digital information using a predetermined key, comprising the steps of:

decoding the encoded digital information into digital information, including a plurality of digital blocks, using the predetermined key;

transforming each of the digital blocks into the frequency domain using a spectral transform;

identifying a plurality of frequencies and associated amplitudes for each of the transformed digital blocks;

selecting a subset of the identified amplitudes for each of the transformed digital blocks using a primary mask from the key;

comparing the selected amplitudes with original amplitudes stored in the predetermined key to determine the position of encoded message information; and

assembling the message using the encoded message information and a reverse transformation table.

27. The method of claim 26 wherein the step of transforming comprises:

transforming each of the digital blocks into the frequency domain using a fast Fourier transform.

28. The method of claim 27, further comprising the steps of:

calculating a hash value for the assembled message; and

comparing the calculated hash value with an original hash value in the predetermined key.

29. A method for descaling a digital signal using a key, comprising the steps of:

determining original dimensions of the digital signal from the key;

scaling the digital signal to the original dimensions;

obtaining a reference signal portion from the key; and

comparing the reference signal portion with a corresponding signal portion in the scaled signal.

30. A method for protecting a digital signal comprising the step of:

creating a predetermined key comprised of a transfer function-based mask set and offset coordinate values of the original digital signal; and

encoding the digital signal using the predetermined key.

31. The method of claim 30, wherein the digital signal represents a continuous analog waveform.

32. The method of claim 30, wherein the predetermined key comprises a plurality of mask sets.

33. The method of claim 30, wherein the mask set is ciphered by a key pair comprising a public key and a private key.

34. The method of claim 30, further comprising the step of:

using a digital watermarking technique to encode information that identifies ownership, use, or other information about the digital signal, into the digital signal.

35. The method of claim 30, wherein the digital signal represents a still image, audio or video.

36. The method of claim 30, further comprising the steps of:

selecting the mask set, including one or more masks having random or pseudo-random series of bits; and

validating the mask set at the start of the transfer function-based mask set.

37. The method of claim 36, wherein said step of validating comprises the step of:

comparing a hash value computed at the start of the transfer function-based mask set with a determined transfer function of the hash value.

38. The method of claim 36, wherein said step of validating comprises the step of:

comparing a digital signature at the start of the transfer function-based mask set with a determined transfer function of the digital signature.

39. The method of claim 36, further comprising the step of:

using a digital watermarking technique to embed information that identifies ownership, use, or other information about the digital signal, into the digital signal; and

wherein said step of validating is dependent on validation of the embedded information.

40. The method of claim 30, further comprising the step of:

computing a secure one way hash function of carrier signal data in the digital signal, wherein the hash function is insensitive to changes introduced into the carrier signal for the purpose of carrying the transfer function-based mask set.

41. A method for protecting a digital signal, comprising the steps of:

creating a predetermined key comprised of a transfer function-based mask set and offset coordinate values of the original digital signal;

authenticating the predetermined key containing the correct transfer function-based mask set during playback of the data; and

metering the playback of the data to monitor content to determine if the digital signal has been altered.

42. The method of claim 30, wherein the digital signal is a bit stream and further comprising the steps of:

generating a plurality of masks to be used for encoding, including a random primary mask, a random convolution mask and a random start of message delimiter;

generating a message bit stream to be encoded;

loading the message bit stream, a stega-cipher map truth table, the primary mask, the convolution mask and the start of message delimiter into memory;

initializing the state of a primary mask index, a convolution mask index, and a message bit index; and

setting a message size equal to the total number of bits in the message bit stream.

43. The method of claim 42 wherein the digital information has a plurality of windows, further comprising the steps of:

calculating over which windows in the sample stream the message will be encoded;

computing a secure one way hash function of the information in the calculated windows, the hash function generating hash values insensitive to changes in the samples induced by a stega-cipher; and

encoding the computed hash values in an encoded stream of data.

44. The method of claim 40, wherein said step of selecting comprises the steps of:

collecting a series of random bits derived from keyboard latency intervals in random typing;

processing the initial series of random bits through an MD5 algorithm;

using the results of the MD5 processing to seed a triple-DES encryption loop;

cycling through the triple-DES encryption loop, extracting the least significant bit of each result after each cycle; and

concatenating the triple-DES output bits into the random series of bits.

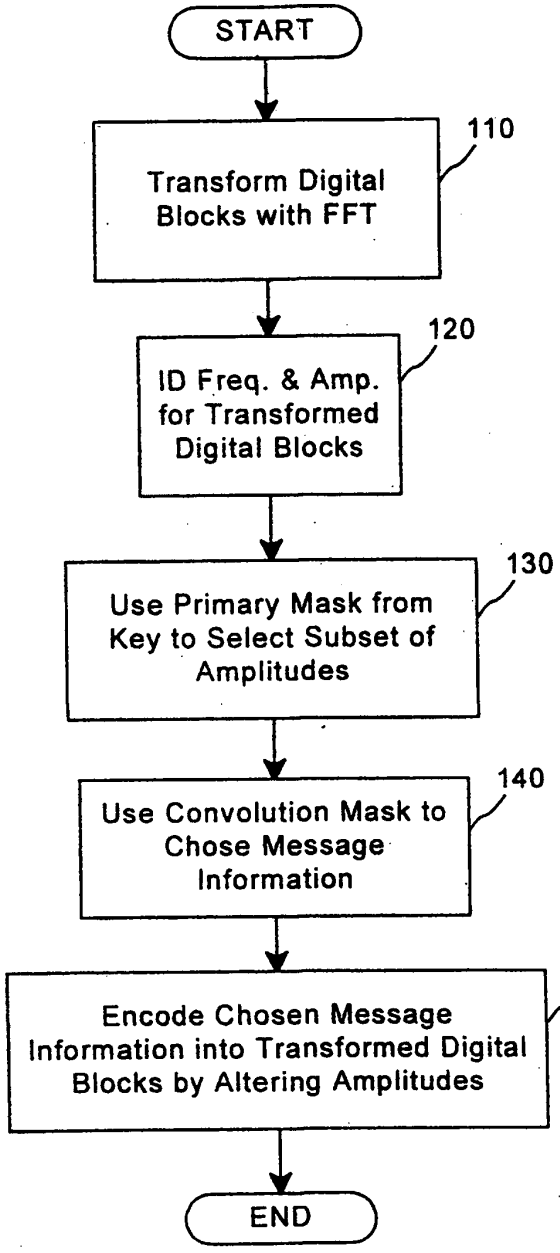

START
Transform Digital Blocks with FFT
110
ID Freq. & Amp. for Transformed Digital Blocks
120
Use Primary Mask from Key to Select Subset of Amplitudes
130
Use Convolution Mask to Chose Message Information
140
Encode Chosen Message Information into Transformed Digital Blocks by Altering Amplitudes
150
END

FIG. 1

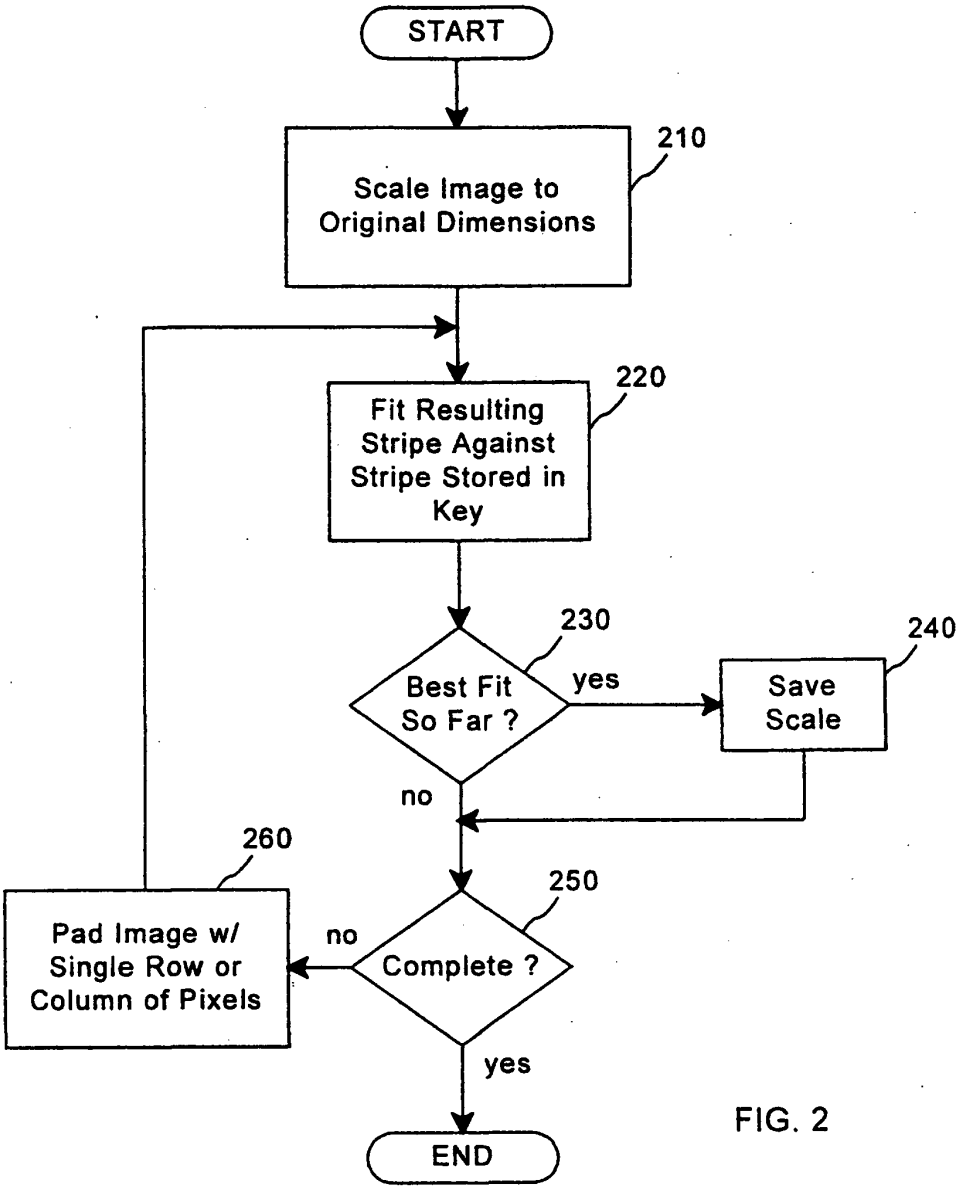

START
Scale Image to Original Dimensions
210
Fit Resulting Stripe Against Stripe Stored in Key
220
Best Fit So Far ?
230
yes
Save Scale
240
no
Complete ?
250
no
Pad Image w/ Single Row or Column of Pixels
260
yes
END

FIG. 2

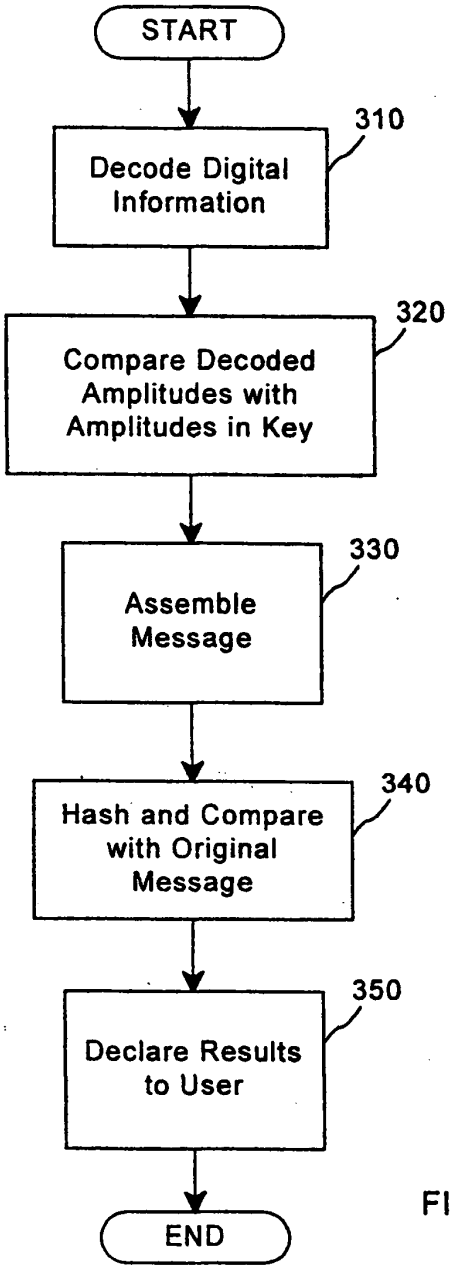

START
310
Decode Digital Information
320
Compare Decoded Amplitudes with Amplitudes in Key
330
Assemble Message
340
Hash and Compare with Original Message
350
Declare Results to User
END

FIG. 3

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/US 99/07262

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04N H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 613 004 A (MOSKOWITZ SCOTT A ET AL) 18 March 1997 (1997-03-18) abstract column 6, line 30 - column 9, line 49 column 16, line 8 - line 64	1,2, 15-17, 26-28, 30-38,42
A	DELAIGLE J -F ET AL: "DIGITAL WATERMARKING" PROCEEDINGS OF THE SPIE, vol. 2659, 1 February 1996 (1996-02-01), pages 99-110, XP000604065 the whole document	1,5,6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 July 1999	21/07/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Hubeau, R

2

Form PCT/ISA/210 (second sheet) (July 1992)

DISH-Blue Spike-842
Exhibit 1004, Page 0796

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/US 99/07262

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	SCHNEIDER M ET AL: "ROBUST CONTENT BASED DIGITAL SIGNATURE FOR IMAGE AUTHENTICATION" PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON IMAGE PROCESSING (IC, LAUSANNE, SEPT. 16 - 19, 1996, vol. 3, 16 September 1996 (1996-09-16), pages 227-230, XP002090178 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERSISBN: 0-7803-3259-8 the whole document	1,17,18, 26-28
A	COX I J ET AL: "SECURE SPREAD SPECTRUM WATERMARKING FOR MULTIMEDIA" IEEE TRANSACTIONS ON IMAGE PROCESSING, vol. 6, no. 12, 1 December 1997 (1997-12-01), pages 1673-1686, XP000724633 ISSN: 1057-7149 the whole document	1-3,5,6, 26,27
A,P	PING WAH WONG: "A Public Key Watermark for Image Verification and Authentication" IEEE INTERNATIONAL CONFERENCE ON IMAGE PROCESSING, vol. 1, 4 - 7 October 1998, pages 455-459, XP002108799 Los Alamitos, CA, USA the whole document	1-4

2

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

DISH-Blue Spike-842
Exhibit 1004, Page 0797

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/US 99/07262

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5613004 A	18-03-1997	EP 0872073 A	21-10-1998
		WO 9642151 A	27-12-1996
		US 5687236 A	11-11-1997

Form PCT/ISA/210 (patent family annex) (July 1992)

Your Ref.: 066358.0102JP

Our Ref.: S-1181-1/002365

JAPANESE TRANSLATION OF PCT APPLICATION

International Patent Application No.

PCT/US99/07262

Date of International Application:

April 2, 1999

TITLE OF THE INVENTION

Multiple Transform Utilization and Applications
for Secure Digital Watermarking

INVENTOR

SCOTT A. MOSKOWITZ

APPLICANT

SCOTT A. MOSKOWITZ

YUASA AND HARA

受領書

平成１２年１０月　２日
特　許　庁　長　官

識別番号　　１００００８９７０５
氏名（名称）　　社本　一夫　　殿
提出日　　平成１２年１０月　２日

以下の書類を受領しました。

項番	書類名	整理番号	受付番号	出願番号通知（事件の表示）
1	国内書面	002365	50001273422	PCT/US99/ 7262

以　上

【書類名】　国内書面

【整理番号】　002365

【提出日】　平成12年10月 2日

【あて先】　特許庁長官殿

【出願の表示】

【国際出願番号】　PCT/US99/07262

【出願の区分】　特許

【発明者】

【住所又は居所】　アメリカ合衆国フロリダ州３３１６０，マイアミ，コリンズ・アベニュー　１６７１１，ナンバー　２５０５

【氏名】　モスコウィッツ，スコット・エイ

【特許出願人】

【住所又は居所】　アメリカ合衆国フロリダ州３３１６０，マイアミ，コリンズ・アベニュー　１６７１１，ナンバー　２５０５

【氏名又は名称】　スコット・エイ・モスコウィッツ

【代理人】

【識別番号】　100089705

【住所又は居所】　東京都千代田区大手町二丁目２番１号　新大手町ビル２０６区　ユアサハラ法律特許事務所

【弁理士】

【氏名又は名称】　社本　一夫

【電話番号】　03-3270-6641

【選任した代理人】

【識別番号】　100071124

【弁理士】

【氏名又は名称】　今井　庄亮

【選任した代理人】

【識別番号】　100076691

【弁理士】

Proof - 2000/10/02

【氏名又は名称】　増井　忠弐

【選任した代理人】

【識別番号】　100075270

【弁理士】

【氏名又は名称】　小林　泰

【選任した代理人】

【識別番号】　100096013

【弁理士】

【氏名又は名称】　富田　博行

【選任した代理人】

【識別番号】　100087424

【弁理士】

【氏名又は名称】　大塚　就彦

【手数料の表示】

【予納台帳番号】　051806

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書の翻訳文　1

【物件名】　図面の翻訳文　1

【物件名】　要約書の翻訳文　1

【プルーフの要否】　要

DISH-Blue Spike-842
Exhibit 1004, Page 0802

【書類名】　明細書

【発明の名称】　安全なデジタル透かしのための複数の変換の利用及び適用

【特許請求の範囲】

【請求項１】　メッセージをデジタル情報に符号化する方法であって、前記デジタル情報は複数のデジタル・ブロックを含んでいる、方法において、

前記デジタル・ブロックのそれぞれをスペクトル変換を用いて周波数領域に変換するステップと、

前記変換されたデジタル・ブロックのそれぞれに対して、複数の周波数と関連する振幅とを識別するステップと、

前記デジタル・ブロックのそれぞれに対して、鍵からの基本マスクを用いて、前記識別された振幅の部分集合を選択するステップと、

畳み込みマスクを用いて発生された変換テーブルを用いて、前記メッセージからメッセージ情報を選ぶステップと、

前記選ばれたメッセージ情報に基づいて前記選択された振幅を変更することによって、前記選ばれたメッセージ情報を前記変換されたデジタル・ブロックのそれぞれに符号化するステップと、

を含むことを特徴とする方法。

【請求項２】　請求項１記載の方法において、前記変換するステップは、

高速フーリエ変換を用いて、前記デジタル・ブロックのそれぞれを前記周波数領域に変換するステップを含むことを特徴とする方法。

【請求項３】　請求項２記載の方法において、前記デジタル情報は、画像を形成する複数のカラー・チャネルにおけるピクセルを含み、前記デジタル・ブロックのそれぞれは、前記カラー・チャネルの１つにおけるピクセル領域を表すことを特徴とする方法。

【請求項４】　請求項１記載の方法において、前記デジタル情報はオーディオ情報を含むことを特徴とする方法。

【請求項５】　請求項２記載の方法において、前記識別するステップは、

前記変換されたデジタル・ブロックのそれぞれに対して最大の値を有する所定の数の振幅を識別するステップを含むことを特徴とする方法。

DISH-Blue Spike-842
Exhibit 1004, Page 0803

【請求項６】　請求項２記載の方法において、前記選ばれたメッセージ情報はメッセージ・ビットであり、前記符号化するステップは、

前記メッセージ・ビットが真である場合には強度率を用いて前記選択された振幅を減少させ、前記メッセージ・ビットが偽である場合には前記選択された振幅を減少させないことによって、前記選ばれたメッセージ・ビットを前記変換されたデジタル・ブロックのそれぞれに符号化するステップを含むことを特徴とする方法。

【請求項７】　請求項６記載の方法において、前記強度率はユーザによって定義されることを特徴とする方法。

【請求項８】　請求項２記載の方法において、前記選択された振幅と関連する周波数とのそれぞれを前記鍵に記憶するステップを更に含むことを特徴とする方法。

【請求項９】　請求項２記載の方法において、前記デジタル情報の基準部分集合を前記鍵に記憶するステップを更に含むことを特徴とする方法。

【請求項１０】　請求項２記載の方法において、前記デジタル情報は画像を形成するピクセルを含んでおり、更に、

前記ピクセルの基準部分集合を前記鍵にセーブするステップと、

前記画像の元の寸法を前記鍵に記憶するステップと、

を含むことを特徴とする方法。

【請求項１１】　請求項１記載の方法において、前記デジタル情報はオーディオ情報を含んでおり、更に、

オーディオ情報の基準部分集合を前記鍵にセーブするステップと、

前記オーディオ情報の元の寸法を前記鍵に記憶するステップと、

を含むことを特徴とする方法。

【請求項１２】　請求項１０記載の方法において、ピクセルの前記基準部分集合は前記画像におけるピクセルの線を形成することを特徴とする方法。

【請求項１３】　請求項１１記載の方法において、オーディオ情報の前記基準部分集合は振幅設定を含むことを特徴とする方法。

【請求項１４】　請求項８記載の方法において、前記画像は矩形であり、ピ

DISH-Blue Spike-842
Exhibit 1004, Page 0804

クセルの前記基準部分集合は前記矩形の対角線を形成することを特徴とする方法。

【請求項１５】　請求項２記載の方法において、

所定の鍵が前記符号化されたメッセージ情報を復号化することを要求するステップを更に含むことを特徴とする方法。

【請求項１６】　請求項２記載の方法において、

公開鍵の対が前記符号化されたメッセージ情報を復号化することを要求するステップを更に含むことを特徴とする方法。

【請求項１７】　請求項２記載の方法において、

前記メッセージに対する元のハッシュ値を計算するステップと、

前記元のハッシュ値を前記鍵に記憶するステップと、

を更に含むことを特徴とする方法。

【請求項１８】　鍵を用いてでる情報をデスケーリングする方法であって、

前記デジタル情報の元の寸法を前記鍵から決定するステップと、

前記デジタル情報を前記元の寸法にスケーリングするステップと、

情報の基準部分集合を前記鍵から取得するステップと、

前記基準部分集合を前記スケーリングされたデジタル情報における対応する情報と比較するステップと、

を含むことを特徴とする方法。

【請求項１９】　請求項１８記載の方法において、デスケーリングされる前記デジタル情報はデジタル画像であり、前記鍵から情報の基準部分集合を取得するステップは前記鍵からピクセルの基準部分集合を取得するステップを含むことを特徴とする方法。

【請求項２０】　請求項１８記載の方法において、デスケーリングされる前記デジタル情報はオーディオ・デジタル情報であり、前記鍵から情報の基準部分集合を取得するステップは前記鍵からオーディオ情報の基準部分集合を取得するステップを含むことを特徴とする方法。

【請求項２１】　請求項１９記載の方法において、前記比較するステップは前記比較に基づいて第１の適合する値を決定し、この方法は、更に、

DISH-Blue Spike-842
Exhibit 1004, Page 0805

前記スケーリングされたデジタル画像をパッド・ピクセルのエリアを用いてパディングするステップと、

ピクセルの前記基準部分集合を前記パディングされた画像における対応するピクセルと再度比較して第２の適合する値を決定するステップと、

を含むことを特徴とする方法。

【請求項２２】　請求項２０記載の方法において、パッド・ピクセルの前記エリアは、単一のピクセルのローであることを特徴とする方法。

【請求項２３】　請求項２０記載の方法において、パッド・ピクセルの前記エリアは、単一のピクセルのコラムであることを特徴とする方法。

【請求項２４】　請求項２０記載の方法において、前記パディング及び再度比較するステップは複数回実行されることを特徴とする方法。

【請求項２５】　請求項２０記載の方法において、前記決定された適合する値の中で最良の適合する値を選び、前記デジタル画像を元のサイズに回復し、前記最良の適合する値と関連する任意のパッド・ピクセルを含むステップを更に含むことを特徴とする方法。

【請求項２６】　所定の鍵を用いて符号化されたデジタル情報からメッセージを抽出する方法であって、

前記所定の鍵を用いて、前記符号化されたデジタル情報を複数のデジタル・ブロックを含むデジタル情報に復号化するステップと、

スペクトル変換を用いて、前記デジタル・ブロックのそれぞれを周波数領域に変換するステップと、

前記変換されたデジタル・ブロックのそれぞれに対して、複数の周波数と関連する振幅とを識別するステップと、

前記鍵からの基本マスクを用いて、前記変換されたデジタル・ブロックのそれぞれに対して、前記識別された振幅の部分集合を選択するステップと、

前記選択された振幅と前記所定の鍵に記憶された元の振幅とを比較し、符号化されたメッセージ情報の位置を決定するステップと、

前記符号化されたメッセージ情報と逆変換テーブルとを用いて、前記メッセージをアセンブルするステップと、

DISH-Blue Spike-842
Exhibit 1004, Page 0806

を含むことを特徴とする方法。

【請求項２７】　請求項２６記載の方法において、前記変換するステップは

高速フーリエ変換を用いて、前記デジタル・ブロックのそれぞれを周波数領域に変換するステップを含むことを特徴とする方法。

【請求項２８】　請求項２７記載の方法において、

前記アセンブルされたメッセージに対するハッシュ値を計算するステップと、

前記計算されたハッシュ値を前記所定の鍵の中の元のハッシュ値と比較するステップと、

を更に含むことを特徴とする方法。

【請求項２９】　鍵を用いてデジタル信号をデスケーリングする方法であって、

前記鍵から前記デジタル信号の元の寸法を決定するステップと、

前記デジタル信号を前記元の寸法にスケーリングするステップと、

前記鍵から基準信号部分を取得するステップと、

前記基準信号部分を前記スケーリングされた信号における対応する信号部分と比較するステップと、

を含むことを特徴とする方法。

【請求項３０】　デジタル信号を保護する方法であって、

伝達関数ベースのマスク・セットと元のデジタル信号のオフセット座標値とから構成される所定の鍵を作成するステップと、

前記デジタル信号を前記所定の鍵を用いて符号化するステップと、

を含むことを特徴とする方法。

【請求項３１】　請求項３０記載の方法において、前記デジタル信号は連続的なアナログ波形を表すことを特徴とする方法。

【請求項３２】　請求項３０記載の方法において、前記所定の鍵は複数のマスク・セットを含むことを特徴とする方法。

【請求項３３】　請求項３０記載の方法において、前記マスク・セットは、公開鍵と秘密鍵とを含む鍵の対によって暗号化されることを特徴とする方法。

DISH-Blue Spike-842
Exhibit 1004, Page 0807

【請求項３４】　請求項３０記載の方法において、

デジタル透かし技術を用いて前記デジタル信号に関する権利者、使用又はそれ以外の情報を識別する情報を前記デジタル信号の中に符号化するステップを更に含むことを特徴とする方法。

【請求項３５】　請求項３０記載の方法において、前記デジタル信号は静止画像、オーディオ又はビデオを表すことを特徴とする方法。

【請求項３６】　請求項３０記載の方法において、

ランダム又は疑似ランダムな一連のビットを有する１つ又は複数のマスクを含むマスク・セットを選択するステップと、

前記マスク・セットを、前記伝達関数ベースのマスク・セットの開始において有効化するステップと、

を更に含むことを特徴とする方法。

【請求項３７】　請求項３６記載の方法において、前記有効化するステップは、

前記伝達関数ベースのマスク・セットの開始において計算されたハッシュ値を前記ハッシュ値の所定の伝達関数と比較するステップを含むことを特徴とする方法。

【請求項３８】　請求項３６記載の方法において、前記有効化するステップは、

前記伝達関数ベースのマスク・セットの開始におけるデジタル署名を前記デジタル署名の所定の伝達関数と比較するステップを含むことを特徴とする方法。

【請求項３９】　請求項３６記載の方法において、

デジタル透かし技術を用いて前記デジタル信号に関する権利者、使用又はそれ以外の情報を識別する情報を前記デジタル信号の中に埋め込むステップを更に含み、

前記有効化するステップは、前記埋め込まれた情報の有効化に依存することを特徴とする方法。

【請求項４０】　請求項３０記載の方法において、

前記デジタル信号においてキャリア信号データの安全な一方向ハッシュ関数を

DISH-Blue Spike-842
Exhibit 1004, Page 0808

計算するステップを更に含んでおり、前記ハッシュ関数は、前記伝達関数ベースのマスク・セットを搬送する目的で前記キャリア信号の中に導入された変化を感知しないことを特徴とする方法。

【請求項４１】　デジタル信号を保護する方法であって、

伝達関数ベースのマスク・セットと元のデジタル信号のオフセット座標値とで構成された所定の鍵を作成するステップと、

正しい伝達関数ベースのマスク・セットを含む前記所定の鍵を前記データの再生の間に認証するステップと、

前記データの再生を測定してコンテンツをモニタし、前記デジタル信号が変更されたかどうかを判断するステップと、

を含むことを特徴とする方法。

【請求項４２】　請求項３０記載の方法において、前記デジタル信号はビット・ストリームであり、この方法は、更に、

符号化のために用いられ、ランダム基本マスクと、ランダム畳み込みマスクと、メッセージ・デリミタのランダム開始とを含む複数のマスクを発生するステップと、

符号化されるメッセージ・ビット・ストリームを発生するステップと、

前記メッセージ・ビット・ストリームと、ステガ・サイファ・マップ真理テーブルと、前記基本マスクと、前記畳み込みマスクと、メッセージ・デリミタの前記開始とをメモリにロードするステップと、

基本マスク・インデクスと、畳み込みマスク・インデクスと、メッセージ・ビット・インデクスとの状態を初期化するステップと、

前記メッセージ・ビット・ストリームにおける全ビット数と等しくなるようにメッセージ・サイズを設定するステップと、

を含むことを特徴とする方法。

【請求項４３】　請求項４２記載の方法において、前記デジタル情報は複数のウィンドウを有しており、この方法は、更に、

サンプル・ストリームにおけるどのウィンドウの上で前記メッセージが符号化されるかを計算するステップと、

DISH-Blue Spike-842
Exhibit 1004, Page 0809

前記計算されたウィンドウにおける情報の安全な一方向ハッシュ関数を計算するステップであって、前記ハッシュ関数はステガ・サイファによって導かれるサンプルにおける変化を感知しないハッシュ値を発生する、ステップと、

データの符号化されたストリームにおける前記計算されたハッシュ値を符号化するステップと、

を含むことを特徴とする方法。

【請求項４４】　請求項４０記載の方法において、前記選択するステップは、

ランダム・タイピングにおけるキーボード・レイテンシ期間から導かれた一連のランダム・ビットを収集するステップと、

初期の一連のランダム・ビットをＭＤ５アルゴリズムを介して処理するステップと、

前記ＭＤ処理の結果を用いて、トリプルＤＥＳ暗号化ループを供給し、各サイクルの後のそれぞれの結果の最下位ビットを抽出するステップと、

前記トリプルＤＥＳ出力ビットをランダムな一連のビットの中に連結するステップと、

を含むことを特徴とする方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタル情報の保護に関する。更に詳しくは、本発明は、安全なデジタル透かしのための複数の変換の利用及び適用に関する。

【０００２】

【関連出願への相互参照】

本発明は、１９９６年1月１７日に出願された米国特許出願第０８／５８７，９４３号"Method for Stega-Cipher Protection of Computer Code"に基づいて優先権を主張している。この米国特許出願の開示のすべてを、本出願において援用する。

【０００３】

DISH-Blue Spike-842
Exhibit 1004, Page 0810

【従来の技術】

商業的に価値のある情報が「デジタル」形式で制作され記憶されることが増加している。例えば、音楽、写真及び画像のすべてが、１及び０などの一連の数として記憶され伝送されることが可能である。デジタル技術によると、元の情報を非常に正確に再生することができる。しかし、不運なことに、デジタル技術によると、その持ち主の許可を得ることなく、情報を容易にコピーすることもできるのである。

【０００４】

デジタル透かし（電子透かし、digital watermark）は、デジタル化されたマルチメディア・コンテンツの制作者（creators）と出版業者（publishers）とがコンテンツのローカルで安全な識別及び認証を要求する収束点に存在している。侵害行為（piracy）は貴重なデジタル情報の流通を損なう方向に作用するから、そのような作品のコピーや二次的（derivative）なコピーに対する責任を確立することが重要である。デジタル透かしシステムの目的は、基礎となるコンテンツ信号の中に、ほとんど又は全く痕跡を残すことなく、そして知覚可能であることが標準となるように、与えられた１つ又は複数の情報信号を挿入することである。その際に、基礎となる信号における符号化レベルと位置感度（location sensitivity）とを最大化することにより、この透かしを除去しようと試みるとコンテンツ信号に強制的に損傷が生じるようになっている。「マスタ」、ステレオ、ＮＴＳＣ（National Television Standards Committee）ビデオ、オーディオ・テープ又はコンパクト・ディスクであるかどうかなど、マルチメディア・コンテンツの様々な形態を考慮すると、質に関する寛容度は、個人ごとに変動し、そのコンテンツの基礎となる商業的及び美的な価値に影響を与える。従って、著作権、所有権（ownership right）、購入者情報又はこれらの何らかの組合せや関連データをそのコンテンツの中に結合させ、それにより、それが商業的であってもそれ以外の態様であっても認証されていない流通がそれ以後なされる場合には、そのコンテンツが損傷を受け、従って、その価値が低下するようにすることが望ましい。デジタル透かしは、このような関心の多くに向けられたものであり、この技術分野における研究は、これまでに、極めて堅固で安全な実現に対する豊かな

DISH-Blue Spike-842
Exhibit 1004, Page 0811

基礎を提供してきている。

【０００５】

特に関心が向けられているのは、コンテンツのデジタル化された「作品」（piece）の価値とそのコンテンツに値する「保護」を提供するためのコストとのバランスである。現実の世界における経済行動と並行するように、商業銀行の安全性（セキュリティ）を知覚できるからといって、銀行預金をするのに要する費用及び時間のために、人々は直ちに現金を銀行に預金するということにはならない。ほとんどの個人にとっては、１００米ドルをもっているからといって、それを財布にしまっておく以上の保護が必要とされることはない。また、ワールド・ワイド・ウェブ（WWW）すなわちウェブが存在するからといって、オーディオや、静止画像等の媒体のようなデジタル化することができる媒体に対して価値が創造されたことを意味しない。ウェブは、単に、情報交換のための媒体であり、コンテンツの商業的な価値を決定することはない。しかし、媒体を交換するためにウェブを用いることにより、その価値を決定するのに役立つ情報が提供されるため、デジタル化されたコンテンツに対する責任が要求される。デジタル透かしは、このプロセスにおけるツール（道具）であって、著作権などの法的権利に関するより公的な課題を確立するそれ以外の機構に代わるものではないことに注意してほしい。例えば、デジタル透かしは、コンテンツの価値を判断する際の「履歴平均」（historical average）アプローチに代わるものではない。これは、コンテンツの知覚された価値だけに基づいて購入をしようとする個人の市場（マーケット）のことである。例えば、インターネット又はそれ以外の任意の電子的な交換手段を介して写真が流通しても、その写真の基礎的な価値が増加することは必ずしもない。しかし、そのような形式の「放送」によってより大きな観客に到達する機会が生じることは、「潜在的」により大きな市場に基づく価値を生じさせる望ましい機構でありうる。この決定は、当該権利者のみが唯一なすことができる。

【０００６】

実際、多くの場合に、コンテンツの時間的な価値に依存して、アクセスが適切に制御されていない場合には、価値が現実に低下することがありうる。月刊誌と

DISH-Blue Spike-842
Exhibit 1004, Page 0812

して販売されている雑誌の場合には、その雑誌が販売されている期間を超えて、その雑誌に掲載されている写真の価値を評価することは困難である。コンパクト・ディスクの価値に関しても、同様な時間に関する変動要素があるし、デジタル化されたオーディオ信号のパッケージングとパッケージを伴わない電子的な交換とのような有形的な変動要素もある。インターネットは、単に、消費者により迅速に到達する手段を提供するだけであって、それ以外の「市場に基づく」価値に取って代わるものではない。デジタル透かしは、適切に実現されるのであれば、権利者の決定に関する必要な層を追加することになり、デジタル透かしが「証明可能な程度に安全」（provably secure）であるときには、価値を決定し評価する際に大いに役立つ。本発明は、デジタル透かし技術の改良であり、現実世界における商品の真偽判定方法と類似する態様で、デジタル化されたコンテンツを「改ざん不能」（tamper-proof）にする手段を与える。

【０００７】

デジタル透かし技術における一般的な弱点は、透かしを実現する方法に関する。ほとんどのアプローチにおいて、保護されるべき作品の制作者ではなくデジタル透かしを実現する者に、検出及び復号制御に関して依存している。様々な透かし技術が有するこの基本的側面のために、第三者がそのようなデジタル透かしの実現を成功裏に利用する際には、この技術の改良に対する適切な経済的インセンティブが失われる。特定の形式の利用がいったんなされると、それ以後の透かしの検出が曖昧になる。そして、それ以後の時点において同じ透かしプロセスを用いた符号化を成功であると見なすことになる。

【０００８】

安全なデジタル透かしのいくつかの実現例がこの基本的な制御の課題に取り組んでおり、「キー・ベース」（key-based）のアプローチの基礎を形成している。これらは、以下の米国特許及び出願中の米国特許出願がカバーしている。すなわち、"Steganographic Method and Device"と題する米国特許第５，６１３，００４号及びそれから生じた米国特許出願第０８／７７５，２１６号；"Human Assisted Random Key Generation and Application for Digital Watermark System"と題する米国特許出願第０８／５８７，９４４号；"Method for Stega-Cipher

DISH-Blue Spike-842
Exhibit 1004, Page 0813

Protection of Computer Code"と題する米国特許出願第０８／５８７，９４３号；"Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data"と題する米国特許出願第０８／６７７，４３５号；及び"Z-Transform Implementation of Digital Watermarks"と題する米国特許出願第０８／７７２，２２２号である。これらの米国特許及び米国特許出願における開示内容は本出願において援用する。公開鍵暗号システムは、米国特許第４，２００，７７０号、第４，２１８，５８２号、第４，４０５，８２９号及び第４，４２４，４１４号に記載されている。これらの米国特許における開示内容は、本出願において援用する。

【０００９】

これらのデジタル透かしによるセキュリティ方法を改良することによって、複数の変換を用い、信号特性を操作し、必要な関係を符号化及び復号化動作に用いられるマスク・セットすなわち「鍵」に適用することが、これらの方法の最適化された組合せとして考察される。透かしの符号化は、符号化アルゴリズムにおいて用いられる変換に関して最終的にほんの僅かに異なるが、公開された分散型のアーキテクチャというより大きな課題によって、抹消しようとする試みに打ち勝つ、より堅固なアプローチが要求され、更には、透かしの検出を不可能にする手段が要求される。これらの「攻撃」は、計算論的に比較すると、正反対な態様（diametrically）で関連している。例えば、クロッピング（cropping）とスケーリング（scaling）とは、信号処理の向きが異なり、結果的には特定の透かしアプローチを脆弱化する可能性があるが、すべての透かしアプローチについてはそういうことはない。

【００１０】

ブロック・ベース又は全体のデータ・セット変換のいずれかを用いて符号化を行う現時点で利用できるアプローチは、必ず、空間領域又は周波数領域のどちらか一方においてデータを符号化するが、両方の領域においてそうすることは決してない。同時的なクロッピング及びスケーリングは、空間及び周波数領域に影響し、それによって、使用可能な透かしシステムのほとんどを曖昧にする。複数の操作を生き延びる能力は、透かしの入れられた媒体のセキュリティを確実にしよ

DISH-Blue Spike-842
Exhibit 1004, Page 0814

うとしている者にとっては明確な利点である。本発明は、鍵ベースのアプローチを用いて既存の透かしを改良することを目指している。その際に、それ以後に透かしが入れられるコンテンツを権利者やコンテンツ制作者がより広く制御できるようにする。

【００１１】

現時点で利用可能な多くの静止画透かしアプリケーションは、鍵ベースの実現例とは根本的に異なっている。これらの製品としては、デジマーク（Digimarc）社やシグナム（Signum）社による製品があるが、これらの製品は、復号化動作に関してはオリジナルの画像との比較に完全に依存している透かしメッセージを符号化することによって、堅固（robust）な透かしを提供することを目指している。ブロックごとに実行される離散コサイン変換である変換のそれ以後の結果は、デジタル的に符号が付される。埋め込まれた透かしは、画像の知覚的な質とは全く関係がなく、従って、一般的に利用可能なデコーダの逆方向の適用が、攻撃の非常によい最初のラインとなる。同様にして、符号化プロセスは、第三者によって適用されることもありうる。これは、いくつかの堅固性のテストにおいて示されているように、或るプロセスを用いて他のプロセスを用いて透かしが入れられた画像の結果を符号化するものである。透かしを放棄しないこと（nonrepudiation）はできない。その理由は、デジマーク社とシグナム社とが、画像の権利に関するすべての登録の機関として機能しているからである。

【００１２】

攻撃の別のラインとして、エラーのない検出が困難又は不可能であるように追加されている高周波ノイズの一部を除去するローパス・フィルタがある。最終的には、単純なＪＰＥＧ変換の多くのテストがこのような透かしは生き延びることができないことを示す。その理由は、ＪＰＥＧが、透かしを入れるプロセスによって用いられる符号化変換と同じ変換に基づいているからである。これ以外の注意すべき実現例としては、例えば、ＮＥＣの研究者たちによって開発されたシグナファイ（Signafy）によるものなどがあるが、画像の全体の変換を実行することによって、透かしメッセージを符号化しているようである。このプロセスの目的は、画像の「候補となる」透かしビット又は領域をより一貫性をもって識別し

DISH-Blue Spike-842
Exhibit 1004, Page 0815

て、信号の知覚的に著しい領域において符号化を行うことである。そうであっても、シグナファイは、復号化を達成するのに、オリジナルの透かしの入れられていない画像に依存する。

【００１３】

これらの方法は、すべてが、透かしを比較的エラーのない態様で検出することを確実にするために、オリジナルの透かしの入れられていない画像に依然として依存している。ステガノグラフィック（steganographic）な方法では、復号化動作のためにその媒体のオリジナルな透かしの入れられていないコピーを用いることなく透かしのセキュリティを提供すると共に、ユーザに暗号化された鍵を用いて暗号的なセキュリティをも提供することが目的とされる。すなわち、符号化動作と復号化動作とのために、同じ鍵が用いられる。それぞれのユーザが非対称的な符号化及び復号化動作を実行するための公開／秘密鍵対を有するような公開鍵対を用いることもできる。公開鍵暗号に関する議論と暗号化に関する利点とは、広く文書化がなされている。公開鍵インフラストラクチャの利用可能性が増加していることは、証明可能なセキュリティを認識しうるということを示している。透かしの実現化がこのように鍵ベースであることにより、セキュリティについては鍵に依存することが可能であり、それによって、透かしメッセージと透かしの入れられたコンテンツとのセキュリティ及び認証に対する多層化（layered）されたアプローチが得られる。

【００１４】

これ以外の実現例が生き延びること（survivability）に対するに対する攻撃も容易に利用可能であることが知られている。透かしメッセージに対する興味深いネットワーク・ベースの攻撃も知られているが、これは、中央の登録サーバを騙して、画像が登録されている権利者とは別の誰かが権利を有していると想定させるものである。また、これによると、集中的な透かし技術は十分に堅固なものではなく、マルチメディア作品のデジタル化されたコピーの権利者に関する適切な確認を行うことはできないという懸念が現実のものとなる。

【００１５】

【発明が解決しようとする課題】

DISH-Blue Spike-842
Exhibit 1004, Page 0816

複数の変換を実行することに関する計算論的な要求は、静止画やオーディオなどのある種の媒体にとっては禁止されないのであるから、本発明は、復号化を実行するのにオリジナルの透かしの入れられていないコピーを必要とすることなしに、媒体に確実に透かしを入れる手段を提供することを目的とする。これらの変換は、コンテンツの観察者又は権利者に対して単純には明らかでない態様で実行することができる。しかし、これらの観察者や権利者は、透かしが依然として検出可能であると考えることができる。更に、特定の媒体のタイプが一般的に圧縮されている場合（ＪＰＥＧ、ＭＰＥＧなど）には、複数の変換を用いて、透かしを入れるプロセスに先立ってマスク・セットを適切に設定し、透かしの入れられた従って知覚された「安全」なコピーを未知の第三者に解放する前に、ユーザに生き残り可能性について警告することができる。本発明の結果は、透かしへのより現実的なアプローチであって、鍵の証明可能なセキュリティだけでなく媒体のタイプも考慮している。従って、電子商取引のためのより信頼性の高いモデルも可能である。

【００１６】

透かしを挿入するために最適化された「封筒」を作成し、デジタル的にサンプリングされたコンテンツに対する確実な責任を確立することにより、大きな透かしセキュリティの基礎が得られるが、これは、本発明の補助的な目的である。発生される所定の又はランダムな鍵は、隠された情報信号にアクセスするために不可欠な地図であるだけではなく、オリジナルな信号の部分集合であって、それにより、オリジナルな信号との比較が不要になる。これによって、デジタル透かしの全体的なセキュリティが向上する。

【００１７】

同時的なクロッピング及びスケーリングが生き延びること（生き残ること、survival）は、画像及びオーディオ透かしに関しては、困難である。というのは、そのような変換は、画像やオーディオの偶然的（inadvertent）な使用と、透かしへの意図的な攻撃とで共通だからである。対応の効果は、オーディオの場合にはるかに明らかであるが、広帯域の変動などのように狭い意味で「周波数ベース」である透かしは、作品の元の長さから「クロッピング」又はクリップされたオ

DISH-Blue Spike-842
Exhibit 1004, Page 0817

ーディオ・サンプルにおけるアライメントの問題を有している。スケーリングは、人間の聴覚系にとってはるかにより顕著であるが、僅かな変化が、消費者には明らかではないにもかかわらず、周波数だけのタイプの透かしに影響することがありうる。ほとんどが周波数ベースの埋め込み形信号処理である、利用可能なオーディオ透かしアプリケーションに対するはるかに大きな脅威は、時間ベースの変換であり、これには、オーディオ信号の時間ベースの圧縮及び解凍が含まれる。シグナファイは、広帯域ベースの透かしの例であり、ソラナ（Solana）テクノロジ、ＣＲＬ、ＢＢＮ、ＭＩＴなどによるアプリケーションも同様である。「空間領域」アプローチというのが、デジマルク、シグナム、ＡＲＩＳ、アービトロン（Arbitron）などによって開発された技術に対するより適切な名称である。興味深いことに、時間ベースのアプローチは、画像について考察される場合には、基本的には空間ベースのアプローチである。ピクセルは、「畳み込み的」（convolutional）である。これら間の差異は、周波数の広帯域化された（spread-spectrum-ed）領域は「あまりに」うまく定義されているために、埋め込まれた信号と同じサブバンドでのランダム・ノイズの過剰な符号化を受けることになるという点である。

【００１８】

ジョバンニ（Giovannni）は、現実の透かしに対して、ブロック・ベースのアプローチを用いる。しかし、それには、スケーリングされた画像をその元のスケールに回復させることができる画像認識が伴っている。この「デスケーリング」は、画像が復号化される前に適用される。他のシステムでは、元の画像を透かし入りの画像と「区別」して「デスケーリング」を行っている。デスケーリングが、あらゆる画像、オーディオ又はビデオ透かしの生き残りにとって固有の重要性を有していることは明らかである。明らかでないのは、区別の動作がセキュリティの見地から受け入れ可能であるか、ということである。更に、画像のユーザ又は制作者ではなく、透かし「機関」によって区別が実行されなければならない場合には、権利者は、元の透かしの入っていないコンテンツを支配できないことになる。符号化／復号化鍵／鍵の対の内部でマスク・セットを用いることとは別に、元の信号を用いなければならない。オリジナルは、検出及び復号化を実行する

DISH-Blue Spike-842
Exhibit 1004, Page 0818

のに必要であるが、以上で説明した攻撃に関しては、透かしの入れられたコンテンツに対する権利を明確に確立することは不可能である。

【００１９】

以上を鑑みると、以上で論じた課題を解決する安全なデジタル透かしのための複数の変換の利用及び適用に対する実質的な必要性が存在することを理解することができるであろう。

【００２０】

【課題を解決するための手段】

安全なデジタル透かしのための複数の変換の利用及び適用によってこの技術における短所は大幅に改善することができる。本発明の或る実施例では、保護されるべきデジタル情報におけるデジタル・ブロックは、高速フーリエ変換を用いて周波数領域に変換される。複数の周波数及び関連する振幅が、変換されたデジタル・ブロックのそれぞれに対して識別され、識別された振幅の部分集合が、鍵からの基本マスクを用いてデジタル・ブロックのそれぞれに対して選択される。メッセージ情報は、畳み込みマスクを用いて発生された変換テーブルを用いて、メッセージから選択される。選ばれたメッセージ情報は、選択されたメッセージ情報に基づいて選択される振幅を変化させることによって、変換されたデジタル・ブロックのそれぞれに符号化される。

【００２１】

以下で明らかになる本発明のこれらの及びそれ以外の効果及び特徴により、本発明の性質は、以下で行う本発明の詳細な説明と、冒頭の特許請求の範囲と、添付の図面とを参照することによって、より明確に理解することができるはずである。

【００２２】

【発明の実施の形態】

本発明の或る実施例によると、安全なデジタル透かしのために複数の変換が用いられる。周波数領域又は空間領域の変換を用いる透かしには２つのアプローチが存在する。すなわち、小さなブロックを用いる場合とデータ・セット全体を用いる場合とである。オーディオやビデオのような時間ベースの媒体に対しては、

DISH-Blue Spike-842
Exhibit 1004, Page 0819

小さな部分において作業するのが実際的である。というのは、ファイル全体では、サイズが数メガバイトにもなりうるからである。しかし、静止画については、ファイルははるかに小さいのが通常であり、１回の操作で変換することができる。２つのアプローチは、それぞれが、各自の利点を有している。ブロック・ベースの方法は、クロッピングに対する抵抗性を有する。クロッピング（cropping）というのは、信号の部分的な切り取り又は除去である。データは複数の小さな部分（piece）に記憶されるので、クロッピングは、単に、いくつかの部分が失われることを意味する。１つの完全な透かしを復号化するのに十分なブロックが残っている限り、クロッピングによって、その透かしが除去されることはない。しかし、ブロック・ベースのシステムは、スケーリングに弱い。アフィン・スケーリング（affine scaling）又は「収縮」（shrinking）などのスケーリングは、信号の高周波の損失につながる。ブロックのサイズが３２サンプルであり、データが２００％スケーリングされる場合には、関係のあるデータは、６４サンプルをカバーすることになる。しかし、デコーダは、依然として、データは３２サンプルにあると考えるので、透かしを適切に読み取るのに必要な空間の半分しか用いない。セット全体のアプローチは、逆の振る舞いを有する。このアプローチは、スケーリングを生き延びるのは非常に得意である。その理由は、このアプローチでは、データを全体として扱い、符号化の前にデータを特定のサイズにスケーリングするのが一般的であるからである。しかし、どのように小さなクロッピングであっても、変換のアライメントを混乱させ、透かしを曖昧にしてしまう可能性がある。

【００２３】

本発明を用いると、そして、これまでに開示されている材料を組み入れることによって、符号化鍵／鍵の対を用いて画像や歌やビデオを認証し、暗号による誤った肯定的な一致を排除し、オリジナルな透かしの入れられていない作品の代わりに第三者の権限を備えた登録を通じて著作権の通信を提供することが可能となる。

【００２４】

本発明は、従来技術に対する明らかな改良を提供するのであるが、元（オリジ

DISH-Blue Spike-842
Exhibit 1004, Page 0820

ナル）の信号の座標値を鍵の上にオフセットし、次にそれを用いてユーザ又は認証を受けた「鍵の持ち主」による復号化又は検出動作が行われることによって、過去に開示された内容に対する改良がなされる。このオフセットは、透かしが、成功裏に符号化されうるデータの量を、シャノンのノイズを含むチャネルの符号化定理に基づいて「運ばせる」（ペイロードさせる）ことができるコンテンツにおいて必要であり、これによって、透かしメッセージを有する信号の十分に不可視的な「飽和」が回避され、権利者が単一のメッセージを検出することが可能となる。例えば、或る画像が単一の１００ビットのメッセージ又は１２のＡＳＣＩＩ文字を運ぶのに十分なペイロードだけを有するというのも、全くありうることである。本発明の発明者によってテストがなされたオーディオでの実現例では、毎秒１０００ビットが、１６ビットの４４．１ｋＨｚのオーディオ信号において、不可聴的に符号化される。電子的に利用可能なほとんどの画像は、同じ「ペイロード」率を与えることができるほどに十分なデータを有していない。従って、クロッピング及びスケーリングが同時に生き延びることは画像の場合の方が、それに対応する商業的に利用可能なオーディオ又はビデオ・トラックの場合よりも困難であることになる。追加されるセキュリティの効果は、広帯域又は周波数のみのアプリケーションに基づく透かしシステムのランダマイザが制限されているほど、透かしデータのランダム値は、制限された信号帯域上で「ホッピング」することになり、また、鍵もまた、ランダムな態様でより効果的に符号化を行うのに用いられる暗号化された又はランダムなデータの独立なソースである、ということである。鍵は、実際に、ビット数で測定した場合に、透かしメッセージ自体よりも大きなランダム値を有しうる。透かしデコーダは、画像が、そのオリジナルのスケールに含まれていることを求められ、また、その「デスケーリング」された寸法に基づいてクロッピングされたかどうかを決定することができる。

【００２５】

コンテンツに透かしを入れそのコンテンツの流通を有効化するために鍵を要求するシステムの利点は明らかである。異なる情報を符号化するには異なる鍵を用いることができる。その際に、安全な一方向ハッシュ関数や、デジタル署名や、更には一時的パッド（one-time pads）でさえも鍵の中に組み入れることによっ

DISH-Blue Spike-842
Exhibit 1004, Page 0821

て、埋め込まれた信号を保護し、透かしの入れられた画像とその鍵／鍵の対を拒絶せずに有効化することができる。後に、これらの同じ鍵を用いて、埋め込まれたデジタル署名だけを後で有効化する、又は、デジタル透かしメッセージを完全に復号化する。コンテンツにデジタル透かしが入れられているということだけでなく、流通業者はそれ以外にはどのような機能も有していない鍵を用いてデジタル署名のチェックを実行することによって透かしの有効性をチェックしなければならないということも、出版業者は、容易に要求することができる。

【００２６】

安全なデジタル透かしが、いくらか論じられ始めている。レイトン（Leighton）は、米国特許第５，６６４，０１８号に、デジタル透かしにおける共謀的な攻撃（collusion attack）を防止する手段を記載している。しかし、レイトンは、記載されているセキュリティを現実的には提供できない可能性がある。例えば、透かし技術が線形であるような特定の場合には、「挿入封筒」又は「透かし空間」が矛盾なく定義されており（well-defined）、従って、認証を受けていないものによる共謀よりは複雑でない攻撃を受ける可能性がある。透かし符号化レベルにおける過剰符号化（over encoding）は、そのような線形の実現例における１つの単純な攻撃に過ぎない。レイトンによって無視された別の考慮として、商業的価値のあるコンテンツは、多くの場合に、既に透かしの入れられていない形態でいずれかの場所に既に存在しており、潜在的な侵害行為に容易にさらされる状態にあるので、どのようなタイプの共謀行為も不要であるということがある。この例として、コンパクト・ディスクやデジタル放送されたビデオなど多くがある。透かしデータの前処理を用いて埋め込まれた信号にデジタル署名をすることによって、共謀の成功を回避することができる可能性が大きい。透かしを入れる媒体に依存するが、非常に個別化された（granular）透かしアルゴリズムは、ベースラインとなる透かしが何らかの機能を有しているという予測よりも、デジタル的にサンプリングがなされるあらゆる媒体において共通な与えられた量子化人工物を、何か観測可能なものよりも低いレベルで成功裏に符号化できる可能性が高い。

【００２７】

DISH-Blue Spike-842
Exhibit 1004, Page 0822

更に、ここで開示されている「ベースライン」透かしは、かなり主観的なものである。これは、この技術分野のいずれかの場所で信号の「知覚的に意義のある」領域として説明されるだけである。すなわち、透かし関数の線形性を減少させる、又は、透かしの挿入を反転させることにより、「ベースライン」透かしを阿ｓくせいするのに要求される追加的な作業なしに同じ効果が得られるように思われる。実際、透かしアルゴリズムは、追加的なステップなしに、ターゲット挿入封筒又は領域を既に定義することができるべきである。更に、本発明の発明者によって既に開示されている出願では、透かしデータに加えて、利用可能な透かし領域の「ビット空間」又は符号化とは関係のないランダム・ノイズよりも少ないビットを符号化するように設定することにより、可能性のある攻撃やそれ以外の抹消の試みを混乱させることができる透かし技術が説明されている。「候補ビット」の領域は、任意の数の圧縮方式又は変換によって定義することができ、すべてのビットを符号化するすることは必要でない。更に、すべてのビットを符号化することは、符号化方式を知りながら領域を複製することができるものにとっては、現実的には、セキュリティ上の弱点として作用する可能性がある。やはり、セキュリティは、実際の透かしメッセージの外部にオフセットされていなければならず、それによって、真に堅固で安全な透かしの実現が得られるのである。

【００２８】

対照的に、本発明は、様々な暗号化プロトコルを用いて実現し、基礎となるシステムにおける信頼性及びセキュリティの両方を強化することができる。所定の鍵は、マスクの組として説明される。これらのマスクには、基本、畳み込み及びメッセージ・デリミタが含まれるが、メッセージのデジタル署名などの追加的な領域にも拡張することができる。これまでに開示されている技術では、これらのマスクの機能は、写像に対してだけ定義されていた。公開及び秘密鍵を鍵の対として用いて、鍵が危険にさらされることがない可能性を増加させることができる。符号化の前に、上述のマスクは、暗号的な見地から安全なランダム発生プロセスによって発生される。ＤＥＳなどのブロック暗号は、十分にランダムなシード値（seed value）と組み合わされて、暗号的に安全なランダム・ビット発生器をエミュレートする。これらの鍵は、考察しているサンプル・ストリームにそれら

DISH-Blue Spike-842
Exhibit 1004, Page 0823

を一致させる情報と共にデータベースにセーブされ、デスクランブリング（スクランブル解除）や後の検出又は復号化動作に用いられる。

【００２９】

これらの同じ暗号化プロトコルを、スクランブルされていない状態でストリームされたコンテンツを正しく表示又は再生するために認証された鍵を要求するストリームされたコンテンツを管理する際に、本発明の実施例と組み合わせることができる。デジタル透かしの場合と同様に、対称的又は非対称的な公開鍵の対が、様々な実現例において用いられる。更に、真正の鍵の対を維持する認証機関に対する必要性も、対称的な鍵の実現例以上のセキュリティを得るためには、伝送の際のセキュリティを考える際には考慮すべき問題となる。

【００３０】

次に、本発明によるデジタル情報保護システムの或る実施例を説明する。ここで添付の図面を参照するが、同じ要素については、複数の図面にわたって同じ参照番号が付されている。図１には、本発明の実施例によるデジタル情報符号化方法のブロック流れ図が図解されている。１つの画像が「ブロック」ごとに処理されるのであるが、ここで、各ブロックは、例えば、単色チャネルにおける３２Ｘ３２のピクセル領域である。ステップ１１０では、各ブロックが、スペクトル変換又は高速フーリエ変換（ＦＦＴ）を用いて、周波数領域に変換される。ステップ１２０及び１３０において、最大の３２の振幅が識別され、これら３２の中の部分集合が、鍵からの基本マスクを用いて選択される。次に、１メッセージ・ビットが、ステップ１４０及び１５０において各ブロックの中に符号化される。このビットは、畳み込みマスクを用いて発生された変換テーブルを用いてメッセージから選ばれる。このビットが真である場合には、選択された振幅は、ユーザによって定義された強度率（strength fraction）だけ減少される。ビットが偽である場合には、振幅は不変である。

【００３１】

選択された振幅と周波数とは、それぞれが、鍵の中に記憶される。すべての画像が処理された後で、ピクセルの対角線方向のストライプが鍵にセーブされる。このストライプは、例えば、左上の角で開始して、画像を通って４５度の角度で

DISH-Blue Spike-842
Exhibit 1004, Page 0824

進むことができる。画像の元の寸法も、鍵に記憶される。

【００３２】

図２は、本発明の実施例によるデジタル情報デスケーリング方法のブロック流れ図である。画像が復号化のために選ばれると、最初に、クロッピング及び／又はスケーリングがなされているかどうかがチェックされる。されている場合には、画像は、ステップ２１０において、元の寸法にスケーリングされる。結果的に得られる「ストライプ」すなわちピクセルの対角線は、ステップ２２０において、鍵に記憶されているストライプとの適合が調べられる。適合がそれ以前の最良の適合よりも優れている場合には、スケールがステップ２３０及び２４０においてセーブされる。望むのであれば、例えば、ステップ２６０において、ゼロ・ピクセルの単一のロー又はコラムを用いて、画像をパディングすることができる。そして、このプロセスを反復して、適合が改善するかどうかを見ることができる。

【００３３】

ステップ２５０において完全な適合が見出される場合には、プロセスは終了する。完全な適合が得られない場合には、ユーザによって設定されるクロップ「半径」まで、プロセスが継続される。例えば、クロップ半径が４である場合には、画像を、４つのロー及び／又は４つのコラムまでパディングすることができる。ゼロによって置き換えられた任意のクロッピングされた領域を用いて、最良の適合が選ばれ、画像は、園もとの寸法まで回復される。

【００３４】

情報は、いったんデスケーリングされると、図３に示されている本発明の実施例に従って復号化される。復号化は、符号化の逆プロセスである。復号化された振幅は、鍵に記憶されたものと比較され、ステップ３１０及び３２０において、符号化されたビットの位置が決定される。メッセージは、ステップ３３０において、逆変換テーブルを用いてアセンブルされる。次に、ステップ３４０では、メッセージはハッシュ化され、このハッシュが元のメッセージのハッシュと比較される。元のハッシュは、符号化の間に鍵に記憶される。ハッシュが一致する場合には、メッセージは有効であると宣言され、ステップ３５０においてユーザに与

DISH-Blue Spike-842
Exhibit 1004, Page 0825

えられる。

【００３５】

この出願においては様々な実施例が特に図解され説明されているが、本発明の修正及び変形は、以上の説明によってカバーされ、本発明の精神と意図された範囲とから逸脱することなく、冒頭の特許請求の範囲に含まれる。更に、オーディオ及びビデオ・コンテンツに対して、時間ベースの信号操作や振幅及びピッチ動作のために、同様の動作が適用された。透かしの入れられていないオリジナルを用いることなくデスケーリング又はそれ以外の態様で迅速に差異を判断できる能力が、安全なデジタル透かしにとっては、固有の重要性を有している。デジタル化されたコンテンツはネットワークを介して交換されるので、拒絶されないことと第三者による認証とを保証することも重要である。

【図面の簡単な説明】

【図１】

本発明の或る実施例によるデジタル情報の符号化方法のブロック流れ図である。

【図２】

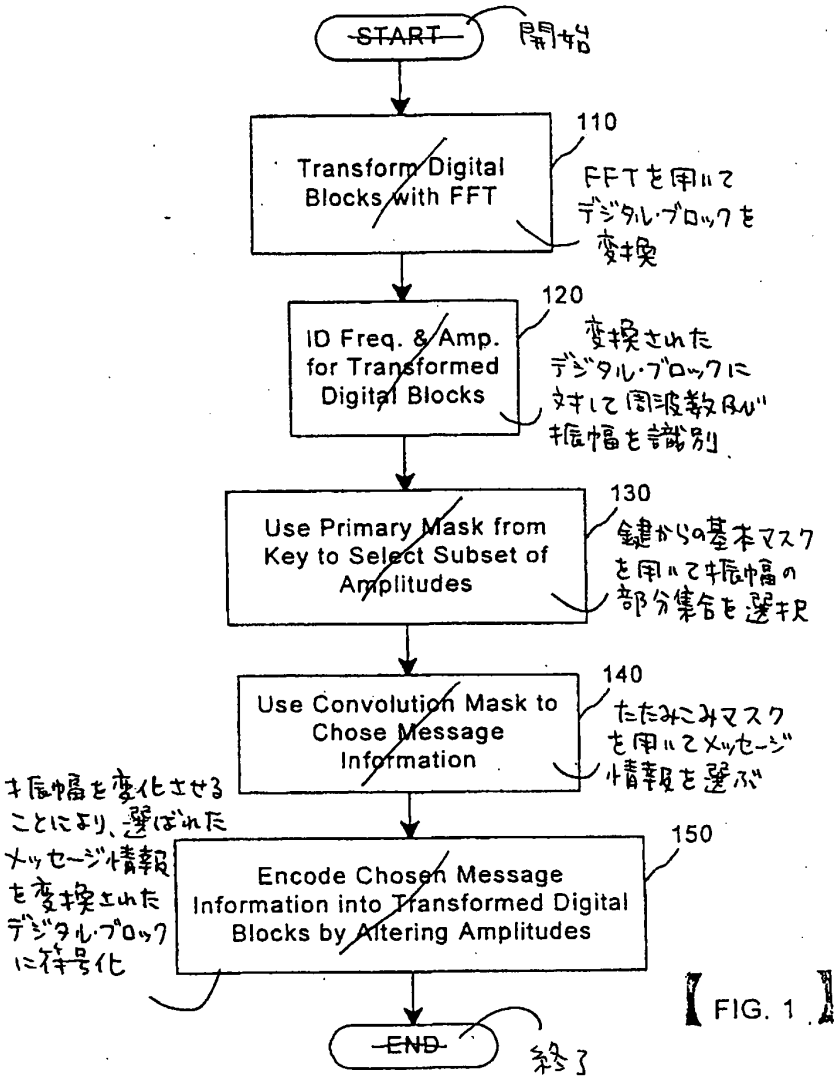
本発明の或る実施例によるデジタル情報のデスケーリング方法のブロック流れ図である。

【図３】

本発明の或る実施例によるデジタル情報の復号化方法のブロック流れ図である。

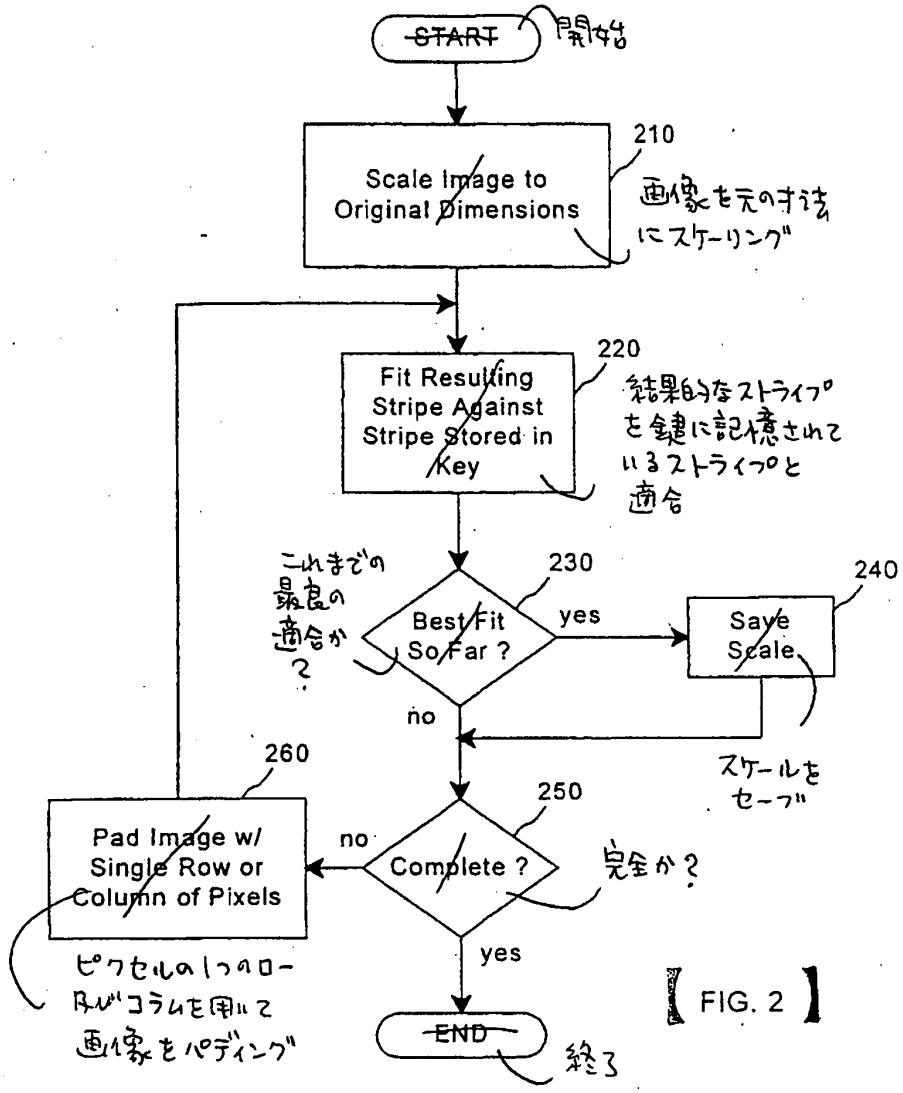
DISH-Blue Spike-842
Exhibit 1004, Page 0826

【書類名】　図面



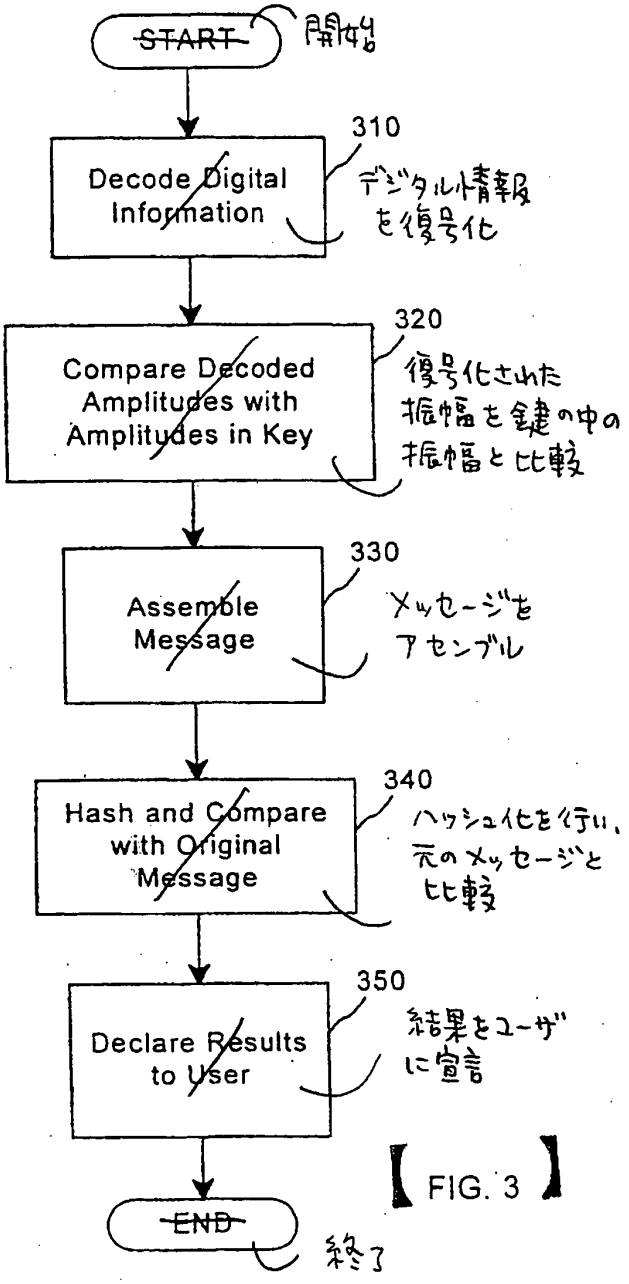
【FIG. 1】

DISH-Blue Spike-842
Exhibit 1004, Page 0827



【 FIG. 2 】

Proof - 2000/10/02

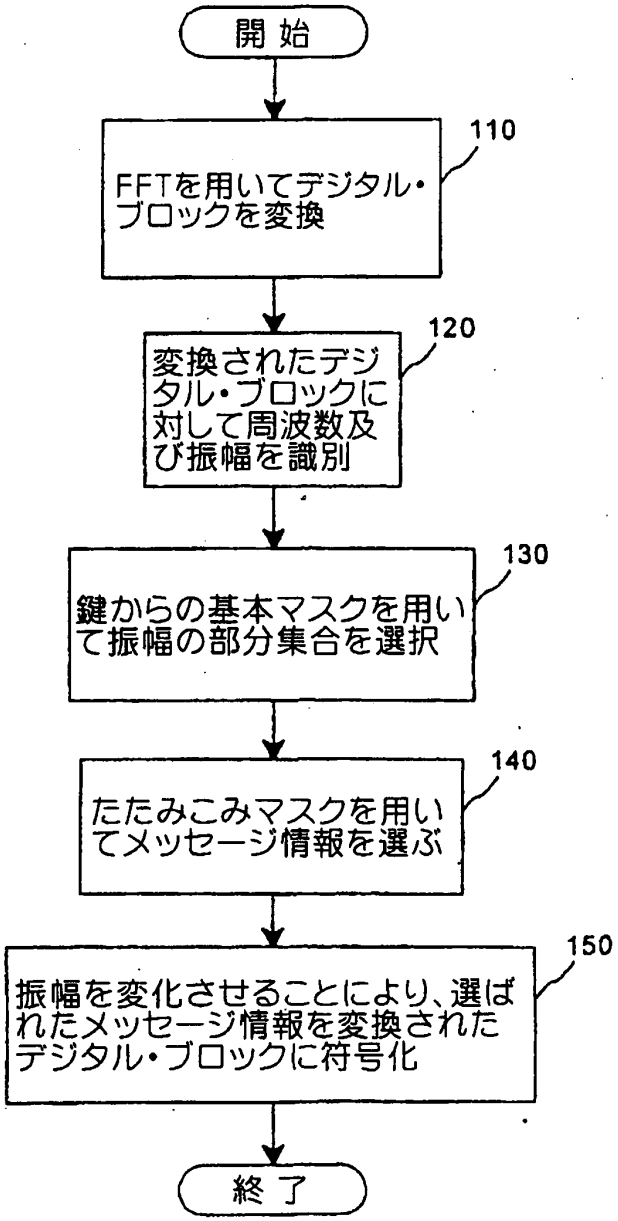


【 FIG. 3 】

Proof - 2000/10/02

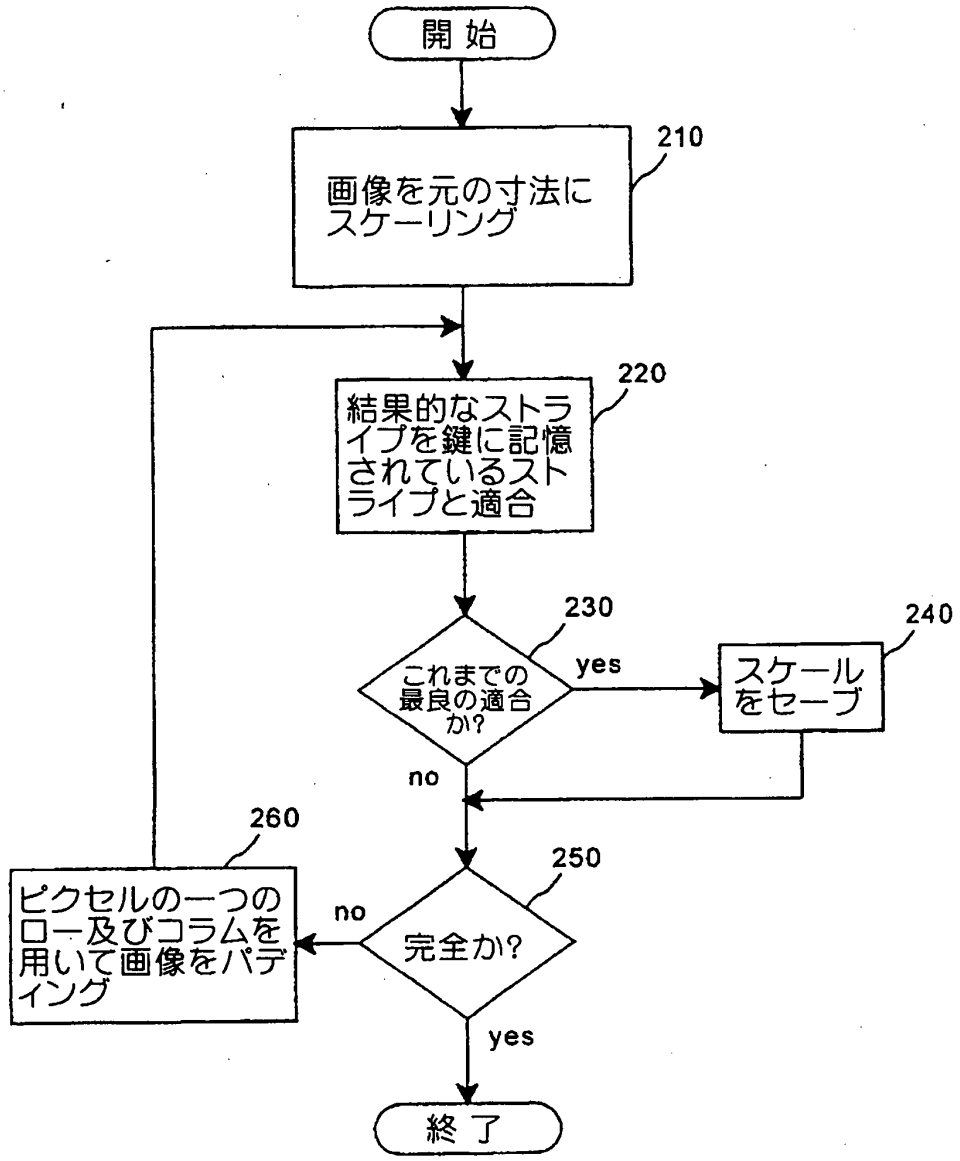
【書類名】　図面

【図１】



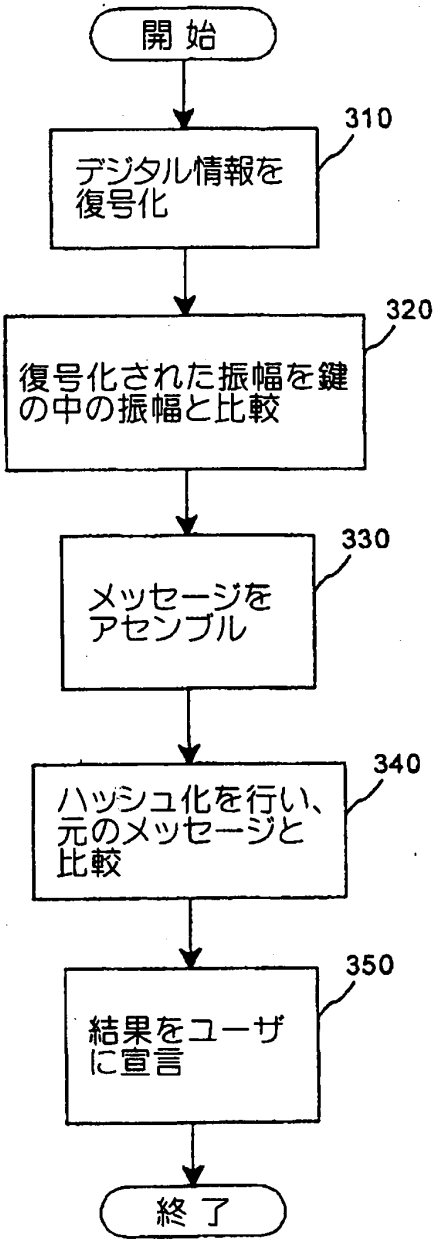
DISH-Blue Spike-842
Exhibit 1004, Page 0830

【図２】



Proof - 2000/10/13

【図３】



DISH-Blue Spike-842
Exhibit 1004, Page 0832

【書類名】　要約書

【要約】　安全なデジタル透かしのための複数の変換の利用及び適用である。本発明の或る実施例では、保護されるべきデジタル情報におけるデジタル・ブロックは、高速フーリエ変換を用いて周波数領域に変換される。複数の周波数及び関連する振幅が、変換されたデジタル・ブロックのそれぞれに対して識別され、識別された振幅の部分集合が、鍵からの基本マスクを用いてデジタル・ブロックのそれぞれに対して選択される。メッセージ情報が、畳み込みマスクを用いて発生された変換テーブルを用いて、メッセージから選択される。選ばれたメッセージ情報は、選択されたメッセージ情報に基づいて選択される振幅を変化させることによって、変換されたデジタル・ブロックのそれぞれに符号化される。

DISH-Blue Spike-842
Exhibit 1004, Page 0833

Amendment

【書類名】　手続補正書　　Filed: October 13, 2000

【整理番号】　002365I

【提出日】　平成12年10月13日

【あて先】　特許庁長官　殿

【事件の表示】

【国際出願番号】　PCT/US99/07262

【出願の区分】　特許

【補正をする者】

【住所又は居所】　アメリカ合衆国フロリダ州３３１６０，マイアミ，コリンズ・アベニュー　１６７１１，ナンバー　２５０５

【氏名又は名称】　スコット・エイ・モスコウィッツ

【代理人】

【識別番号】　100089705

【住所又は居所】　東京都千代田区大手町二丁目２番１号　新大手町ビル２０６区　ユアサハラ法律特許事務所

【弁理士】

【氏名又は名称】　社本　一夫

【手続補正　1】

【補正対象書類名】　図面

【補正対象項目名】　全図

【補正方法】　変更

【補正の内容】　1

【その他】　浄書につき、図面の実体的内容には変更なし。

【プルーフの要否】　要

Proof - 2000/10/13

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 7/167 — A1

(11) International Publication Number: **WO 00/57643**

(43) International Publication Date: 28 September 2000 (28.09.00)

(21) International Application Number: PCT/US00/06522

(22) International Filing Date: 14 March 2000 (14.03.00)

(30) Priority Data:
60/125,990 24 March 1999 (24.03.99) US

(71) Applicant *(for all designated States except US)*: BLUE SPIKE, INC. [US/US]; 16711 Collins Avenue, Miami, FL 33160 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: MOSKOWITZ, Scott, A. [US/US]; 16711 Collins Avenue, Miami, FL 33160 (US). BERRY, Michael [US/US]; 12401 Princess Jeanne, Albuquerque, NM 87112 (US).

(74) Agents: CHAPMAN, Floyd, B. et al.; Baker Botts, L.L.P., 1299 Pennsylvania Avenue, N.W., Washington, DC 20004 (US).

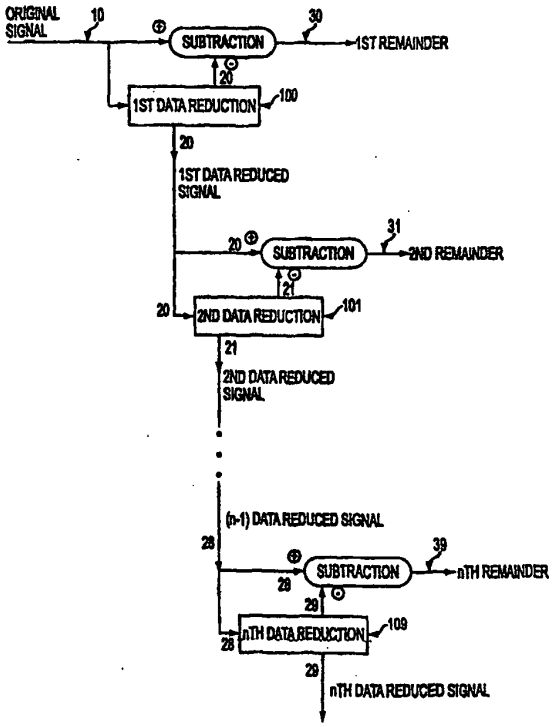
(81) Designated States: JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: UTILIZING DATA REDUCTION IN STEGANOGRAPHIC AND CRYPTOGRAPHIC SYSTEMS

(57) Abstract

The present invention is a method for protecting a data signal where the method comprises the following steps: applying a data reduction technique (200) to the signal to produce a reduced signal, subtracting (60) the reduced data signal from the original signal to produce a remainder signal (39), embedding (300) a first watermark into the reduced data signal to produce a watermarked redued data signal, and adding (50) the watermarked reduced signal to the remainder signal to produce an output signal (90). A second watermark (301) may be embedded into the remainder signal (39) before the final addition (50) step. Cryptographic techniques may be employed to encrypt the remainder signal and/or the reduced signal prior to the addition step (50).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

UTILIZING DATA REDUCTION IN STEGANOGRAPHIC AND CRYPTOGRAPHIC SYSTEMS

FIELD OF INVENTION

This invention relates to digital signal processing, and more particularly to a method and a system for encoding at least one digital watermark into a signal as a means of conveying information relating to the signal and also protecting against unauthorized manipulation of the signal.

BACKGROUND OF INVENTION

Digital watermarks help to authenticate the content of digitized multimedia information, and can also discourage piracy. Because piracy is clearly a disincentive to the digital distribution of copyrighted content, establishment of responsibility for copies and derivative copies of such works is invaluable. In considering the various forms of multimedia content, whether "master," stereo, NTSC video, audio tape or compact disc, tolerance of quality will vary with individuals and affect the underlying commercial and aesthetic value of the content. It is desirable to tie copyrights, ownership rights, purchaser information or some combination of these and related data into the content in such a manner that the content must undergo damage, and therefore reduction of its value, with subsequent, unauthorized distribution, commercial or otherwise. Digital watermarks address many of these concerns.

A matter of general weakness in digital watermark technology relates directly to the manner of implementation of the watermark. Many approaches to digital watermarking leave detection and decode control with the implementing party of the digital watermark, not the creator of the work to be protected. This weakness removes proper economic incentives for improvement of the technology. One specific form of exploitation mostly regards efforts to obscure subsequent watermark detection. Others regard successful over encoding using the same watermarking process at a subsequent time. Yet another way to perform secure digital watermark implementation is through "key-based" approaches.

This paper draws a distinction between a "forensic watermark," based on provably-secure methods, and a "copy control" or "universal" watermark which is intended to be low cost and easily implemented into any general computing or consumer electronic device. A watermark can be forensic if it can identify the source of the data from which a copy was made. For example, assume that digital data are stored on a disk and provided to "Company A" (the "A disk"). Company A makes an unauthorized copy and delivers the copy to "Company B" (the "B disk"). A forensic watermark, if present in the digital data stored on the "A disk," would identify the "B disk" as having been copied from the "A disk."

On the other hand, a copy control or universal watermark is an embedded signal which is governed by a "key" which may be changed (a "session key") to increase security, or one that is easily accessible to devices that may offer less than strict cryptographic security. The "universal" nature of the watermark is the computationally inexpensive means for accessing or other associating the watermark with operations that can include playback, recording or manipulations of the media in which it is embedded.

A fundamental difference is that the universality of a copy control mechanism, which must be redundant enough to survive many signal manipulations to eliminate most casual piracy, is at odds with the far greater problem of establishing responsibility for a given instance of a suspected copying of a copyrighted media work. The more dedicated pirates must be dealt with by encouraging 3rd party authentication with "forensic watermarks" or those that constitute "transactional watermarks" (which are encoded in a given copy of said content to be watermarked as per the given transaction).

The goal of a digital watermark system is to insert a given information signal or signals in such a manner as to leave little or no evidence of the presence of the information signal in the underlying content signal. A separate but equal goal is maximizing the digital watermark's encoding level and "location sensitivity" in the underlying content signal such that the watermark cannot be removed without damage to the content signal.

One means of implementing a digital watermark is to use key-based security. A predetermined or random key can be generated as a map to access the hidden information signal. A key pair may also be used. With a typical key pair, a party possesses a public and a private key. The private key is maintained in confidence by the owner of the key, while the owner's public key is disseminated to those persons in the public with whom the owner would regularly communicate. Messages being communicated, for example by the owner to another, are encrypted with the private key and can only be read by another person who possesses the corresponding public key. Similarly, a message encrypted with the person's public key can only be decrypted with the corresponding private key. Of course, the keys or key pairs may be processed in separate software or hardware devices handling the watermarked data.

SUMMARY OF THE INVENTION

A method of securing a data signal comprises the steps of: applying a data reduction technique to reduce the data signal into a reduced data signal; subtracting said reduced data signal from the data signal to produce a remainder signal; using a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal; using a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal; and adding said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.

A system for securing a data signal comprises: means to apply a data reduction technique to reduce the data signal into a reduced data signal; means to subtract said reduced data signal from the data signal to produce a remainder signal; means to apply a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal; means to apply a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal; and means to add said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.

A method of securing a data signal comprises the steps of: applying a data reduction technique to reduce the data signal into a reduced data signal; subtracting said reduced data signal from the data signal to produce a remainder signal; embedding a first watermark into said reduced data signal to produce a watermarked, reduced data signal; embedding a second watermark into said remainder signal to produce a watermarked remainder signal; and adding said watermarked, reduced data signal to said watermarked remainder signal to produce an output signal.

A method of protecting a data signal comprises: applying a data reduction technique to reduce the data signal into a reduced data signal; subtracting said reduced data signal from the data signal to produce a remainder signal; using a first scrambling technique to scramble said reduced data signal to produce a scrambled, reduced data signal; using a second scrambling technique to scramble said remainder signal to produce a scrambled remainder signal; and adding said scrambled, reduced data signal to said scrambled remainder signal to produce an output signal.

There are two design goals in an overall digital watermarking system's low cost, and universality. Ideally, a method for encoding and decoding digital watermarks in digitized media for copy control purposes should be inexpensive and universal. This is essential in preventing casual piracy. On the other hand, a more secure form of protection, such as a "forensic watermarks," can afford to be computationally intensive to decode, but must be unaffected by repeated re-encoding of a copy control watermark. An ideal method for achieving these results would separate the signal into different areas, each of which can be accessed independently. The embedded signal or may simply be "watermark bits" or "executable binary code," depending on the application and type of security sought. Improvements to separation have been made possible by enhancing more of the underlying design to meet a number of clearly problematic issues. The present invention interprets the signal as a stream which may be split into separate streams of digitized samples or may undergo data reduction (including both lossy and lossless compression, such as MPEG lossy compression and Meridian's lossless compression, down sampling, common to many studio operations, or any

related data reduction process). The stream of data can be digital in nature, or may also be an analog waveform (such as an image, audio, video, or multimedia content). One example of digital data is executable binary code. When applied to computer code, the present invention allows for more efficient, secure, copyright protection when handling functionality and associations with predetermined keys and key pairs in software applications or the machine readable versions of such code in microchips and hardware devices. Text may also be a candidate for authentication or higher levels of security when coupled with secure key exchange or asymmetric key generation between parties. The subsets of the data stream combine meaningful and meaningless bits of data which may be mapped or transferred depending on the application intended by the implementing party.

The present invention utilizes data reduction to allow better performance in watermarking as well as cryptographic methods concerning binary executable code, its machine readable form, text and other functionality-based or communication-related applications. Some differences may simply be in the structure of the key itself, a pseudo random or random number string or one which also includes additional security with special one way functions or signatures saved to the key. The key may also be made into key pairs, as is discussed in other disclosures and patents referenced herein. The present invention contemplates watermarks as a plurality of digitized sample streams, even if the digitized streams originate from the analog waveform itself. The present invention also contemplates that the methods disclosed herein can be applied to non-digitized content. Universally, data reduction adheres to some means of "understanding "the reduction. This disclosure looks at data reduction which may include down sampling, lossy compression, summarization or any means of data reduction as a novel means to speed up watermarking encode and decode operations. Essentially a lossy method for data reduction yields the best results for encode and decode operations.

It is desirable to have both copy control and forensic watermarks in the same signal to address the needs of the hardware, computer, and software industries while

also providing for appropriate security to the owners of the copyrights. This will become clearer with further explanation of the sample embodiments discussed herein.

The present invention also contemplates the use of data reduction for purposes of speedier and more tiered forms of security, including combinations of these methods with transfer function functions. In many applications, transfer functions (e.g., scrambling), rather than mapping functions (e.g., watermarking), are preferable or can be used in conjunction with mapping. With "scrambling," predetermined keys are associated with transfer functions instead of mapping functions, although those skilled in the art may recognize that a transfer function is simply a subset of mask sets encompassing mapping functions. It is possible that tiered scrambling with data reduction or combinations of tiered data reduction with watermarking and scrambling may indeed increase overall security to many applications.

The use of data reduction can improve the security of both scrambling and watermarking applications. All data reduction methods include coefficients which affect the reduction process. For example, when a digital signal with a time or space component is down sampled, the coefficient would be the ratio of the new sample rate to the original sample rate. Any coefficients that are used in the data reduction can be randomized using the key, or key pair, making the system more resistant to analysis. Association to a predetermined key or key pair and additional measure of security may include biometric devices, tamper proofing of any device utilizing the invention, or other security measures.

Tests have shown that the use of data reduction in connection with digital watermarking schemes significantly reduces the time required to decode the watermarks, permitting increases in operational efficiency.

Particular implementations of the present invention, which have yielded incredibly fast and inexpensive digital watermarking systems, will now be described. These systems may be easily adapted to consumer electronic devices, general purpose computers, software and hardware. The exchange of predetermined keys or key pairs may facilitate a given level of security. Additionally, the complementary increase in

security for those implementations where transfer functions are used to "scramble" data, is also disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the invention and some advantages thereof, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

FIG. 1 is a functional block diagram that shows a signal processing system that generates "n" remainder signals and "n" data reduced signals.

FIG. 2 is a functional block diagram for an embodiment of the present invention which illustrates the generation of an output signal comprised of a data-reduced, watermarked signal and a first remainder signal.

FIG. 3 is a functional block diagram for an embodiment of the present invention which illustrates the generation of an output signal comprised of a data-reduced, watermarked signal and a watermarked, first remainder signal.

FIG. 4 is a functional block diagram for decoding the output signal generated by the system illustrated in FIG. 2.

FIG. 5 is a functional block diagram for decoding the output signal generated by the system illustrated in FIG. 3.

FIG. 6 is a functional block diagram for an embodiment of the present invention which illustrates the generation of an output signal comprised of a data-reduced, scrambled signal and a first remainder signal.

FIG. 7 is a functional block diagram for an embodiment of the present invention which illustrates the generation of an output signal comprised of a data--reduced, scrambled signal and a scrambled, first remainder signal.

FIG. 8 is a functional block diagram for decoding the output signal generated by the system illustrated in FIG. 6.

FIG. 9 is a functional block diagram for decoding the output signal generated by the system illustrated in FIG. 7.

DETAILED DESCRIPTION

The embodiments of the present invention and its advantages are best understood by referring to the drawings, like numerals being used for like and corresponding parts of the various drawings.

An Overview

A system for achieving multiple levels of data reduction is illustrated in FIG. 1. An input signal 10 (for example, instructional text, executable binary computer code, images, audio, video, multimedia or even virtual reality imaging) is subjected to a first data reduction technique 100 to generate a first data reduced signal 20. First data reduced signal 20 is then subtracted from input signal 10 to generate a first remainder signal 30.

First data reduced signal 20 is subjected to a second data reduction technique 101 to generate a second data reduced signal 21. Second data reduced signal 21 is then subtracted from first data reduced signal 20 to generate a second remainder signal 31.

Each of the successive data reduced signals is, in turn, subjected to data reduction techniques to generate a further data reduced signal, which, in turn, is subtracted from its respective parent signal to generate another remainder signal. This process is generically described as follows. An (n-1) data reduced signal 28 (i.e, a signal that has been data reduced n-1 times) is subjected to an nth data reduction technique 109 to generate an nth data reduced signal 29. The nth data reduced signal 29 is then subtracted from the (n-1) data reduced signal 28 to produce an n^{th} remainder signal 39.

An output signal can be generated from the system illustrated in FIG. 1 in numerous ways. For example, each of the n remainder signals (which, through represented by reference numerals 30-39, are not intended to be limited to 10 signals) and the n^{th} data signal may optionally subjected to a watermarking technique, or even optionally subjected to a encryption technique, and each of the (n+1) signals (whether

watermarked or encrypted, or otherwise untouched) may then be added together to form an output signal. By way of more particular examples, each of the (n+1) signals (i.e., the n remainder signals and the n^{th} data reduced signal) can be added together without any encryption or watermarking to form an output signal; or one or more of the (n+1) signals may be watermarked and then all (n+1) signals may be added together; or one or more of the (n+1) signals may be encrypted and then all (n+1) signals may be added together. It is anticipated that between these three extremes lie numerous hybrid combinations involving one or more encryptions and one or more watermarkings.

Each level may be used to represent a particular data density. E.g., if the reduction method is down-sampling, for a DVD audio signal the first row would represent data sampled at 96 kHz, the second at 44.1 kHz., the third at 6 kHz., etc. There is only an issue of deciding what performance or security needs are contemplated when undertaking the data reduction process and choice of which types of keys or key pairs should be associated with the signal or data to be reduced. Further security can be increased by including block ciphers, special one way functions, one time stamps or even biometric devices in the software or hardware devices that can be embodied. Passwords or biometric data are able to assist in the determination of the identity of the user or owner of the data, or some relevant identifying information.

An example of a real world application is helpful here. Given the predominant concern, at present, of MPEG 1 Layer 3, or MP3, a perceptual lossy compression audio data format, which has contributed to a dramatic re-evaluation of the distribution of music, a digital watermark system must be able to handle casual and more dedicated piracy in a consistent manner. The present invention contemplates compatibility with MP3, as well as any perceptual coding technique that is technically similar. One issue, is to enable a universal copy control "key" detect a watermark as quickly as possible from a huge range of perceptual quality measures. For instance, DVD 24 bit 96 kHz, encoded watermarks, should be detected in at least "real time," even after the signal has been down sampled, to say 12 kHz of the 96 kHz originally referenced. By delineating and starting with less data, since the data-reduced signal is obviously smaller though

still related perceptually to the original DVD signal, dramatic increases in the speed and survival of the universal copy control bits can be achieved. The present invention also permits the ability to separate any other bits which may be associated with other more secure predetermined keys or key pairs.

Where the data stream is executable computer code, the present invention contemplates breaking the code into objects or similar units of functionality and allowing for determination of what is functionally important. This may be more apparent to the developer or users of the software or related hardware device. Data reduction through the use of a subset of the functional objects related to the overall functionality of the software or executable code in hardware or microchips, increase the copyright protection or security sought, based on reducing the overall data to be associated with predetermined keys or key pairs. Similarly, instead of mapping functions, transfer functions, so-called "scrambling," appear better candidates for this type of security although both mapping and transferring may be used in the same system. By layering the security, the associated keys and key pairs can be used to substantially improve the security and to offer easier methods for changing which functional "pieces" of executable computer code are associated with which predetermined keys. These keys may take the form of time-sensitive session keys, as with transactions or identification cards, or more sophisticated asymmetric public key pairs which may be changed periodically to ensure the security of the parties' private keys. These keys may also be associated with passwords or biometric applications to further increase the overall security of any potential implementation.

An example for text message exchange is less sophisticated but, if it is a time sensitive event, e.g., a secure communication between two persons, benefits may also be encountered here. Security may also be sought in military communications. The ability to associate the securely exchanged keys or key pairs while performing data reduction to enhance the detection or decoding performance, while not compromising the level of security, is important. Though a steganographic approach to security, the present invention more particularly addresses the ability to have data reduction to

increase speed, security, and performance of a given steganographic system. Additionally, data reduction affords a more layered approach when associating individual keys or key pairs with individual watermark bits, or digital signature bits, which may not be possible without reduction because of considerations of time or the payload of what can be carried by the overall data "covertext" being transmitted.

Layering through data reduction offers many advantages to those who seek privacy and copyright protection. Serialization of the detection chips or software would allow for more secure and less "universal" keys, but the interests of the copyright owners are not always aligned with those of hardware or software providers. Similarly, privacy concerns limit the amount of watermarking that can be achieved for any given application. The addition of a pre-determined and cryptographic key-based "forensic" watermark, in software or hardware, allows for 3rd party authentication and provides protection against more sophisticated attacks on the copy control bits. Creating a "key pair" from the "predetermined" key is also possible.

Separation of the watermarks also relates to separate design goals. A copy control mechanism should ideally be inexpensive and easily implemented, for example, a form of "streamed watermark detection." Separating the watermark also may assist more consistent application in broadcast monitoring efforts which are time-sensitive and ideally optimized for quick detection of watermarks. In some methods, the structure of the key itself, in addition to the design of the "copy control" watermark, will allow for few false positive results when seeking to monitor radio, television, or other streamed broadcasts (including, for example, Internet) of copyrighted material. As well, inadvertent tampering with the embedded signal proposed by others in the field can be avoided more satisfactorily. Simply, a universal copy control watermark may be universal in consumer electronic and general computing software and hardware implementations, but less universal when the key structure is changed to assist in being able to log streaming, performance, or downloads, of copyrighted content. The embedded bits may actually be paired with keys in a decode device to assure accurate broadcast monitoring and tamper proofing, while not requiring a watermark to exceed

the payload available in an inaudible embedding process. E.g., A full identification of the song, versus time-based digital signature bits, embedded into a broadcast signal, may not be recovered or may be easily over encoded without the use of block ciphers, special one way functions or one time pads, during the encoding process, prior to broadcast. Data reduction as herein disclosed makes this operation more efficient at higher speeds.

A forensic watermark is not time sensitive, is file-based, and does not require the same speed demands as a streamed or broadcast-based detection mechanism for copy control use. Indeed, a forensic watermark detection process may require additional tools to aid in ensuring that the signal to be analyzed is in appropriate scale or size, ensuring signal characteristics and heuristic methods help in appropriate recovery of the digital watermark. Simply, all aspects of the underlying content signal should be considered in the embedding process because the watermarking process must take into account all such aspects, including for example, any dimensional or size of the underlying content signal. The dimensions of the content signal may be saved with the key or key pair, without enabling reproduction of the unwatermarked signal. Heuristic methods may be used to ensure the signal is in proper dimensions for a thorough and accurate detection authentication and retrieval of the embedded watermark bits. Data reduction can assist in increasing operations of this nature as well, since the data reduction process may include information about the original signal, for example, signal characteristics, signal abstracts, differences between samples, signal patterns, and related work in restoring any given analog waveform.

The present invention provides benefits, not only because of the key-based approach to the watermarking, but the vast increase in performance and security afforded the implementations of the present invention over the performance of other systems.

The architecture of key and key-pair based watermarking is superior to statistical approaches for watermark detection because the first method meets an evidentiary level of quality and are mathematically provable. By incorporating a level

of data reduction, key and key paired based watermarking is further improved. Such levels of security are plainly necessary if digital watermarks are expected to establish responsibility for copies of copyrighted works in evidentiary proceedings. More sophisticated measures of trust are necessary for use in areas which exceed the scope of copyright but are more factually based in legal proceedings. These areas may include text authentication or software protection (extending into the realm of securing microchip designs and compiled hardware as well) in the examples provided above and are not contemplated by any disclosure or work in the art.

The present invention may be implemented with a variety of cryptographic protocols to increase both confidence and security in the underlying system. A predetermined key is described as a set of masks: a plurality of mask sets. These masks may include primary, convolution and message delimiters but may extend into additional domains. In previous disclosures, the functionality of these masks is defined solely for mapping. Public and private keys may be used as key pairs to further increase the unlikeliness that a key may be compromised. Examples of public key cryptosystems may be found in the following U.S. Patents Nos: 4,200,770; 4,218,582; 4,405,829; and 4,424,414, which examples are incorporated herein by reference. Prior to encoding, the masks described above are generated by a cryptographically secure random generation process. Mask sets may be limited only by the number of dimensions and amount of error correction or concealment sought, as has been previously disclosed.

A block cipher, such as DES, in combination with a sufficiently random seed value emulates a cryptographically secure random bit generator. These keys, or key pairs, will be saved along with information matching them to the sample stream in question in a database for use in subsequent detection or decode operation. These same cryptographic protocols may be combined with the embodiments of the present invention in administering streamed content that requires authorized keys to correctly display or play said streamed content in an unscrambled manner. As with digital watermarking, symmetric or asymmetric public key pairs may be used in a variety of

implementations. Additionally, the need for certification authorities to maintain authentic key-pairs becomes a consideration for greater security beyond symmetric key implementations, where transmission security is a concern.

Signal Processing in a Multi-watermark System (A Plurality of Streams May Be Watermarked)

FIG. 2 illustrates a system and method of implementing a multiple-watermark system. An input signal 11 (e.g., binary executable code, instruction text. or other data), is first processed by a lossy data-reduction scheme 200 (e.g., down-sampling, bit-rate reduction, or compression method) to produced a data-reduced signal 40. Data-reduced signal 40 is then embedded with a watermark (process step 300) to generate a watermarked, data-reduced signal 50, while a copy of the unmarked, data-reduced signal 40 is saved.

The saved, unwatermarked data-reduced signal (signal 40) is subtracted from the original input signal 11, yielding a remainder signal 60 composed only of the data that was lost during the data-reduction. A second watermark is then applied (process step 301) to remainder signal 60 to generate a watermarked remainder signal 70. Finally, the watermarked remainder 70 and the watermarked, data-reduced signal 50 are added to form an output signal 80, which is the final, full-bandwidth, output signal.

The two watermarking techniques (process steps 300 and 301) may be identical (i.e., be functionally the same), or they may be different.

To decode the signal, a specific watermark is targeted. Duplicating the data-reduction processes that created the watermark in some cases can be used to recover the signal that was watermarked. Depending upon the data-reduction method, it may or may not be necessary to duplicate the data-reduction process in order to read a watermark embedded in a remainder signal. Because of the data-reduction, the decoding search can occur much faster than it would in a full-bandwidth signal. Detection speed of the remainder watermark remains the same as if there were no other watermark present.

FIG. 4 illustrates a functional block diagram for one means of decoding the output signal generated by the system illustrated in FIG. 2. A signal to be analyzed 80 (e.g., the same output from FIG. 2) is processed by a data-reduction scheme 200. Data reduced signal 41 can then be decoded to remove the message that was watermarked in the original data reduced signal. Further, data reduced signal 41 can be subtracted from signal to be analyzed 80 to form a differential signal 61 which can then be decoded to remove the message that was watermarked in the original remainder signal. A decoder may only be able to perform one of the two decodings. Differential access and/or different keys may be necessary for each decoding.

Additionally, the watermarking described in connection with this embodiment above may be done with a plurality of predetermined keys or key pairs associated with a single watermark "message bit," code object, or text.

Signal Processing in a Single Watermark System

FIG. 3 illustrates a system and method of implementing a single watermark system. The process and system contemplated here is identical to process described in connection to FIG. 2, above, except that no watermark is embedded in the remainder signal. Hence, the watermarked, data-reduced signal 50 is added directly to the remainder signal 60 to generate an output signal 90. Additionally, the watermarking described in connection with this embodiment above may be done with a plurality of predetermined keys or key pairs associated with a single watermark "message bit," code object, or text.

In either process, an external key can be used to control the insertion location of either watermark. In a copy-control system, a key is not generally used, whereas in a forensic system, a key must be used. The key can also control the parameters of the data-reduction scheme. The dual scheme can allow a combination of copy-control and forensic watermarks in the same signal. A significant feature is that the copy-control watermark can be read and rewritten without affecting the forensic mark or compromising its security.

FIG. 5 illustrates a functional block diagram for one means of decoding the output signal generated by the system illustrated in FIG. 3. A signal to be analyzed 90 (e.g., the same output from FIG. 3) is processed by a data-reduction scheme 200. Data reduced signal 41 can then be decoded to remove the message that was watermarked in the original data reduced signal.

Signal Processing in a Multi-scrambler System (A Plurality of Streams May Be Scrambled)

FIG. 6 illustrates a system and method of implementing a multi-scrambler system. An input signal 12 (e.g., binary executable code, instruction text. or other data), is first processed by a lossy data-reduction scheme 400 (e.g., down-sampling, bit-rate reduction, or compression method) to produced a data-reduced signal 45. Data-reduced signal 45 is then scrambled using a first scrambling technique (process step 500) to generate a scrambled, data-reduced signal 55, while a copy of the unscrambled, data-reduced signal 45 is saved.

The saved, unscrambled data-reduced signal (signal 45) is subtracted from the original input signal 12, yielding a remainder signal 65 composed only of the data that was lost during the data-reduction. A second scrambling technique is then applied (process step 501) to remainder signal 65 to generate a scrambled remainder signal 75. Finally, the scrambled remainder signal 75 and the scrambled data-reduced signal 55 are added to form an output signal 85, which is the final, full-bandwidth, output signal.

The two scrambling techniques (process steps 500 and 501) may be identical (i.e., be functionally the same), or they may be different.

Additionally the scrambling described in connection with this embodiment may be done with a plurality of predetermined keys or key pairs associated with a single scrambling operation containing only a "message bit," code object, or text.

To decode the signal, unscrambling follows the exact pattern of the scrambling process except that the inverse of the scrambling transfer function is applied to each portion of the data, thus returning it to its pre-scrambled state.

FIG. 8 illustrates a functional block diagram for one means of decoding the output signal generated by the system illustrated in FIG. 6. A signal to be analyzed 85 (e.g., the same output from FIG. 6) is processed by a data-reduction scheme 200. Data reduced signal 46 can be subtracted from signal to be analyzed 85 to form a differential signal 66, which signal can then be descrambled in process 551 using the inverse transfer function of the process that scrambled the original remainder signal (e.g., the inverse of scrambling process 501). Descrambling process 551 generates an descrambled signal 76. Data reduced signal 46 may further be descrambled in process 550 using the inverse transfer function of the process that scrambled the original data reduced signal (e.g., the inverse of scrambling process 500). Descrambling process 550 generates an descrambled signal 56, which may then be added to descrambled signal 76 to form an output signal 98.

Signal Processing in a Single Scrambling Operation

FIG. 7 illustrates a system and method of implementing a single scrambling system. The process and system contemplated here is identical to process described in connection to FIG. 6, above, except that no scrambling is applied to the remainder signal. Hence, the scrambled data-reduced signal 55 is added directly to the remainder signal 65 to generate an output signal 95.

Additionally the scrambling described in connection with this embodiment may be done with a plurality of predetermined keys or key pairs associated with a single scrambling operation containing only a "message bit," code object, or text.

FIG. 9 illustrates a functional block diagram for one means of decoding the output signal generated by the system illustrated in FIG. 7. A signal to be analyzed 95 (e.g., the same output from FIG. 7) is processed by a data-reduction scheme 200. Data reduced signal 46 can be subtracted from signal to be analyzed 95 to form a differential

signal 66. Data reduced signal 46 may further be descrambled in process 550 using the inverse transfer function of the process that scrambled the original data reduced signal (e.g., the inverse of scrambling process 500). Descrambling process 550 generates an descrambled signal 56, which may then be added to differential signal 66 to form an output signal 99.

Sample Embodiment: Combinations

Another embodiment may combine both watermarking and scrambling with data reduction. Speed, performance and computing power may influence the selection of which techniques are to be used. Decisions between data reduction schemes ultimately must be measured against the types of keys or key pairs to use, the way any pseudo random or random number generation is done (chaotic, quantum or other means), and the amount of scrambling or watermarking that is necessary given the needs of the system.

It is quite possible that some derived systems would yield a fairly large decision tree, but the present invention offers many benefits to applications in security that are not disclosed in the art.

Conclusions

Data signals fall into two categories: those which can undergo lossy data reduction and remain functional and those which cannot. Audio, images, video are examples of the first. Computer code is an example of the second. In general, all members of the first category contain an aesthetic component, which may be reduced and/or manipulated during a data reduction, in addition to a functional component which serves to identify the signal. For example, an audio signal may have noise added while still remaining recognizably identifiable as a particular song. However, beyond a certain point, the addition of more noise will cause the signal to become unidentifiable, thus impairing the functional character of the signal. In the absence of

an aesthetic component, as with computer code where every bit of data is necessary, lossy compression that retains functionality is not possible.

Signals in the first category are the only candidates for watermarking. A watermark is a distortion of the aesthetic component, generally of an imperceptible nature. This category will gain speed benefits during the watermark decoding process when a lossy data-reduction method is used as described above.

Scrambling, on the other hand, may be applied to any signal, regardless of its aesthetic component, since it allows for perfect reconstruction of the original signal. A scrambling system can be made more secure by applying a data reduction method prior to scrambling, even if this data reduction makes the intermediate signals non-functional, as is the case with signals in category two.

Data reduction can make both watermarking and scrambling more secure. Data reduction can also speed the decoding process for watermarks. Finally, data reduction can allow natural channelization of watermarks for different purposes.

While the invention has been particularly shown and described in the foregoing detailed description, it will be understood by those skilled in the art that various other changes in form and detail may be made without departing from the spirit and scope of the invention.

WHAT IS CLAIMED IS:

1. A method of securing a data signal comprising:

applying a data reduction technique to reduce the data signal into a reduced data signal;

subtracting said reduced data signal from the data signal to produce a remainder signal;

embedding a first watermark into said reduced data signal to produce a watermarked, reduced data signal;

embedding a second watermark into said remainder signal to produce a watermarked remainder signal; and

adding said watermarked, reduced data signal to said watermarked remainder signal to produce an output signal.

2. The method of claim 1 wherein the step of subtracting is comprised of

storing a copy of the data signal; and

subtracting said reduced data signal from the copy of the data signal to produce a remainder signal.

3. The method of claim 1, wherein at least one of the watermarks is embedded using at least one key.

4. The method of claim 1, wherein at least one of the watermarks is embedded using a key pair.

5. The method of claim 4, wherein one key of the key pair is publicly available while the other key of the key pair is secret.

6. A method of protecting a data signal comprising:

applying a data reduction technique to reduce the data signal into a reduced data signal;

subtracting said reduced data signal from the data signal to produce a remainder signal;

embedding a first watermark into said reduced data signal to produce a watermarked, reduced data signal; and

adding said watermarked, reduced data signal to said remainder signal to produce an output signal.

7. The method of claim 6 wherein the step of adding said watermarked, reduced data signal to said remainder signal comprises:

embedding a second watermark into said remainder signal to produce a watermarked remainder signal; and

adding said watermarked, reduced data signal to said watermarked remainder signal to produce an output signal.

8. The method of claim 7, wherein at least one of the watermarks is embedded using at least one key.

9. The method of claim 7, wherein at least one of the watermarks is embedded using a key pair.

10. The method of claim 9, wherein one key of the key pair is publicly available while the other key of the key pair is secret.

11. A method of protecting a data signal:

applying a data reduction technique to reduce the data signal into a reduced data signal;

subtracting said reduced data signal from the data signal to produce a remainder signal;

using a first scrambling technique to scramble said reduced data signal to produce a scrambled, reduced data signal;

using a second scrambling technique to scramble said remainder signal to produce a scrambled remainder signal; and

adding said scrambled, reduced data signal to said scrambled remainder signal to produce an output signal.

12. The method of claim 11 wherein said first and second scrambling techniques are identical.

13. A method of securing a data signal comprising:

applying a data reduction technique to reduce the data signal into a reduced data signal;

subtracting said reduced data signal from the data signal to produce a remainder signal;

using a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal;

using a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal; and

adding said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.

14. The method of claim 13 wherein said first and second cryptographic techniques are identical.

15. The method of claim 13 wherein at least one of said first and second cryptographic techniques is a watermarking technique.

16. The method of claim 15, wherein at least one of the watermarks is embedded using at least one key.

17. The method of claim 15, wherein at least one of the watermarks is embedded using a key pair.

18. The method of claim 13 wherein at least one of said first and second cryptographic techniques is a scrambling technique.

19. The method of claim 13 wherein one of said first and second cryptographic techniques is a watermarking technique and the other is a scrambling technique.

20. The method of claim 13 wherein said first and second cryptographic techniques are identical.

21. A system for securing a data signal comprising:

means to apply a data reduction technique to reduce the data signal into a reduced data signal;

means to subtract said reduced data signal from the data signal to produce a remainder signal;

means to apply a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal;

means to apply a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal; and

means to add said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.

22. The system of claim 21 wherein said first and second cryptographic techniques are identical.

23. The system of claim 21 wherein at least one of said means to apply a first and second cryptographic technique utilizes a watermarking technique.

24. The system of claim 21 wherein at least one of said means to apply a first and second cryptographic technique utilizes a scrambling technique.

25. The system of claim 13 wherein said means to apply a first cryptographic technique is a means to apply a watermarking technique and said means to apply a second cryptographic technique is a means to apply a scrambling technique.

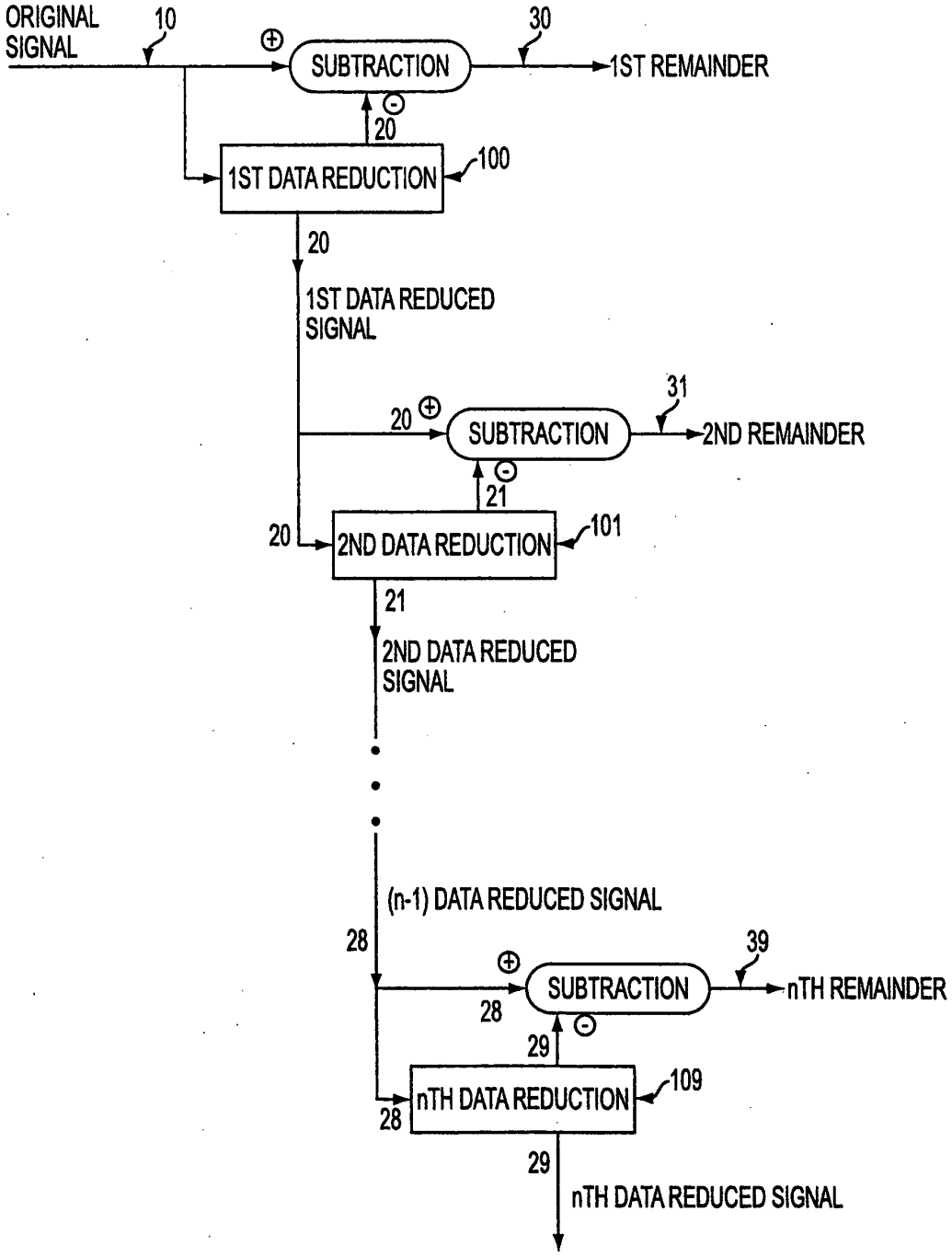


FIG. 1

DISH-Blue Spike-842
Exhibit 1004, Page 0860

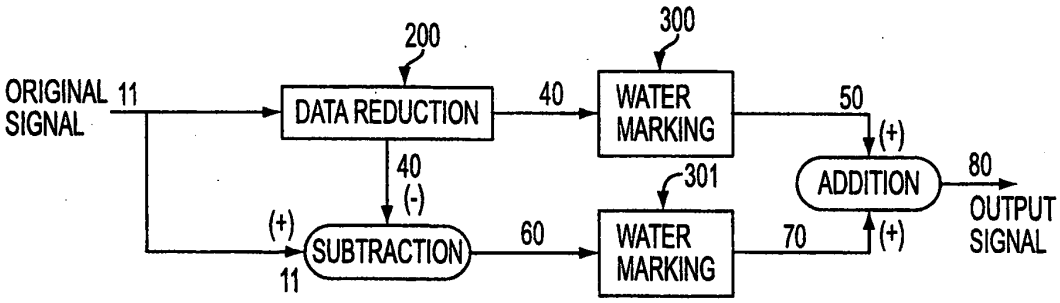

ORIGINAL SIGNAL
11
200
DATA REDUCTION
40
300
WATER MARKING
50
(+)
ADDITION
80
OUTPUT SIGNAL
40
(-)
301
(+)
SUBTRACTION
60
WATER MARKING
70
(+)
11

FIG. 2

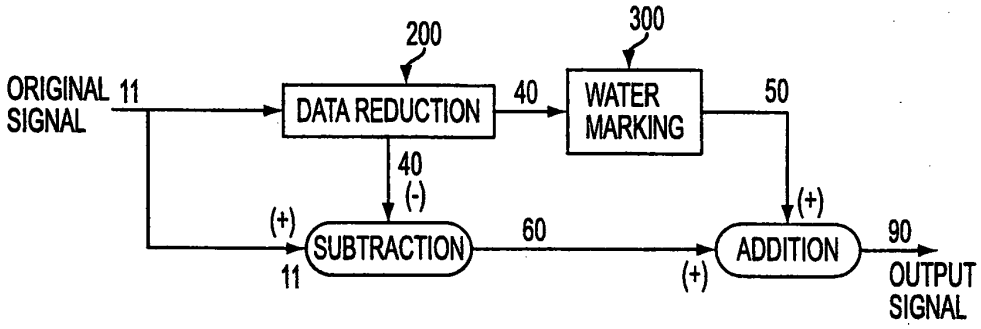

ORIGINAL SIGNAL
11
200
DATA REDUCTION
40
300
WATER MARKING
50
40
(-)
(+)
(+)
SUBTRACTION
60
ADDITION
90
OUTPUT SIGNAL
11
(+)

FIG. 3

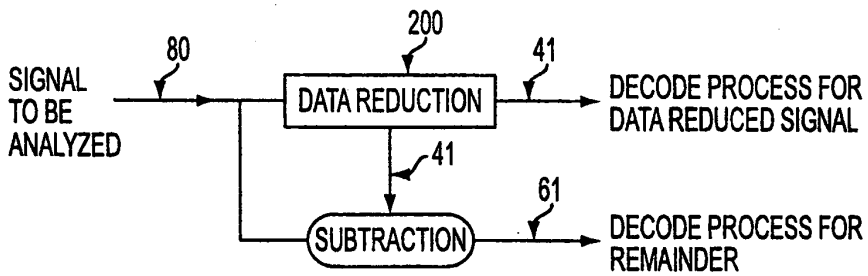

200
80
41
SIGNAL TO BE ANALYZED
DATA REDUCTION
DECODE PROCESS FOR DATA REDUCED SIGNAL
41
61
SUBTRACTION
DECODE PROCESS FOR REMAINDER

FIG. 4

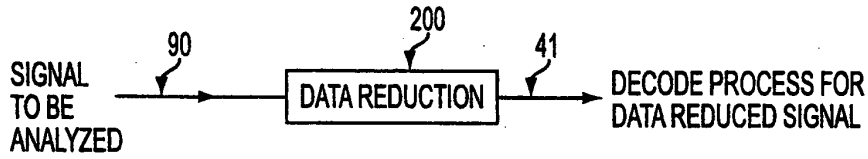

200
90
41
SIGNAL TO BE ANALYZED
DATA REDUCTION
DECODE PROCESS FOR DATA REDUCED SIGNAL

FIG. 5

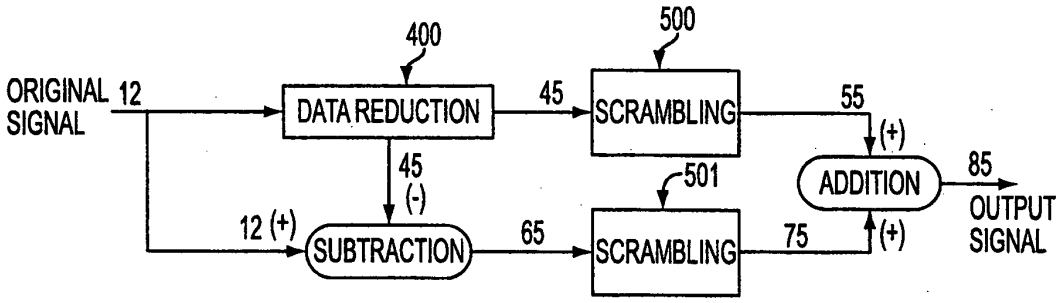

400
500
ORIGINAL SIGNAL
12
DATA REDUCTION
45
SCRAMBLING
55
(+)
45
(-)
501
ADDITION
85
OUTPUT SIGNAL
12 (+)
SUBTRACTION
65
SCRAMBLING
75
(+)

FIG. 6

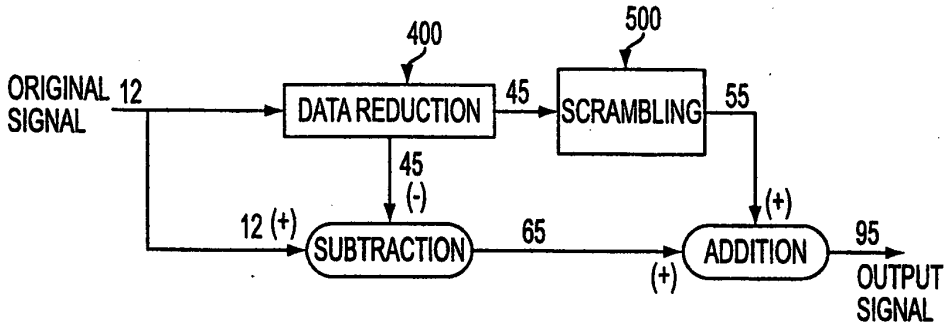

400
500
ORIGINAL SIGNAL
12
DATA REDUCTION
45
SCRAMBLING
55
45
(-)
(+)
12 (+)
SUBTRACTION
65
ADDITION
95
(+)
OUTPUT SIGNAL

FIG. 7

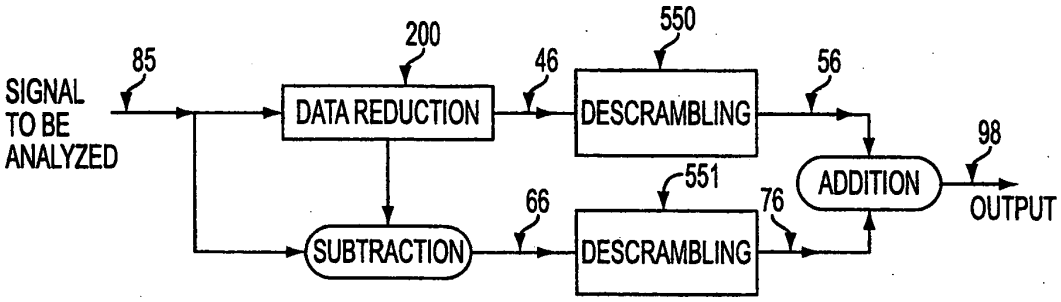

SIGNAL TO BE ANALYZED
85
200
DATA REDUCTION
46
550
DESCRAMBLING
56
98
ADDITION
OUTPUT
66
SUBTRACTION
551
DESCRAMBLING
76

FIG. 8

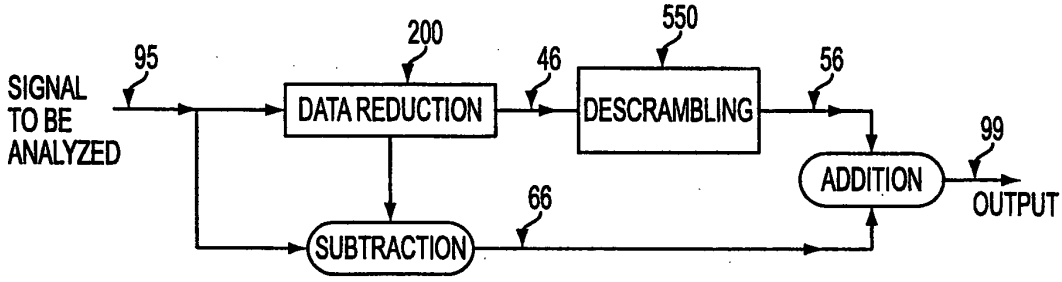

SIGNAL TO BE ANALYZED
95
200
DATA REDUCTION
46
550
DESCRAMBLING
56
99
ADDITION
OUTPUT
66
SUBTRACTION

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/06522

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04N 7/167
US CL : 713/176
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/200,206,207,237,238; 705/54; 704/216-218, 226-228, 500, 501, 503,504; 713/176; 360/49; 348/461, 462

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Watermark Digest: Art Unit 2767

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

IEEE, EAST, Internet, Dialog

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,E	US 6,061,793 A [TEWFIK et al.] 09 MAY 2000, Entire Document	1-25
X	US 5,809,139 A [GIROD et al.] 15 SEPTMBER 1998, Entire Document	1-25
X	US 5,848,155 A [COX] 08 DECEMBER 1998, Entire Document	1-25
A,P	US 5,889,868 A [MOSKOWITZ et al.] 30 MARCH 1999, Entire Document	1-25
A,P	US 5,915,027 A [COX et al.] 22 JUNE 1999, Entire Document	1-25
A,P	US 5,940,134 A [WIRTZ] 17 AUGUST 1999, Entire Document	1-25

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
30 JUNE 2000	18 AUG 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer PAUL E. CALLAHAN Telephone No. (703) 305-1338

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/06522

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 5,991,426 A [COX et al.] 23 NOVEMBER 1999, Entire Document	1-25
A,E	US 6,069,914 A [COX] 30 MAY 2000, Entire Document	1-25
A,P	US 5,943,422 A [VAN WIE et al.] 24 AUGUST 1999, Entire Document	1-25

Form PCT/ISA/210 (continuation of second sheet) (July 1998)*

European Patent Office

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 00 91 9398

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 98 37513 A (TELSTRA R & D MAN PTY LTD ;BIGGAR MICHAEL (AU); JOHNSON ANDREW (AU) 27 August 1998 (1998-08-27) * page 6, line 25 - page 7, line 10 *	6	H04N7/167 H04N7/26 H04N1/32 G06F17/30
Y	US 4 969 204 A (MELNYCHUCK PAUL W ET AL) 6 November 1990 (1990-11-06) * column 2, line 9 - column 2, line 48 *	1-10	
Y	EP 0 651 554 A (EASTMAN KODAK CO) 3 May 1995 (1995-05-03) * column 6, line 43 - column 9, line 19; figure 2 *	1-10	
A	JOHNSON A ET AL: "TRANSFORM PERMUTED WATERMARKING FOR COPYRIGHT PROTECTION OF DIGITAL VIDEO" IEEE GLOBECOM 1998. GLOBECOM '98. THE BRIDGE TO GLOBAL INTEGRATION. SYDNEY, NOV. 8 - 12, 1998, IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, NEW YORK, NY: IEEE, US, vol. 2, 1998, pages 684-689, XP000825846 ISBN: 0-7803-4985-7 * page 685, left-hand column, paragraph 2 - page 685, left-hand column, paragraph 3 *	1-10	
P,X	WO 99 62044 A (HANDEL THEODORE G ;UNIV CALIFORNIA (US); SANDFORD MAXELL T II (US)) 2 December 1999 (1999-12-02) * abstract * * page 4, line 17 - page 5, line 5 *	6	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
H04N
G06F

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search	Date of completion of the search	Examiner
MUNICH	27 June 2002	Schoeyer, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C04)

3

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2002 (10.01.2002)

PCT

(10) International Publication Number
WO 02/03385 A1

(51) International Patent Classification[7]: G11B 20/00, G06F 1/00

(21) International Application Number: PCT/US00/18411

(22) International Filing Date: 5 July 2000 (05.07.2000)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant and
(72) Inventor: **MOSKOWITZ, Scott, A.** [US/US]; 16711 Collins Avenue #2505, Miami, FL 33160 (US).

(74) Agents: **CHAPMAN, Floyd, B.** et al.; Wiley Rein & Fielding, Intellectual Property Department, 1776 K Street, N.W., Washington, DC 20006 (US).

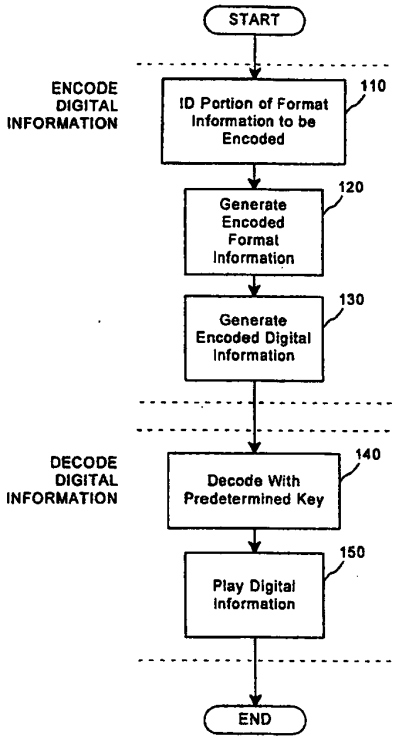
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: COPY PROTECTION OF DIGITAL DATA COMBINING STEGANOGRAPHIC AND CRYPTOGRAPHIC TECHNIQUES



(57) Abstract: A method for combining transfer functions with predetermined key creation. In one embodiment, digital information, including a digital sample and format information, is protected by identifying and encoding a portion of the format information. Encoded digital information, including the digital sample and the encoded format information generated to protect the original digital information. In another embodiment, a digital signal, including digital samples in a file format having an inherent granularity, is protected by creating a predetermined key. The predetermined key is comprised of a transfer function-based mask set to manipulate data at the inherent granularity of the file format of the underlying digitized samples.

WO 02/03385 A1

COPY PROTECTION OF DIGITAL DATA COMBINING STEGANOGRAPHIC AND CRYPTOGRAPHIC TECH NIQUES

BACKGROUND OF THE INVENTION

Increasingly, commercially valuable information is being created and stored in "digital" form. For example, music, photographs and video can all be stored and transmitted as a series of numbers, such as 1's and 0's. Digital techniques let the original information be recreated in a very accurate manner. Unfortunately, digital techniques also let the information be easily copied without the information owner's permission.

Because unauthorized copying is clearly a disincentive to the digital distribution of valuable information, it is important to establish responsibility for copies and derivative copies of such works. For example, if each authorized digital copy of a popular song is identified with a unique number, any unauthorized copy of the song would also contain the number. This would allow the owner of the information, such as a song publisher, to investigate who made the unauthorized copy. Unfortunately, it is possible that the unique number could be erased or altered if it is simply tacked on at the beginning or end of the digital information.

As will be described, known digital "watermark" techniques give creators and publishers of digitized multimedia content localized, secured identification and authentication of that content. In considering the various forms of multimedia content, such as "master," stereo, National Television Standards Committee (NTSC) video, audio tape or compact disc, tolerance of quality will vary with individuals and affect the underlying commercial and aesthetic value of the content. For example, if a digital version of a popular song sounds distorted, it will be less valuable to users. It is therefore desirable to embed copyright, ownership or purchaser information, or some combination of these and related data, into the content in a way that will damage the content if the watermark is removed without authorization.

To achieve these goals, digital watermark systems insert ownership information in a way that causes little or no noticeable effects, or "artifacts," in the underlying content signal. For example, if a digital watermark is inserted into a

digital version of a song, it is important that a listener not be bothered by the slight changes introduced by the watermark. It is also important for the watermark technique to maximize the encoding level and "location sensitivity" in the signal to force damage to the content signal when removal is attempted. Digital watermarks address many of these concerns, and research in the field has provided extremely robust and secure implementations.

What has been overlooked in many applications described in the art, however, are systems which closely mimic distribution of content as it occurs in the real world. For instance, many watermarking systems require the original un-watermarked content signal to enable detection or decode operations. These include highly publicized efforts by NEC, Digimarc and others. Such techniques are problematic because, in the real world, original master copies reside in a rights holders vaults and are not readily available to the public.

With much activity overly focused on watermark survivability, the security of a digital watermark is suspect. Any simple linear operation for encoding information into a signal may be used to erase the embedded signal by inverting the process. This is not a difficult task, especially when detection software is a plug-in freely available to the public, such as with Digimarc. In general, these systems seek to embed cryptographic information, not cryptographically embed information into target media content.

Other methods embed ownership information that is plainly visible in the media signal, such as the method described in US Patent No. 5,530,739 to Braudaway et al. The system described in Braudaway protects a digitized image by encoding a visible watermark to deter piracy. Such an implementation creates an immediate weakness in securing the embedded information because the watermark is plainly visible. Thus, no search for the embedded signal is necessary and the watermark can be more easily removed or altered. For example, while certainly useful to some rights owners, simply placing the symbol "©" in the digital information would only provide limited protection. Removal by adjusting the brightness of the pixels forming the "©" would not be difficult with respect to the computational resources required.

Other relevant prior art includes US Patents No. 4,979,210 and 5,073,925 to Nagata et al., which encodes information by modulating an audio signal in the amplitude/time domain. The modulations introduced in the Nagata process carry a "copy/don't copy" message, which is easily found and circumvented by one skilled in the art. The granularity of encoding is fixed by the amplitude and frequency modulation limits required to maintain inaudibility. These limits are relatively low, making it impractical to encode more information using the Nagata process.

Although US Patent No. 5,664,018 to Leighton describes a means to prevent collusion attacks in digital watermarks, the disclosed method may not actually provide the security described. For-example, in cases where the watermarking technique is linear, the "insertion envelope" or "watermarking space" is well-defined and thus susceptible to attacks less sophisticated than collusion by unauthorized parties. Over-encoding at the watermarking encoding level is but one simple attack in such linear implementations. Another consideration not made by Leighton is that commercially-valuable content may already exist in a un-watermarked form somewhere, easily accessible to potential pirates, gutting the need for any type of collusive activity. Digitally signing the embedded signal with preprocessing of watermark data is more likely to prevent successful collusion. Furthermore, a "baseline" watermark as disclosed is quite subjective. It is simply described elsewhere in the art as the "perceptually significant" regions of a signal. Making a watermarking function less linear or inverting the insertion of watermarks would seem to provide the same benefit without the additional work required to create a "baseline" watermark. Indeed, watermarking algorithms should already be capable of defining a target insertion envelope or region without additional steps. What is evident is the Leighton patent does not allow for initial prevention of attacks on an embedded watermark as the content is visibly or audibly unchanged.

It is also important that any method for providing security also function with broadcasting media over networks such as the Internet, which is also referred to as "streaming." Commercial "plug-in" products such as RealAudio and RealVideo, as well as applications by vendors VDONet and Xtreme, are common in such network environments. Most digital watermark implementations focus on

common file base signals and fail to anticipate the security of streamed signals. It is desirable that any protection scheme be able to function with a plug-in player without advanced knowledge of the encoded media stream.

Other technologies focus solely on file-based security. These technologies illustrate the varying applications for security that must be evaluated for different media and distribution environments. Use of cryptolopes or cryptographic containers, as proposed by IBM in its Cryptolope product, and InterTrust, as described in U.S. Patents No. 4,827,508, 4,977,594, 5,050,213 and 5,410,598, may discourage certain forms of piracy. Cryptographic containers, however, require a user to subscribe to particular decryption software to decrypt data. IBM's InfoMarket and InterTrust's DigiBox, among other implementations, provide a generalized model and need proprietary architecture to function. Every user must have a subscription or registration with the party which encrypts the data. Again, as a form of general encryption, the data is scrambled or encrypted without regard to the media and its formatting. Finally, control over copyrights or other neighboring rights is left with the implementing party, in this case, IBM, InterTrust or a similar provider. Methods similar to these "trusted systems" exist, and Cerberus Central Limited and Liquid Audio, among a number of companies, offer systems which may functionally be thought of as subsets of IBM and InterTrust's more generalized security offerings. Both Cerberus and Liquid Audio propose proprietary player software which is registered to the user and "locked" in a manner parallel to the locking of content that is distributed via a cryptographic container. The economic trade-off in this model is that users are required to use each respective companies' proprietary player to play or otherwise manipulate content that is downloaded. If, as is the case presently, most music or other media is not available via these proprietary players and more companies propose non-compatible player formats, the proliferation of players will continue. Cerberus and Liquid Audio also by way of extension of their architectures provide for "near-CD quality" but proprietary compression. This requirement stems from the necessity not to allow content that has near-identical data make-up to an existing consumer electronic standard, in Cerberus and Liquid Audio's case the so-called Red Book audio CD standard of 16 bit 44.1 kHz, so that comparisons with the proprietary file may not

yield how the player is secured. Knowledge of the player's file format renders its security ineffective as a file may be replicated and played on any common player, not the intended proprietary player of the provider of previously secured and uniquely formatted content. This is the parallel weakness to public key crypto-systems which have gutted security if enough plain text and cipher text comparisons enable a pirate to determine the user's private key.

Many approaches to digital watermarking leave detection and decoding control with the implementing party of the digital watermark, not the creator of the work to be protected. A set of secure digital watermark implementations address this fundamental control issue forming the basis of key-based approaches. These are covered by the following patents and pending applications, the entire disclosures of which are hereby incorporated by reference: US Patent No. 5,613, 004 entitled "Steganographic Method and Device" and its derivative US patent application Serial No. 08/775,216, US patent application Serial No. 08/587,944 entitled "Human Assisted Random Key Generation and Application for Digital Watermark System," US Patent Application Serial No. 08/587,943 entitled "Method for Stega-Cipher Protection of Computer Code," US patent application Serial No. 08/677,435 entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data," and US Patent Application Serial No. 08/772,222 entitled "Z-Transform Implementation of Digital Watermarks." Public key crypto-systems are described in US Patents No. 4,200,770, 4,218,582, 4,405,829 and 4,424,414, the entire disclosures of which are also hereby incorporated by reference.

In particular, an improved protection scheme is described in "Method for Stega-Cipher Protection of Computer Code," US patent application Serial No. 08/587,943. This technique uses the key-based insertion of binary executable computer code within a content signal that is subsequently, and necessarily, used to play or otherwise manipulate the signal in which it is encoded. With this system, however, certain computational requirements, such as one digital player per digital copy of content, may be necessitated. For instance, a consumer may download many copies of watermarked content. With this technique, the user would also be downloading as many copies of the digital player program. While this form of

security may be desirable for some applications, it is not appropriate in many circumstances. Finally, even when digital information is distributed in encoded form, it may be desirable to allow unauthorized users to play the information with a digital player, perhaps with a reduced level of quality. For example, a popular song may be encoded and freely distributed in encoded form to the public. The public, perhaps using commonly available plug-in digital players, could play the encoded content and hear the music in some degraded form. The music may sound choppy, or fuzzy or be degraded in some other way. This lets the public decide, based on the available lower quality version of the song, if they want to purchase a key from the publisher to decode, or "clean-up," the content. Similar approaches could be used to distribute blurry pictures or low quality video. Or even "degraded" text, in the sense that only authenticated portions of the text can be determined with the predetermined key or a validated digital signature for the intended message.

In view of the foregoing, it can be appreciated that a substantial need exists for a method allowing encoded content to be played, with degraded quality, by a plug-in digital player, and solving the other problems discussed above.

SUMMARY OF THE INVENTION

The disadvantages of the art are alleviated to a great extent by a method for combining transfer functions with predetermined key creation. In one embodiment, digital information, including a digital sample and format information, is protected by identifying and encoding a portion of the format information. Encoded digital information, including the digital sample and the encoded format information, is generated to protect the original digital information.

In another embodiment, a digital signal, including digital samples in a file format having an inherent granularity, is protected by creating a predetermined key. The predetermined key is comprised of a transfer function-based mask set to manipulate data at the inherent granularity of the file format of the underlying digitized samples.

With these and other advantages and features of the invention that will become hereinafter apparent, the nature of the invention may be more clearly understood by reference to the following detailed description of the invention, the appended claims and to the several drawings attached herein.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block flow diagram of a method for copy protection or authentication of digital information according to an embodiment of the present invention.

DETAILED DESCRIPTION

In accordance with an embodiment of the present invention, a method combines transfer functions with predetermined key creation. Increased security is achieved in the method by combining elements of "public-key steganography" with cryptographic protocols, which keep in-transit data secure by scrambling the data with "keys" in a manner that is not apparent to those with access to the content to be distributed. Because different forms of randomness are combined to offer robust, distributed security, the present invention addresses an architectural "gray space" between two important areas of security: digital watermarks, a subset of the more general art of steganography, and cryptography. One form of randomness exists in the mask sets that are randomly created to map watermark data into an otherwise unrelated digital signal. The second form of-randomness is the random permutations of data formats used with digital players to manipulate the content with the predetermined keys. These forms can be thought of as the transfer function versus the mapping function inherent to digital watermarking processes.

According to an embodiment of the present invention, a predetermined, or randomly generated, key is used to scramble digital information in a way that is unlike known "digital watermark" techniques and public key crypto-systems. As used herein, a key is also referred to as a "mask set" which includes one or more random or pseudo-random series of bits. Prior to encoding, a mask can be generated by any cryptographically secure random generation process. A block cipher, such as a Data Encryption Standard (DES) algorithm, in combination with a sufficiently random seed value, such as one created using a Message Digest 5 (MD5) algorithm, emulates a cryptographically secure random bit generator. The keys are saved in a database, along with information matching them to the digital signal, for use in descrambling and subsequent viewing or playback. Additional file format or transfer property information is prepared and made available to the encoder, in a bit addressable manner. As well, any authenticating function can be

combined, such as Digital Signature Standard (DSS) or Secure Hash Algorithm (SHA).

Using the predetermined key comprised of a transfer function-based mask set, the data representing the original content is manipulated at the inherent granularity of the file format of the underlying digitized samples. Instead of providing, or otherwise distributing, watermarked content that is not noticeably altered, a partially "scrambled" copy of the content is distributed. The key is necessary both to register the sought-after content and to descramble the content into its original form.

The present invention uses methods disclosed in "Method for Stega-Cipher Protection of Computer Code," US Patent Application Serial No. 08/587,943, with respect to transfer functions related to the common file formats, such as PICT, TIFF, AIFF, WAV, etc. Additionally, in cases where the content has not been altered beyond being encoded with such functional data, it is possible for a digital player to still play the content because the file format has not been altered. Thus, the encoded content could still be played by a plug-in digital player as discrete, digitally sampled signals, watermarked or not. That is, the structure of the file can remain basically unchanged by the watermarking process, letting common file format based players work with the "scrambled" content.

For example, the Compact Disc-Digital Audio (CD-DA) format stores audio information as a series of frames. Each frame contains a number of digital samples representing, for example, music, and a header that contains file format information. As shown in FIG. 1, according to an embodiment of the present invention some of the header information can be identified and "scrambled" using the predetermined key at steps 110 to 130. The music samples can remain unchanged. Using this technique, a traditional CD-DA player will be able to play a distorted version of the music in the sample. The amount of distortion will depend on the way, and extent, that the header, or file format, information has been scrambled. It would also be possible to instead scramble some of the digital samples while leaving the header information alone. In general, the digital signal would be protected by manipulating data at the inherent granularity, or "frames," of the CD-

DA file format. To decode the information, a predetermined key is used before playing the digital information at steps 140 and 150.

A key-based decoder can act as a "plug-in" digital player of broadcast signal streams without foreknowledge of the encoded media stream. Moreover, the data format orientation is used to partially scramble data in transit to prevent unauthorized descrambled access by decoders that lack authorized keys. A distributed key can be used to unscramble the scrambled content because a decoder would understand how to process the key. Similar to on-the-fly decryption operations, the benefits inherent in this embodiment include the fact that the combination of watermarked content security, which is key-based, and the descrambling of the data, can be performed by the same key which can be a plurality of mask sets. The mask sets may include primary, convolution and message delimiter masks with file format data included. r

The creation of an optimized "envelope" for insertion of watermarks provides the basis of much watermark security, but is also a complementary goal of the present invention. The predetermined or random key that is generated is not only an essential map to access the hidden information signal, but is also the descrambler of the previously scrambled signal's format for playback or viewing.

In a system requiring keys for watermarking content and validating the distribution of the content, different keys may be used to encode different information while secure one way hash functions or one-time pads may be incorporated to secure the embedded signal. The same keys can be used to later validate the embedded digital signature, or even fully decode the digital watermark if desired. Publishers can easily stipulate that content not only be digitally watermarked but that distributors must check the validity of the watermarks by performing digital signature-checks with keys that lack any other functionality. The system can extend to simple authentication of text in other embodiments.

Before such a market is economically feasible, there are other methods for deploying key-based watermarking coupled with transfer functions to partially scramble the content to be distributed without performing full public key encryption, i.e., a key pair is not necessarily generated, simply, a predetermined key's function is created to re-map the data of the content file in a lossless process.

Moreover, the scrambling performed by the present invention may be more dependent on the file in question. Dissimilarly, encryption is not specific to any particular media but is performed on data. The file format remains unchanged, rendering the file useable by any conventional viewer/player, but the signal quality can be intentionally degraded in the absence of the proper player and key. Public-key encryption seeks to completely obscure the sensitive "plaintext" to prevent comparisons with the "ciphertext" to determine a user's private keys. Centralized encryption only differs in the utilization of a single key for both encryption and decryption making the key even more highly vulnerable to attacks to defeat the encryption process. With the present invention, a highly sought after photograph may be hazy to the viewer using any number of commonly available, nonproprietary software or hardware, without the authorized key. Similarly, a commercially valuable song may sound poor.

The benefit of some form of cryptography is not lost in the present invention. In fact, some piracy can be deterred when the target signal may be known but is clearly being protected through scrambling. What is not anticipated by known techniques, is an ala carte method to change various aspects of file formatting to enable various "scrambled states" for content to be subsequently distributed. An image may lack all red pixels or may not have any of the most significant bits activated. An audio sample can similarly be scrambled to render it less-than-commercially viable.

The present invention also provides improvements over known network-based methods, such as those used for the streaming of media data over the Internet. By manipulating file formats, the broadcast media, which has been altered to "fit" within electronic distribution parameters, such as bandwidth availability and error correction considerations; can be more effectively utilized to restrict the subsequent use of the content while in transit as well as real-time viewing or playing.

The mask set providing the transfer function can be read on a per-use basis by issuing an authorized or authenticating "key" for descrambling the signal that is apparent to a viewer or a player or possessor of the authenticating key. The mask set can be read on a per-computer basis by issuing the authorized key that is

more generalized for the computer that receives the broadcast signals. Metering and subscription models become viable advantages over known digital watermark systems which assist in designating the ownership of a copy of digitized media content, but do not prevent or restrict the copying or manipulation of the sampled signal in question. For broadcast or streamed media, this is especially the case. Message authentication is also possible, though not guaranteeing the same security as an encrypted file as with general crypto systems.

The present invention thus benefits from the proprietary player model without relying on proprietary players. No new players will be necessary and existing multimedia file formats can be altered to exact a measure of security which is further increased when coupled with digital watermarks. As with most consumer markets for media content, predominant file formats exist, de facto, and corresponding formats for computers likewise exist. For a commercial compact disc quality audio recording, or 16 bit 44.1 kHz, corresponding file formats include: Audio Interchange File Format (AIFF), Microsoft WAV, Sound Designer II, Sun's .au, Apple's Quicktime, etc. For still image media, formats are similarly abundant: TIFF, PICT, JPEG, GIF, etc. Requiring the use of additional proprietary players, and their complementary file formats, for limited benefits in security is wasteful. Moreover, almost all computers today are multimedia-capable, and this is increasingly so with the popularity of Intel's MMX chip architecture and the PowerPC line of microchips. Because file formatting is fundamental in the playback of the underlying data, the predetermined key can act both as a map, for information to be encoded as watermark data regarding ownership, and a descrambler of the file that has been distributed. Limitations will only exist in how large the key must be retrofitted for a given application, but any manipulation of file format information is not likely to exceed the size of data required versus that for an entire proprietary player.

As with previous disclosures by the inventor on digital watermarking techniques, the present invention may be implemented with a variety of cryptographic protocols to increase both confidence and security in the underlying system. A predetermined key is described as a set of masks. These masks may include primary, convolution and message delimiter mask. In previous disclosures,

the functionality of these masks is defined solely for mapping. The present invention includes a mask set which is also controlled by the distributing party of a copy of a given media signal. This mask set is a transfer function which is limited only by the parameters of the file format in question. To increase the uniqueness or security of each key used to scramble a given media file copy, a secure one way hash function can be used subsequent to transfer properties that are initiated to prevent the forging of a particular key. Public and private keys may be used as key pairs to further increase the unlikeliness that a key may be compromised.

These same cryptographic protocols can be combined with the embodiments of the present invention in administering streamed content that requires authorized keys to correctly display or play the streamed content in an unscrambled manner. As with digital watermarking, symmetric or asymmetric public key pairs may be used in a variety of implementations. Additionally, the need for certification authorities to maintain authentic key-pairs becomes a consideration for greater security beyond symmetric key implementations. The cryptographic protocols makes possible, as well, a message of text to be authenticated by a message authenticating function in a general computing device that is able to ensure secure message exchanges between authorizing parties.

Although various embodiments are specifically illustrated and described herein, it will be appreciated that modifications and variations of the present invention are covered by the above teachings and within the purview of the appended claims without departing from the spirit and intended scope of the invention.

What is claimed is:

1. A method for copy protection of digital information, the digital information including a digital sample and format information, comprising the steps of:

identifying a portion of the format information to be encoded;

generating encoded format information from the identified portion of the format information; and

generating encoded digital information, including the digital sample and the encoded format information.

2. The method of claim 1, further comprising the step of requiring a predetermined key to decode the encoded format information.

3. The method of claim 2, wherein the digital sample and format information are configured to be used with a digital player, and wherein information output from the digital player will have a degraded quality unless the encoded format information is decoded with the predetermined key.

4. The method of claim 3, wherein the information output from the digital player represents a still image, audio or video.

5. The method of claim 3, wherein the information output represents text data to be authenticated.

6. A method for protecting a digital signal, the digital signal including digital samples in a file format having an inherent granularity, comprising the step of:

creating a predetermined key comprised of a transfer function-based mask set to manipulate data at the inherent granularity of the file format of the underlying digitized samples.

7. The method of claim 6, wherein the digital signal represents a continuous analog waveform.

8. The method of claim 6, wherein the predetermined key comprises a plurality of mask sets.

9. The method of claim 6, wherein the digital signal is a message to be authenticated.

10. The method of claim 6, wherein the mask set is ciphered by a key pair comprising a public key and a private key.

11. The method of claim 6, further comprising the step of:

using a digital watermarking technique to encode information that identifies ownership, use, or other information about the digital signal, into the digital signal.

12. The method of claim 6, wherein the digital signal represents a still image, audio or video.

13. The method of claim 6, further comprising the steps of:

selecting the mask set, including one or more masks having random or pseudo-random series of bits; and

validating the mask set at the start of the transfer function-based mask set.

14. The method of claim 13, wherein said step of validating comprises the step of:

comparing a hash value computed at the start of the transfer function-based mask set with a determined transfer function of the hash value.

15. The method of claim 6, further comprising the steps of:

selecting the mask set, including one or more masks having random or pseudo-random series of bits; and

authenticating the mask set by comparing a hash value computed at the start of the transfer function-based mask set with a determined transfer function of the hash value.

16. The method of claim 13, wherein said step of validating comprises the step of:

comparing a digital signature at the start of the transfer function-based mask set with a determined transfer function of the digital signature.

17. The method of claim 6, further comprising the steps of:

selecting the mask set, including one or more masks having random or pseudo-random series of bits; and

authenticating the mask set by comparing a digital signature at the start of the transfer function-based mask set with a determined transfer function of the digital signature.

18. The method of claim 13, further comprising the step of:

using a digital watermarking technique to embed information that identifies ownership, use, or other information about the digital signal, into the digital signal; and

wherein said step of validating is dependent on validation of the embedded information.

19. The method of claim 6, further comprising the step of:

computing a secure one way hash function of carrier signal data in the digital signal, wherein the hash function is insensitive to changes introduced into the carrier signal for the purpose of carrying the transfer function-based mask set.

20. A method for protecting a digital signal, the digital signal including digital samples in a file format having an inherent granularity, comprising the steps of:

creating a predetermined key comprised of a transfer function-based mask set that can manipulate data at the inherent granularity of the file format of the underlying digitized samples;

authenticating the predetermined key containing the correct transfer function-based mask set during playback of the data; and

metering the playback of the data to monitor content.

21. The method of claim 20, wherein the predetermined key is authenticated to authenticate message information.

22. A method to prepare for the scrambling of a sample stream of data, comprising the steps of:

generating a plurality of mask sets to be used for encoding, including a random primary mask, a random convolution mask and a random start of message delimiter;

obtaining a transfer function to be implemented;

generating a message bit stream to be encoded;

loading the message bit stream, a stega-cipher map truth table, the primary mask, the convolution mask and the start of message delimiter into memory;

initializing the state of a primary mask index, a convolution mask index, and a message bit index; and

setting a message size equal to the total number of bits in the message bit stream.

23. A method to prepare for the encoding of stega-cipher information into a sample stream of data, comprising the steps of:

generating a mask set to be used for encoding, the set including a random primary mask, a random convolution mask, and a random start of message delimiter;

obtaining a message to be encoded;

compressing and encrypting the message if desired;

generating a message bit stream to be encoded;

loading the message bit stream, a stega-cipher map truth table, the primary mask, the convolution mask and the start of message delimiter into memory;

initializing the state of a primary mask index, a convolution mask index, and a message bit index; and

setting the message size equal to the total number of bits in the message bit stream.

24. The method of claim 23 wherein the sample stream of data has a plurality of windows, further comprising the steps of:

calculating over which windows in the sample stream the message will be encoded;

computing a secure one way hash function of the information in the calculated windows, the hash function generating hash values insensitive to changes in the samples induced by a stega-cipher; and

encoding the computed hash values in an encoded stream of data.

25. The method of claim 13, wherein said step of selecting comprises the steps of:

collecting a series of random bits derived from keyboard latency intervals in random typing;

processing the initial series of random bits through an MD5 algorithm;

using the results of the MD5 processing to seed a triple-DES encryption loop;

cycling through the triple-DES encryption loop, extracting the least significant bit of each result after each cycle; and

concatenating the triple-DES output bits into the random series of bits.

26. A method for copy protection of digital information, the digital information including a digital sample and format information, comprising the steps of:

a identifying a portion of the digital sample to be encoded;

generating an encoded digital sample from the identified portion of the digital sample; and

generating encoded digital information, including the encoded digital sample and the format information.

27. The method of claim 26, further comprising the step of requiring a predetermined key to decode the encoded digital sample.

28. The method of claim 27, wherein the digital sample and format information are configured to be used with a digital player, and wherein information output from the digital player will have a degraded quality unless the encoded digital sample is decoded with the predetermined key.

29. The method of claim 27, wherein information output will have non authentic message data unless the encode digital sample is decoded with the predetermined key.

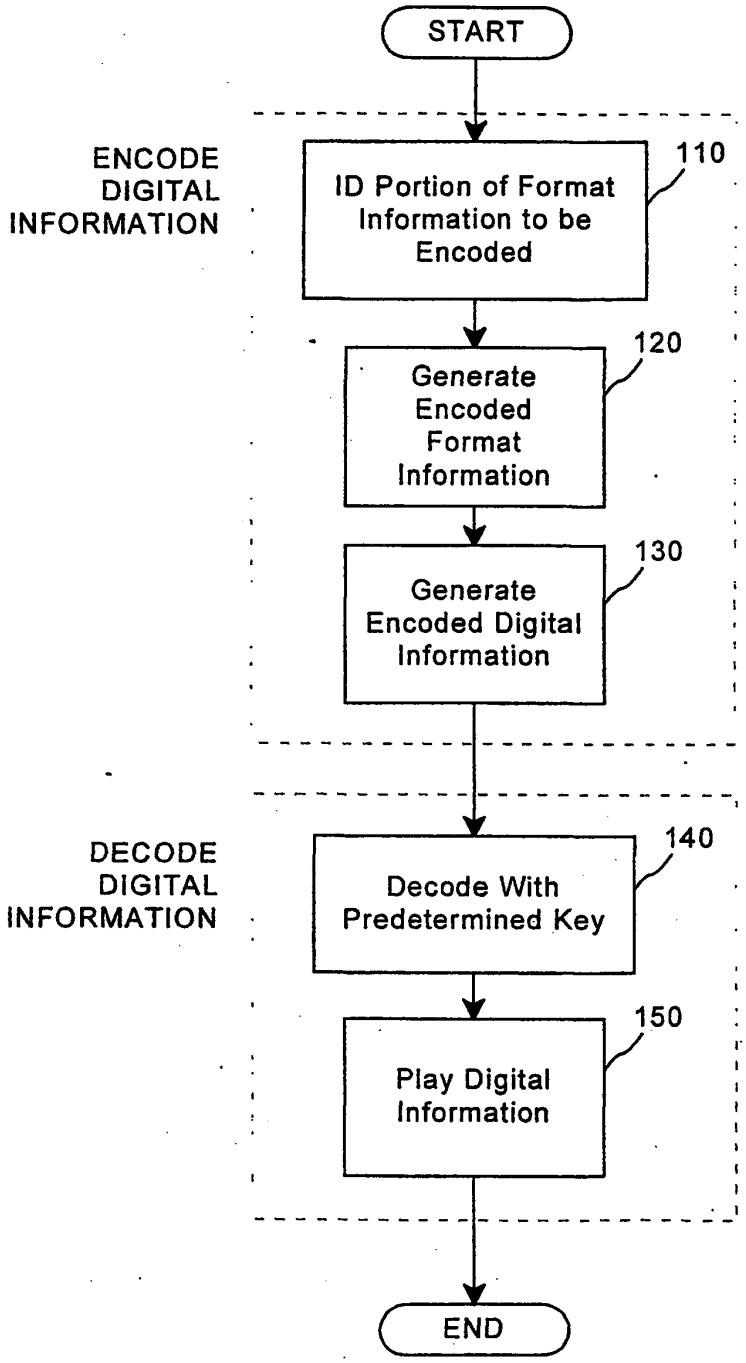

START
ENCODE DIGITAL INFORMATION
ID Portion of Format Information to be Encoded
110
Generate Encoded Format Information
120
Generate Encoded Digital Information
130
DECODE DIGITAL INFORMATION
Decode With Predetermined Key
140
Play Digital Information
150
END

FIG. 1

INTERNATIONAL SEARCH REPORT

	nal Application No PCT/US 00/18411

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B G06F H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	NL 1 005 523 C (EINDHOVEN TECH HOCHSCHULE) 15 September 1998 (1998-09-15) abstract; figure 4 page 1, line 35 -page 3, line 9 page 9, line 21 -page 10, line 5	1,2, 26-29
X	WO 97 44736 A (APPLE COMPUTER) 27 November 1997 (1997-11-27) abstract; figure 4 page 2, line 35 -page 3, line 27 page 9, line 10 -page 11, line 28	1,2
Y		3,4

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2001	30. 07. 2001
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Sigolo, A

Form PCT/ISA/210 (second sheet) (July 1992)

DISH-Blue Spike-842
Exhibit 1004, Page 0887

INTERNATIONAL SEARCH REPORT

tional Application No
PCT/US 00/18411

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 687 236 A (MOSKOWITZ SCOTT A ET AL) 11 November 1997 (1997-11-11) cited in the application column 5, line 1 -column 6, line 37 column 7, line 54 -column 10, line 11 column 11, line 31 -column 12, line 10 column 15, line 42 -column 16, line 32	6-12, 19-21
A		22,23
A	US 5 974 141 A (SAITO MAKOTO) 26 October 1999 (1999-10-26) abstract; figures 4A-4G column 8, line 24 - line 67	5,26
X	WO 99 52271 A (MOSKOWITZ SCOTT A) 14 October 1999 (1999-10-14) abstract page 11, line 15 -page 13, line 13	6,7,10
Y	EP 0 649 261 A (CANON KK) 19 April 1995 (1995-04-19) page 3, line 53 -page 4, line 5 page 7, line 18 - line 23	3,4
A	WO 99 63443 A (DATAMARK TECHNOLOGIES PTE LTD; HO ANTHONY TUNG SHUEN (SG); TAM SIU) 9 December 1999 (1999-12-09) page 2, line 10 -page 5, line 16	6-8,11, 12

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

DISH-Blue Spike-842
Exhibit 1004, Page 0888

INTERNATIONAL SEARCH REPORT

ɪnational application No.
PCT/US 00/18411

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

DISH-Blue Spike-842
Exhibit 1004, Page 0889

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-5,26-29

   Protecting the distribution of digital data to be used with a digital player characterized by encrypting format information and allowing low quality play back in case of lack of decrypting key.

2. Claims: 6-25

   Digital signature encrypting technique combining transfer functions with predetermined key creation.

INTERNATIONAL SEARCH REPORT

Information on patent family members

itional Application No
PCT/US 00/18411

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
NL 1005523 C	15-09-1998	NONE	
WO 9744736 A	27-11-1997	AU 3206397 A	09-12-1997
US 5687236 A	11-11-1997	US 5613004 A	18-03-1997
		EP 0872073 A	21-10-1998
		WO 9642151 A	27-12-1996
US 5974141 A	26-10-1999	US 6076077 A	13-06-2000
		US 6002772 A	14-12-1999
		US 6097818 A	01-08-2000
WO 9952271 A	14-10-1999	US 6205249 B	20-03-2001
		EP 1068720 A	17-01-2001
EP 0649261 A	19-04-1995	JP 7115638 A	02-05-1995
		US 5933499 A	03-08-1999
WO 9963443 A	09-12-1999	AU 7683398 A	20-12-1999
		EP 1103026 A	30-05-2001

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2001 (15.03.2001)

PCT

(10) International Publication Number
WO 01/18628 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US00/21189

(22) International Filing Date: 4 August 2000 (04.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/147,134 4 August 1999 (04.08.1999) US
60/213,489 23 June 2000 (23.06.2000) US

(71) Applicant *(for all designated States except US)*: **BLUE SPIKE, INC.** [US/US]; 16711 Collins Avenue #2505, Miami, FL 33160 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MOSKOWITZ, Scott, A.** [US/US]; 16711 Collins Avenue #2505, Miami, FL 33160 (US). **BERRY, Michael** [US/US]; 12401 Princess Jeanne, Alburquerque, NM 87112 (US).

(74) Agents: **CHAPMAN, Floyd, B.** et al.; Baker Botts, LLP, The Warner, 1299 Pennsylvania Avenue, N.W., Washington, DC 20004 (US).

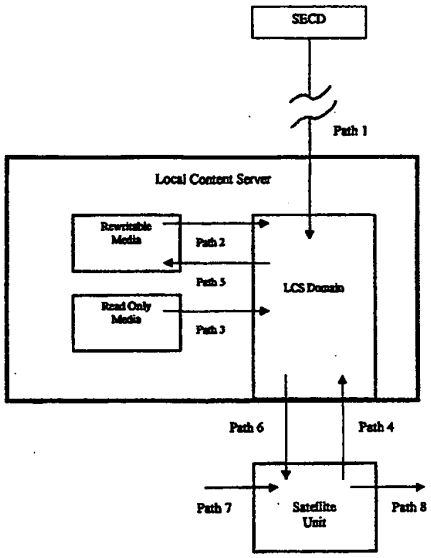
(81) Designated States *(national)*: JP, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *Without international search report and to be republished upon receipt of that report.*

[Continued on next page]

(54) Title: A SECURE PERSONAL CONTENT SERVER



(57) Abstract: A local content server system (LCS) for creating a secure environment for digital content is disclosed, which system comprises: a communications port in communication for connecting the LCS via a network to at least one Secure Electronic Content Distributor (SECD), which SECD is capable of storing a plurality of data sets, is capable of receiving a request to transfer at least one content data set, and is capable of transmitting the at least one content data set in a secured transmission; a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved; a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS, and a programmable address module which can be programmed with an identification code uniquely associated with the LCS. The LCS is provided with rules and procedures for accepting and transmitting content data. Optionally, the system may further comprise: an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected

[Continued on next page]

WO 01/18628 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

to the system through the interface, which SUs are capable of receiving and transmitting digital content; at least one SU; and/or at least one SECD. The SECD may have a storage device for storing a plurality of data sets, as well as a transaction processor for validating the request to purchase and for processing payment for a request to retrieve one of the data sets. The SECD typically includes a security module for encrypting or otherwise securitizing data which the SECD may transmit. A method for creating a secure environment for digital content for a consumer is also disclosed. As part of the method, a LCS requests and receives a digital data set that may be encrypted or scrambled. The digital data set may be embedded with at least one robust open watermark, which permits the content to be authenticated. The digital data set is preferably embedded with additional watermarks which are generated using information about the LCS requesting the copy and/or the SECD which provides the copy. Once received by the LCS, the LCS exercises control over the content and only releases the data to authorized users. Generally, the data is not released until the LCS embeds at least one additional watermark based upon protected information associated with the LCS and/or information associated with the user.

A SECURE PERSONAL CONTENT SERVER

Field of Invention

The present invention relates to the secure distribution of digitized value-added information, or media content, while preserving the ability of publishers to make available unsecured versions of the same value-added information, or media content, without adverse effect to the systems security.

Authentication, verification and authorization are all handled with a combination of cryptographic and steganographic protocols to achieve efficient, trusted, secure exchange of digital information.

Cross-Reference To Related Application

This application is based on and claims the benefit of pending U.S. Patent Application Serial No. 60/147,134, filed 08/04/99, entitled, "A Secure Personal Content Server" and pending U.S. Patent Application Serial No. 60/213,489, filed 06/23/2000, entitled "A Secure Personal Content Server."

This application also incorporates by reference the following applications: pending U.S. Patent Application Serial No. 08/999,766, filed 7/23/97, entitled "Steganographic Method and Device"; pending U.S. Patent Application Serial No. 08/772,222, filed 12/20/96, entitled "Z-Transform Implementation of Digital Watermarks"; pending U.S. Patent Application Serial No. 09/456,319, filed 12/08/99, entitled "Transform Implementation of Digital Watermarks"; pending U.S. Patent Application Serial No. 08/674,726, filed 7/2/96, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management"; pending U.S. Patent Application Serial No. 09/545,589, filed 04/07/2000, entitled "Method and System for Digital Watermarking"; pending U.S. Patent Application Serial No. 09/046,627, filed 3/24/98, entitled "Method for Combining Transfer Function with Predetermined Key Creation"; pending U.S. Patent Application Serial No. 09/053,628, filed 04/02/98, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking"; pending U.S. Patent Application Serial No. 09/281,279, filed 3/30/99, entitled "Optimization Methods for the Insertion, Protection, and Detection..."; U.S. Patent Application Serial No.09/594,719, filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and

Cryptographic Systems" (which is a continuation-in-part of PCT application No. PCT/US00/06522, filed 14 March 2000, which PCT application claimed priority to U.S. Provisional Application No. 60/125,990, filed 24 March 1999); and pending U.S. Application No 60/169,274, filed 12/7/99, entitled "Systems, Methods And Devices For Trusted Transactions." All of the patent applications previously identified in this paragraph are hereby incorporated by reference, in their entireties.

Background of the Invention

The music industry is at a critical inflection point. Digital technology enables anyone to make perfect replica copies of musical recordings from the comfort of their home, or as in some circumstances, in an offshore factory. Internet technology enables anyone to distribute these copies to their friends, or the entire world. Indeed, virtually any popular recording is already likely available in the MP3 format, for free if you know where to look.

How the industry will respond to these challenges and protect the rights and livelihoods of copyright owners and managers and has been a matter of increasing discussion, both in private industry forums and the public media. Security disasters like the cracking of DVD-Video's CSS security system have increased doubt about the potential for effective robust security implementations. Meanwhile, the success of non-secure initiatives such as portable MP3 players lead many to believe that these decisions may have already been made.

Music consumers have grown accustomed to copying their music for their own personal use. This fact of life was written into law in the United States via the Audio Home Recording Act of 1992. Millions of consumers have CD players and purchase music in the Compact Disc format. It is expected to take years for a format transition away from Red Book CD Audio to reach significant market penetration.

Hence, a need exists for a new and improved system for protecting digital content against unauthorized copying and distribution.

Summary of the Invention

A local content server system (LCS) for creating a secure environment for digital content is disclosed, which system comprises: a communications port in communication for connecting the LCS via a network to at least one Secure Electronic Content Distributor (SECD), which SECD is capable of storing a

plurality of data sets, is capable of receiving a request to transfer at least one content data set, and is capable of transmitting the at least one content data set in a secured transmission; a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved; a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS; and a programmable address module which can be programmed with an identification code uniquely associated with the LCS. The LCS is provided with rules and procedures for accepting and transmitting content data. Optionally, the system may further comprise: an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, which SUs are capable of receiving and transmitting digital content; at least one SU; and/or at least one SECD. The SECD may have a storage device for storing a plurality of data sets, as well as a transaction processor for validating the request to purchase and for processing payment for a request to retrieve one of the data sets. The SECD typically includes a security module for encrypting or otherwise securitizing data which the SECD may transmit.

A method for creating a secure environment for digital content for a consumer is also disclosed. As part of the method, a LCS requests and receives a digital data set that may be encrypted or scrambled. The digital data set may be embedded with at least one robust open watermark, which permits the content to be authenticated. The digital data set is preferably be embedded with additional watermarks which are generated using information about the LCS requesting the copy and/or the SECD which provides the copy. Once received by the LCS, the LCS exercises control over the content and only releases the data to authorized users. Generally, the data is not released until the LCS embeds at least one additional watermark based upon protected information associated with the LCS and/or information associated with the user.

Another embodiment of the method of the present invention comprises: connecting a Satellite Unit to an local content server (LCS), sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU; analyzing the message to confirm that the SU is authorized to use the LCS; retrieving a copy of the

requested content data set; assessing whether a secured connection exists between the LCS and the SU; if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS; and delivering the content data set to the SU for its use.

The SU may also request information that is located not on the LCS, but on an SECD, in which case, the LCS will request and obtain a copy from the SECD, provided the requesting SU is authorized to access the information.

Digital technology offers economies of scale to value-added data not possible with physical or tangible media distribution. The ability to digitize information both reduces the cost of copying and enables perfect copies. This is an advantage and a disadvantage to commercial publishers who must weigh the cost reduction against the real threat of unauthorized duplication of their value-added data content. Because cost reduction is an important business consideration, securing payment and authenticating individual copies of digital information (such as media content) presents unique opportunities to information service and media content providers. The present invention seeks to leverage the benefits of digital distribution to consumers and publishers alike, while ensuring the development and persistence of trust between all parties, as well as with any third parties involved, directly or indirectly, in a given transaction.

In another approach that is related to this goal, there are instances where transactions must be allowed to happen after perceptually-based digital information can be authenticated. (Perceptually based information is information whose value is in large part, based upon its ability to be perceived by a human, and includes for example, acoustic, psychoacoustic, visual and psychovisual information.) The process of authenticating before distributing will become increasingly important for areas where the distributed material is related to a trust-requiring transaction event. A number of examples exist. These include virtual retailers (for example, an on-line music store selling CDs and electronic versions of songs); service providers (for example, an on-line bank or broker who performs transactions on behalf of a consumer); and transaction providers (for example, wholesalers or auction houses). These parties have different authentication interests and requirements. By using the

teachings of this application, these interests and requirements may be separated and then independently quantified by market participants in shorter periods of time.

All parties in a transaction must authenticate information that is perceptually observable before trust between the parties can be established. In today's world, information (including perceptually rich information) is typically digitized, and as a result, can easily be copied and redistributed, negatively impacting buyers, sellers and other market participants. Unauthorized redistribution confuses authenticity, non-repudiation, limit of ability and other important "transaction events." In a networked environment, transactions and interactions occur over a transmission line or a network, with buyer and seller at different points on the line or network. While such electronic transactions have the potential to add value to the underlying information being bought and sold (and the potential to reduce the cost of the transaction), instantaneous piracy can significantly reduce the value of the underlying data, if not wholly destroy it. Even the threat of piracy tends to undermine the value of the data that might otherwise exist for such an electronic transaction.

Related situations range from the ability to provably establish the "existence" of a virtual financial institution to determining the reliability of an "electronic stamp." The present invention seeks to improve on the prior art by describing optimal combinations of cryptographic and steganographic protocols for "trusted" verification, confidence and non-repudiation of digitized representations of perceptually rich information of the actual seller, vendor or other associated institutions which may not be commercial in nature (confidence building with logo's such as the SEC, FDIC, Federal Reserve, FBI, etc. apply). To the extent that an entity plays a role in purchase decisions made by a consumer of goods and services relating to data, the present invention has a wide range of beneficial applications. One is enabling independent trust based on real world representations that are not physically available to a consumer or user. A second is the ability to match informational needs between buyers and sellers that may not be universally appealing or cost effective in given market situations. These include auction models based on recognition of the interests or demand of consumers and market participants—which make trading profitable by focusing specialized buyers and

sellers. Another use for the information matching is to establish limits on the liability of such institutions and profit-seeking entities, such as insurance providers or credit companies. These vendors lack appropriate tools for determining intangible asset risk or even the value of the information being exchanged. By encouraging separate and distinct "trust" arrangements over an electronic network, profitable market-based relationships can result.

The present invention can make possible efficient and openly accessible markets for tradable information. Existing transaction security (including on-line credit cards, electronic cash or its equivalents, electronic wallets, electronic tokens, etc.) which primarily use cryptographic techniques to secure a transmission channel--but are not directly associated or dependent on the information being sold--fails to meet this valuable need. The present invention proposes a departure from the prior art by separating transactions from authentication in the sale of digitized data. Such data may include videos, songs, images, electronic stamps, electronic trademarks, and electronic logos used to ensure membership in some institutional body whose purpose is to assist in a dispute, limit liability and provide indirect guidance to consumers and market participants, alike.

With an increasingly anonymous marketplace, the present invention offers invaluable embodiments to accomplish "trusted" transactions in a more flexible, transparent manner while enabling market participants to negotiate terms and conditions. Negotiation may be driven by predetermined usage rules or parameters, especially as the information economy offers potentially many competitive marketplaces in which to transact, trade or exchange among businesses and consumers. As information grows exponentially, flexibility becomes an advantage to market participants, in that they need to screen, filter and verify information before making a transaction decision. Moreover, the accuracy and speed at which decisions can be made reliably enables confidence to grow with an aggregate of "trusted transactions". "Trusted transactions" beget further "trusted transactions" through experience. The present invention also provides for improvements over the prior art in the ability to utilize different independently important "modules" to enable a "trusted transaction" using competitive cryptographic and steganographic elements, as well as being able to support a wide variety of perceptually-based

media and information formats. The envisioned system is not bound by a proprietary means of creating recognition for a good or service, such as that embodied in existing closed system. Instead, the flexibility of the present invention will enable a greater and more diverse information marketplace.

The present invention is not a "trusted system", *per se*, but "trusted transactions" are enabled, since the same value-added information that is sought may still be in the clear, not in a protected storage area or closed, rule-based "inaccessible virtual environment".

A related additional set of embodiments regards the further separation of the transaction and the consumer's identification versus the identification of the transaction only. This is accomplished through separated "trusted transactions" bound by authentication, verification and authorization in a transparent manner. With these embodiments, consumer and vendor privacy could be incorporated. More sophisticated relationships are anticipated between parties, who can mix information about their physical goods and services with a transparent means for consumers, who may not be known to the seller, who choose not to confide in an inherently closed "trusted system" or provide additional personal information or purchasing information (in the form of a credit card or other electronic payment system), in advance of an actual purchase decision or ability to observe (audibly or visibly) the content in the clear. This dynamic is inconsistent with the prior art's emphasis on access control, not transparent access to value-added information (in the form or goods or services), that can be transacted on an electronic or otherwise anonymous exchange.

These embodiments may include decisions about availability of a particular good or service through electronic means, such as the Internet, or means that can be modularized to conduct a transaction based on interconnection of various users (such as WebTV, a Nintendo or Sony game console with network abilities, cellular phone, PalmPilot, etc.). These embodiments may additionally be implemented in traditional auction types (including Dutch auctions). Consumers may view their anonymous marketplace transactions very differently because of a lack of physical human interactions, but the present invention can enable realistic transactions to occur by maintaining open access and offering strict authentication and verification of the

information being traded. This has the effect of allowing legacy relationships, legacy information, and legacy business models to be offered in a manner which more closely reflects many observable transactions in the physical world. The tremendous benefits to sellers and consumers is obvious; existing transactions need not reduce their expectations of security. As well, the ability to isolate and quantify aspects of a transaction by module potentially allows for better price determinations of intangible asset insurance, transaction costs, advertising costs, liability, etc. which have physical world precedent.

It is contemplated that the publisher and/or owner of the copyrights will want to dictate restrictions on the ability of the purchaser to use the data being sold. Such restrictions can be implemented through the present invention, which presents a significant advantage over the prior art (which attempts to effect security through access control and attempted tight reigns over distribution). See US Pat. No. 5,428,606 for a discussion on democratizing digital information exchange between publishers and subscribers of said information.

A goal for providers of value-added content is to maximize profits for the sale of their content. Marketing and promotion of the informational content cannot be eliminated, considering the ever increasing amount of information vying for consumers and other market participant's attention. Nonetheless, in a market where the goods are speculatively valued, marketing budgets are inherently constrained, as you are trying to create demand for a product with little inherent value. Where such markets have participants, both buyers and sellers and their respective agents, with access to the same information in real time, market mechanisms efficiently price the market goods or services. These markets are characterized by "price commoditization" so buyers and sellers are limited to differentiating their offerings by selection and service. If the markets are about information itself, it has proven more difficult to accurately forecast the target price where sellers can maximize their profits. Quality and quantity provide different evaluation criteria of selection and service relating to the information being traded. The present invention regards a particular set of implementations of value-added content security in markets which may include unsecured and secure versions of the same value-added data (such as

songs, video, research, pictures, electronic logos, electronic trademarks, value-added information, etc.).

Transactions for value-added information can occur without any physical location. So, there is a need for a secure personal content server for which the value added information can be offered for transactions in a manner similar to real world transactions. One feature is to offer seemingly similar value added information in differing quality settings. These settings have logical relationships with fidelity and discreteness and are determined by market participants. Another issue is that because purchasers may be anonymous to sellers, it is more important to have a particular value-added information object available so that market participants can fulfill their role are consumers.

One fundamental weakness of current information markets is the lack of mechanisms to ensure that buyers and sellers can reach pricing equilibrium. This deficit is related to the "speculative" , "fashion", and "vanity" aspects of perceptual content (such as music, video, and art or some future recognition to purchasers). For other goods and services being marketed to an anonymous marketplace, market participants may never see (and indeed, may choose to never see, an actual location where the transaction may physically occur. A physical location may simply not exist. There are a number of such virtual operations in business today, which would benefit from the improvements offered under the present system.

The present invention also seeks to provide improvements to the art in enabling a realistic model for building trust between parties (or their agents) not in a "system", per se. Because prior art systems lack any inherent ability to allow for information to flow freely to enable buyers and sellers to react to changing market conditions. The present invention can co-exist with these "trusted systems" to the extent that all market participants in a given industry have relatively similar information with which to price value-added data. The improvement over such systems, however, addresses a core features in most data-added value markets: predictions, forecasts, and speculation over the value of information is largely an unsuccessful activity for buyers and sellers alike. The additional improvement is the ability to maintain security even with unsecured or legacy versions of value-added information available to those who seek choices that fit less quantitative criteria—

"aesthetic quality" of the information versus "commercial price". Purchase or transaction decisions can be made first by authenticating an electronic version of a song, image, video, trademark, stamp, currency, etc.

Additional anticipated improvements include the ability to support varying pricing models such as auctions that are difficult or impossible to accomplish under existing prior art that leaves all access and pricing control with the seller alone, and the separation of the transaction from the exchange of the value-added information, which gives more control to buyers over their identities and purchasing habits, (both sensitive and separately distinct forms of "unrelated" value-added information). Essentially, no system known in the art allows for realistic protocols to establish trust between buyers and sellers in a manner more closely reflecting actual purchasing behavior of consumers and changing selling behavior of sellers. The goal in such transactions is the creation of trust between parties as well as "trusted relationships" with those parties. The present invention is an example of one such system for media content where the "aesthetic" or "gestalt" of the underlying content and its characteristics is a component of buying habits. Without an ability to open distribution systems to varying buyers and sellers, media content may be priced at less than maximum economic value and buyers may be deprived of a competitive, vigorous marketplace for exciting media content from many different creative participants.

To the extent that recognition plays such a key role in an information economy, value-added data should be as accessible as possible to the highest number of market participants in the interests of furthering creativity and building a competitive marketplace for related goods and services. This is to the benefit of both buyers and sellers as well as the other participants in such an economic ecosystem. The Internet and other transmission-based transactions with unknown parties presents a number of challenges to information vendors who wish to develop customer relations, trust and profitable sales. The information economy is largely an anonymous marketplace, thus, making it much more difficult to identify consumers and sellers. The present invention provides remedies to help overcome these weaknesses.

The present invention is concerned with methods and systems which enable secure, paid exchange of value-added information, while separating transaction protocols. The present invention improves on existing means for distribution control by relying on authentication, verification and authorization that may be flexibly determined by both buyers and sellers. These determinations may not need to be predetermined, although pricing matrix and variable access to the information opens additional advantages over the prior art. The present invention offers methods and protocols for ensuring value-added information distribution can be used to facilitate trust in a large or relatively anonymous marketplace (such as the Internet's World Wide Web).

We now define components of the preferred embodiments for methods, systems, and devices.

Definitions:

Local Content Server (LCS): A device or software application which can securely store a collection of value-added digital content. The LCS has a unique ID.

Secure Electronic Content Distributor (SECD): An entity, device or software application which can validate a transaction with a LCS, process a payment, and deliver digital content securely to a LCS. In cryptographic terms, the SECD acts as a "certification authority" or its equivalent. SECDs may have differing arrangements with consumers and providers of value-added information. (The term "content" is used to refer generally to digital data, and may comprise video, audio, or any other data that is stored in a digital format).

Satellite Unit (SU): A portable medium or device which can accept secure digital content from a LCS through a physical, local connection and which can either play or make playable the digital content. The SU may have other functionality as it relates to manipulating the content, such as recording. The SU has a unique ID. An SU may be a CD player, a video camera, a backup drive, or other electronic device which has a storage unit for digital data.

LCS Domain: A secure medium or area where digital content can be stored, with an accompanying rule system for transfer of digital content in and out of the LCS Domain. The domain may be a single device or multiple devices—all of which have some common ownership or control. Preferably, a LCS domain is linked to a

single purchasing account. Inside the domain, one can enjoy music or other digital data without substantial limitations—as typically a license extends to all personal use.

SecureChannel™: A secure channel to pass individualized content to differentiate authentic content from legacy or unauthorized, pirated content. For example, the Secure Channel may be used as an auxiliary channel through which members of the production and distribution chain may communicate directly with individual consumers. Preferably, the Secure Channel is never exposed and can only be accessed through legitimate methods. SecureChannel may carry a value-adding component (VAC). The ability to provide consumers with value adding features will serve to give consumers an incentive to purchase new, secure hardware and software that can provide the additional enhanced services. The SecureChannel may also include protected associated data—data which is associated with a user and/or a particular set of content.

Standard Quality: A transfer path into the LCS Domain which maintains the digital content at a predetermined reference level or degrades the content if it is at a higher quality level. In an audio implementation, this might be defined as Red Book CD Quality (44100 Hz., 16 bits, 2 channels). This transfer path can alternately be defined in terms of a subset of VAC's or a quality level associated with particular VAC's. If a VAC is not in the subset, it is not passed. If a VAC is above the defined quality level, it is degraded.

Low Quality: A transfer path into the LCS Domain which degrades the digital content to a sub-reference level. In an audio implementation, this might be defined as below CD Quality (for instance, 32000 Hz., 16 bits, 2 channels). This transfer path can alternately be defined in terms of an absence of VAC's or a degraded quality level associated with particular VAC's.

High Quality: A transfer path into the LCS Domain which allows digital content of any quality level to pass unaltered. This transfer path can alternately be defined in terms of a complete set of VAC's or the highest quality level available associated with particular VAC's.

Rewritable Media: An mass storage device which can be rewritten (e.g. hard drive, CD-RW, Zip cartridge, M-O drive, etc...).

Read-Only Media: A mass storage device which can only be written once (e.g. CD-ROM, CD-R, DVD, DVD-R, etc...). Note: pre-recorded music, video, software, or images, etc. are all "read only" media.

Unique ID: A Unique ID is created for a particular transaction and is unique to that transaction (roughly analogous to a human fingerprint). One way to generate a Unique ID is with a one-way hash function. Another way is by incorporating the hash result with a message into a signing algorithm will create a signature scheme. For example, the hash result may be concatenated to the digitized, value added information which is the subject of a transaction. Additional uniqueness may be observed in a hardware device so as to differentiate that device, which may be used in a plurality of transactions, from other similar devices.

Value-added: Value-added information is differentiated from non-commoditized information in terms of its marketability or demand, which can vary, obviously, from each market that is created for the information. By way of example, information in the abstract has no value until a market is created for the information (i.e., the information becomes a commodity). The same information can be packaged in many different forms, each of which may have different values. Because information is easily digitized, one way to package the "same" information differently is by different levels of fidelity and discreteness. Value is typically bounded by context and consideration.

Authentication: A receiver of a "message" (embedded or otherwise within the value-added information) should be able to ascertain the original of the message (or by effects, the origin of the carrier within which the message is stored). An intruder should not be able to successfully represent someone else. Additional functionality such as Message Authentication Codes (MAC) could be incorporated (a one-way hash function with a secret key) to ensure limited verification or subsequent processing of value-added data.

Verification: In cryptographic terms, "verification" serves the "integrity" function to prevent an intruder from substituting false messages for legitimate ones. In this sense, the receiver of the message (embedded or otherwise present within the value-added information) should be assured that the message was not modified or altered in transit.

One-way hash function: One-way hash functions are known in the art. A hash function is a function which converts an input into an output, which is usually a fixed-sized output. For example, a simple hash function may be a function which accepts a digital stream of bytes and returns a byte consisting of the XOR function of all of the bytes in the digital stream of input data Roughly speaking, the hash function may be used to generate a "fingerprint" for the input data. The hash function need not be chosen based on the characteristics of the input. Moreover, the output produced by the hash function (i.e., the "hash") need not be secret, because in most instances it is not computationally feasible to reconstruct the input which yielded the hash. This is especially true for a "one-way" hash function--one that can be used to generate a hash value for a given input string, but which hash cannot be used (at least, not without great effort) to create an input string that could generate the same hash value.

Authorization: A term which is used broadly to cover the acts of conveying official sanction, permitting access or granting legal power to an entity.

Encryption: For non digitally-sampled data, encryption is data scrambling using keys. For value-added or information rich data with content characteristics, encryption is typically slow or inefficient because content file sizes tend to be generally large. Encrypted data is called "ciphertext".

Scrambling: For digitally-sampled data, scrambling refers to manipulations of the value-added or information rich data at the inherent granularity of the file format. The manipulations are associated with a key, which may be made cryptographically secure or broken into key pairs. Scrambling is efficient for larger media files and can be used to provide content in less than commercially viable or referenced quality levels. Scrambling is not as secure as encryption for these applications, but provides more fitting manipulation of media rich content in the context of secured distribution. Scrambled data is also called "ciphertext" for the purposes of this invention. Encryption generally acts on the data as a whole, whereas scrambling is applied often to a particular subset of the data concerned with the granularity of the data, for instance the file formatting. The result is that a smaller amount of data is "encoded" or "processed" versus strict encryption, where all of the data is "encoded" or "processed." By way of example, a cable TV signal

can be scrambled by altering the signal which provides for horizontal and vertical tracking, which would alter only a subset of the data, but not all of the data—which is why the audio signal is often untouched. Encryption, however, would generally so alter the data that no recognizable signal would be perceptually appreciated. Further, the scrambled data can be compared with the unscrambled data to yield the scrambling key. The difference with encryption is that the ciphertext is not completely random, that is, the scrambled data is still perceptible albeit in a lessened quality. Unlike watermarking, which maps a change to the data set, scrambling is a transfer function which does not alter or modify the data set.

Detailed Discussion of Invention

The LCS Domain is a logical area inside which a set of rules governing content use can be strictly enforced. The exact rules can vary between implementations, but in general, unrestricted access to the content inside the LCS Domain is disallowed. The LCS Domain has a set of paths which allow content to enter the domain under different circumstances. The LCS Domain also has paths which allow the content to exit the domain.

A simple example provides insight into the scope of an LCS domain. If an LCS is assigned to an individual, then all music, video, and other content data which has lawfully issued to the individual may be freely used on that persons LCS domain (though perhaps "freely" is misleading, as in theory, the individual has purchased a license). A LCS Domain may comprise multiple SUs, for example, a video player, a CD player, etc. An individual may be authorized to take a copy of a song and play it in another's car stereo, but only while the individual's device or media is present. Once the device is removed, the friend's LCS will no longer have a copy of the music to play.

The act of entering the LCS Domain includes a verification of the content (an authentication check). Depending upon the source of the content, such verification may be easier or harder. Unvalidateable content will be subjected to a quality degradation. Content that can be validated but which belongs to a different LCS Domain will be excluded. The primary purpose of the validation is to prevent unauthorized, high-quality, sharing of content between domains.

When content leaves the LCS Domain, the exiting content is embedded with information to uniquely identify the exiting content as belonging to the domain from which the content is leaving. It is allowed to leave at the quality level at which the content was originally stored in the LCS Domain (i.e. the quality level determined by the validation path). For example, the exiting content may include an embedded digital watermark and an attached hash or digital signature; the exiting content may also include a time stamp—which itself may be embedded or merely attached). Once it has exited, the content cannot return to the domain unless both the watermark and hash can be verified as belonging to this domain. The presence of one or the other may be sufficient to allow re-entry, or security can be set to require the presence of more than one identification signal.

This system is designed to allow a certifiable level of security for high-quality content while allowing a device to also be usable with unsecured content at a degraded quality level. The security measures are designed such that a removal of the watermark constitutes only a partial failure of the system. The altered content (i.e., the content from which the watermark has been removed or the content in which the watermark has been degraded) will be allowed back into the LCS Domain, but only at a degraded quality level, a result of the watermark destruction and subsequent obscurity to the system, consumers will not be affected to the extent that the unauthorized content has only been degraded, but access has not been denied to the content. Only a complete forgery of a cryptographically-secure watermark will constitute a complete failure of the system. For a discussion on such implementations please see US Pat. No. 5,613,004, US Pat No. 5,687,236, US Pat. No. 5,745,569, US Pat. No. 5,822,432, US Pat. No. 5,889,868, US Pat. No. 5,905,800, included by reference in their entirety and pending U.S. patent applications with Serial No. 09/046,627 "Method for Combining Transfer Function...", Serial No. 09/053,628 "Multiple Transform Utilization and Application for Secure Digital Watermarking", Serial No. 08/775,216 "Steganographic Method and Device", Serial No. 08/772,222 "Z-Transform Implementation ...", Serial No. 60/125990 "Utilizing Data Reduction in Steganographic and Cryptographic Systems".

Provable security protocols can minimize this risk. Thus the embedding system used to place the watermark does not need to be optimized for robustness, only for imperceptibility (important to publishers and consumers alike) and security (more important to publishers than to consumers). Ideally, as previously disclosed, security should not obscure the content, or prevent market participants from accessing information, which in the long term, should help develop trust or create relationships.

The system can flexibly support one or more "robust" watermarks as a method for screening content to speed processing. Final validation, however, relies upon the fragile, secure watermark and its hash or digital signature (a secure time stamp may also be incorporated). Fragile watermarks, meaning that signal manipulations would affect the watermark, may be included as a means to affect the quality of the content or any additional attributes intended to be delivered to the consumer.

LCS Functions

The LCS provides storage for content, authentication of content, enforcement of export rules, and watermarking and hashing of exported content. Stored content may be on an accessible rewritable medium, but it must be stored as ciphertext (encrypted or scrambled), not plain text, to prevent system-level extraction of the content. This is in contrast to the prior art which affix or otherwise attach meta-data to the content for access control by the variously proposed systems.

Typically, an LCS receives secured data from one or more SECDs. The SECD transfers content only after it has been secured. For example, the SECD may use an individualized cryptographic container to protect music content while in transit. Such a container may use public/private key cryptography, ciphering and/or compression, if desired.

The LCS may be able to receive content from a SECD, and must be able to authenticate content received via any of the plurality of implemented paths. The LCS must monitor and enforce any rules that accompany received content, such as number of available copies. Finally, it is preferred for the LCS to watermark all exported material (with the exception of Path 6 - see below) and supply a hash made from the unique ID of the LCS and the content characteristics (so as to be

maintained perceptually within the information and increase the level of security of the watermark).

SU Functions

The SU enables the content to be usable away from the LCS. The SU is partially within the LCS Domain. A protocol must exist for the SU and LCS to authenticate any connection made between them. This connection can have various levels of confidence set by the level of security between the SU and LCS and determinable by a certification authority or its equivalent, an authorized site for the content, for example. The transfer of content from the SU to the LCS without watermarking is allowed. However, all content leaving the SU must be watermarked. Preferably, the SU watermark contains a hash generated from the SU's Unique ID and the content characteristics of the content being transferred. If the content came from a LCS, the SU watermark must also be generated based, in part, upon the hash received from the LCS. The LCS and SU watermarking procedures do not need to be the same. However, the LCS must be able to read the SU watermarks for all different types of SU's with which it can connect. The SU does not need to be able to read any LCS watermarks. Each LCS and SU must have separate Unique IDs.

Sample Embodiment

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, the objects and advantages thereof, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

FIG. 1 shows in block diagram form a system for one embodiment of an LCS, showing the possible paths for content to enter and exit the system.

FIG. 2 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content enters the LCS Domain from the rewritable media.

FIG. 3 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content enters the LCS Domain from the read-only media.

FIG. 4 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content enters the LCS Domain from the satellite unit.

FIG. 5 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content leaves the LCS Domain.

FIG. 6 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content leaves the LCS Domain from the read-only media.

FIG. 7 is flow diagram illustrating the functions performed by the LCS of FIG. 1 when content leaves the SU to a receiver other than the LCS.

DETAILED DESCRIPTION OF THE INVENTION

The preferred embodiment of the present invention and its advantages are best understood by referring to FIGs. 1 through 7 of the drawings, like numerals being used for like and corresponding parts of the various drawings.

FIG. 1 is a block diagram showing the components of a sample LCS system and showing the possible paths for content to enter and leave the LCS. In the embodiment of Figure 1, the LCS is a general purpose computing device such as a PC with software loaded to emulate the functions of a LCS. The LCS of Figure 1 has a Rewritable media (such as a hard drive), a Read-Only media (such as a CD-ROM drive), and software to control access (which software, in effect, defines the "LCS Domain"). The Secure Electronic Content Distributor (SECD) is connected via a network (such as the Internet, intranet, cable, satellite link, cellular communications network, or other commonly accepted network). The Satellite Unite (SU) is a portable player which connects to the LCS and/or to other players where applicable (for example by way of a serial interface, USB, IEEE 1394, infrared, or other commonly used interface protocol). FIG. 1 also identifies seven (7) path ways.

Path 1 depicts a secure distribution of digital content from a SECD to a LCS. The content can be secured during the transmission using one or more 'security protocols' (e.g., encryption or scrambling). Moreover, a single LCS may have the capability to receive content transmissions from multiple SECDs, and each SECD may use the same security protocols or different security protocols. In the context of FIG. 1, however, only a single SECD is displayed. It is also contemplated that the same SECD may periodically or randomly use different security protocols. A typical security protocol uses an asymmetric cryptographic system, an example being a public key cryptography system where private and public key pairs allow the

LCS to authenticate and accept the received content. Another security protocol may involve the ability to authenticate the received content using a signature scheme.

In FIG. 2, content enters the LCS Domain from the rewritable media (such as a hard drive). This communication path is identified as Path 2 on FIG. 1. The LCS Domain analyzes the content to determine if a watermark is present in the content. If no watermark is present, then the quality of the content is downgraded to Low Quality before it is stored in the LCS Storage. If a watermark is present, then the watermark is extracted and compared with the watermark of the LCS in order to determine if a match exists. In the event of a match, the content is permitted to be stored on the LCS Storage at the same level of quality which the content entered the LCS Domain. Optionally, if a watermark is present, the hash may be checked as further verification; and if the hash matches, the content is allowed in at High Quality. If it does not match, the content is rejected. If the extracted watermark does not match the expected watermark, then the content is denied access to the LCS Storage (i.e., the content is rejected).

In FIG. 3, content enters the LCS Domain from the Read-Only media. This communication path is identified as Path 3 on FIG. 1. The LCS Domain analyzes the content to determine if a watermark is present in the content. If no watermark is present, then the LCS attempts to further analyze the content using other methods (i.e., other than watermarking) to try and verify the content for originality. If the content cannot be verified or is deemed to have been altered, then the content is downgraded to Standard Quality (or even Low Quality) before it is stored in the LCS Storage. If a watermark is present, then the watermark is extracted and compared with the watermark of the LCS in order to determine if a match exists. In the event of a match, or in the event that the content is verified by means other than the watermark, the content is permitted to be stored on the LCS Storage at the same level of quality which the content entered the LCS Domain (which is likely to be High Quality). For example, the Read-Only media may also contain an media-based identifier which verifies the content as an original, as opposed to a copy—and hence, a non-watermark method may be used to verify authenticity.

Optionally, even in the event of a watermark match, a hash may be checked as further verification; and if the hash matches, the content is allowed in at High

Quality, but if there is no match, the content is rejected. If the extracted watermark does not match the expected watermark, or if the LCS is unable to identify any other method for verifying the content's authenticity, then the content may be denied access to the LCS Storage (i.e., the content may be rejected), or if preferred by the user, the content may be permitted into the system at a degraded quality level. It is the user's prerogative to decide how the system will treat non-authenticated content, as well as legacy content.

In FIG. 4, content enters the LCS Domain from the satellite unit. This communication path is identified as Path 4 on FIG. 1. Content from an SU is marked with an SU watermark before exiting the SU. The LCS analyzes the content from the SU for watermarks, and in particular to determine if there is a watermark that matches that of the LCS. If the watermarks match, the content is permitted access to the LCS at the highest quality level. If there is a mismatch, then the content is denied access (i.e., the content is rejected). If the content does not contain a watermark, the quality is downgraded to Low Quality before permitting access to the LCS. Optionally, even in the event of a watermark match, a hash may be checked as further verification; and access at the highest quality level may depend upon both a match in watermarks and a match in hashes.

In FIG. 5, content is shown leaving the LCS Domain. This communication path is identified as Path 5 on FIG. 1. Content is retrieved from the LCS storage and then the content may be watermarked with a watermark that is unique to the LCS (for example, one that is based upon the LCS's Unique ID). Optionally, a hash may be attached to the watermarked content, and/or the hash may be embedded as part of the watermark. If an external hash is used, preferably, for security purposes, the external hash should be created in a different manner from the embedded, watermark hash. Optionally, other information may be included in the watermark, for example, information to specify a time stamp, the number of allowable copies, etc. After watermarking, the content may be permitted to exit the LCS Domain, and may be exported to a device outside the LCS Domain, including for example, a rewritable media, a viewer, player, or other receiver.

In FIG. 6, content is shown leaving the LCS Domain. This communication path is identified as Path 6 on FIG. 1. This path is similar to Path 5, with a few

important differences. The output receiver is an SU, and because the receiver is an SU, the content may leave the LCS without being watermarked. Path 6 requires a secure protocol to determine that the receiver is in fact an SU. Once the path is verified, the content can be exported without a watermark. The LCS may optionally transmit the content together with a hash value which will be uniquely associated with the content.

In FIG. 7, content is shown leaving the SU, to a receiver other than the LCS. This communication path is identified as Path 7 on FIG. 1. Content is retrieved from the SU storage and then the content may be watermarked with a watermark that is unique to the SU (for example, one that is based upon the SU's Unique ID). Optionally, a hash may be attached to the watermarked content, and/or the hash may be embedded as part of the watermark. If an external hash is used, preferably, for security purposes, the external hash should be created in a different manner from the embedded, watermark hash. Optionally, other information may be included in the watermark, for example, information to specify a time stamp, the number of allowable copies, etc., and may even include the hash which the LCS attached to the content After watermarking, the content may be permitted to exit the SU, and may be exported to a device other than the LCS, including for example, a rewritable media, a viewer, player, or other receiver. The quality level of the content leaving the LCS is generally the same quality level as that of the content when stored internally to the LCS.

The system of the present invention is utilized to complete digital data transactions. A typical transaction would have the following steps:

1.) Using an LCS, a user connects to a SECD.

2.) The user reviews a collection of data sets which are available for license (which for purposes of this application, may be equated with a purchase). The user then selects a data set (e.g., a song or other content), and purchases (or otherwise obtains the right to receive) a copy of the data set. (The user may transmit purchase information, for example, credit card information, using digital security that is known in the art of electronic commerce.)

3.) The SECD transmits the secured content to the LCS. Before transmitting any digital content, the SECD embeds at least one watermark and may

also transmit (perhaps through cryptography) at least one hash value along with the data being transmitted. The at least one hash value may be embedded with the at least one watermark or may be attached to the beginning or end of the data being transmitted. Alternately, the hash output may be combined in ways that are known in the art.

4.) The LCS optionally may send its public key to the SECD, in which case the SECD may use the LCS public key to apply an additional security measure to the data to be transmitted, before the data is actually transmitted to the LCS.

5.) The LCS receives the secured content transmitted by the SECD. The LCS may optionally use its private key to remove the additional layer of security which was applied with the LCS's public key.

6.) The LCS may authenticate the secure content that was received from the SECD by checking the watermark(s) and/or hash values. Optionally, the LCS may unpack the secured content from its security wrapper and/or remove any other layers of security. If the content can be authenticated, the content may be accepted into the LCS domain. Otherwise, it may be rejected.

Fragile Watermark Structure

A fragile watermark—one that is encoded in the LSB of each 16 bit sample—can actually hold all of the data that would typically comprise the information being transmitted in the SecureChannel™. At a typical sampling rate of 44.1 kHz, there is 88,200 16 bit samples for each second of data in the time domain (44,100 x 2 stereo channels). This provides 88,200 bits per second which may be used for storing a fragile watermark. A typical 3 minute stereo song could therefore accommodate 1.89 MB of data for a fragile watermark. (The watermark is called fragile, because it is easily removed without greatly sacrificing the quality of the audio data.) 1.89 MB represents an immense capacity relative to the expected size of the typical data to be transmitted in a SecureChannel (100 - 200 K).

Preferably, the fragile watermark is bound to a specific copy of a specific song, so that "information pirates" (i.e., would-be thieves) cannot detect a watermark and then copy it onto another song in an effort to feign authorization when none exists. A fragile watermark may also contain information which can be utilized by various receivers which might receive the signal being packaged. For

instance, a fragile watermark may contain information to optimize the playback of a particular song on a particular machine. A particular example could include data which differentiates an MP3 encoded version of a song and an AAC encoded version of the same song.

One way to bind a fragile watermark to a specific data set is through the use of hash functions. An example is demonstrated by the following sequence of steps:

1.) A digital data set (e.g., a song) is created by known means (e.g., sampling music at 44.1 kHz, to create a plurality of 16 bit data sets). The digital data set comprises a plurality of sample sets (e.g., a plurality of 16 bit data sets).

2) Information relative to the digital data set (e.g., information about the version of the song) is transformed into digital data (which we will call the SecureChannel data), and the SecureChannel data is then divided into a plurality of SecureChannel data blocks, each of which blocks may then be separately encoded.

3) A first block of the SecureChannel data is then is encoded into a first block of sample sets (the first block of sample sets comprising—at a minimum—a sufficient number of sample sets to accommodate the size of the first block of Secure Channel Data), for example by overwriting the LSB of each sample in the first block of sample sets.

4) A hash pool is created comprising the first block of encoded sample sets.

5) A first hash value is then created using i) the hash pool, ii) a random (or pseudorandom) number seeded using a code that serves to identify the owner of the digital data set, and iii) the SecureChannel data;

6) The first hash value is then encoded into a second block of sample sets, the second block of sample sets being sufficient in size to accommodate the size of the first hash value.

7.) The second block of sample sets is then added to the hash pool

8) A second block of the SecureChannel data is then is encoded into a third block of sample sets.

9) The third block of encoded sample sets is added to the hash pool.

10) A second hash value is then created using i) the hash pool, ii) a random (or pseudorandom) number seeded using a code that serves to identify the owner of the digital data set, and iii) the SecureChannel data;

11) The second hash value is then encoded into a fourth block of sample sets.

Steps 7-11 are then repeated for successive blocks of SecureChannel data until all of the SecureChannel data is encoded. Understand that for each block of SecureChannel data, two blocks of content data are utilized. Moreover, for efficiency, one could use a predetermined subset of the samples in the hash pool, instead of the whole block.

Each SecureChannel block may, for example, have the following structure:

```
{
    long    BlockIdentifier;        //A code for the type of block
    long    BlockLength;            //The length of the block
    ...                             //Block data of a length matching BlockLength
    char    IdentityHash[hashSize];
    char    InsertionHash[hashSize];
}
```

In theory, each SecureChannel block may be of a different type of block (i.e., may begin with a different BlockIdentifier). In operation, a software application (or even an ASIC) may read the BlockIdentifier and determine whether it is a recognized block type for the particular application. If the application does not recognize the block type, the application may use the BlockLength to skip this block of SecureChannel.

Certain block types will be required to be present if the SecureChannel is going to be accepted. These might include an identity block and a SecureChannel hash block. The SecureChannel data may or may not be encrypted, depending on whether the data is transfer-restricted (a type of value-adding component, that is, VAC) or simply informative. For instance, user-added SecureChannel data need not be encrypted. A BlockIdentifier may also be used to indicate whether a SecureChannel data block is encrypted or not.

Robust Open Watermark (ROW)

A Robust-Open Watermark may be used to divide content into three categories. (The term "open watermark" is used merely to indicate that the watermark relies on a secret which is shared by an entire class of devices, as opposed to a secure watermark—which is readable only by a single member of a class of devices.) A binary setting may be used, whereby one state (e.g., "1") may be used to identify secure protected content—such as content that is distributed in a secured manner. When the LCS detects a secured status (e.g., by determining that the ROW is "1"), the content must be accompanied by an authenticatable SecureChannel before the content is permitted to enter the LCS Domain (e.g., electronic music distribution or EMD content). The other binary state (e.g., "0") may be used to identify unsecured content, for example, non-legacy media that is distributed in a pre-packaged form (e.g. CD's). When the binary setting is "0", the content may or may not have a SecureChannel. Such "0 content" shall only be admitted from a read-only medium in its original file format (e.g., a 0 CD shall only be admitted if it is present on a Redbook CD medium). On the other hand, if the ROW is absent, then the LCS will understand that the content is "legacy". Legacy content may be admitted, or optionally, may be checked for a fragile watermark—and then admitted only if the fragile watermark is present. It would be possible to permit unfettered usage of legacy content—though again, it is the prerogative of the user who sets up the LCS.

Robust Forensic Watermark

Preferably, a robust forensic watermark is not accessible in any way to the consumer—or to "information pirates." A forensic watermark may be secured by a symmetric key held only by the seller. A transaction ID may be embedded at the time of purchase with a hash matching the symmetric key. The watermark is then embedded using a very low density insertion mask (< 10 %), making it very difficult to find without the symmetric key. Retrieval of such a watermark is not limited by real-time/low cost constraints. The recovery will typically only be attempted on known pirated material, or material which is suspected of piracy. A recovery time of 2 hours on a 400 MHz PC may, therefore, be reasonable.

Sample Embodiment - Renewability

The system of the present invention contemplates the need for updating and replacing previously-embedded watermarks (which may be thought of generally as "renewing" a watermark). If someone is able to obtain the algorithms used to embed a watermark—or is otherwise able to crack the security, it would be desirable to be able to embed a new watermark using a secure algorithm. New watermarks, however, cannot be implemented with complete success over night, and thus, there inevitably will be transition periods where older SPCS are operating without updated software. In such a transition period, the content must continue to be recognizable to both the old SPCSs and the upgraded SPCSs. A solution is to embed both the original and the upgraded watermarks into content during the transition periods. Preferably, it is the decision of the content owner to use both techniques or only the upgraded technique.

The operation of the system of the present invention is complicated, however, by the presence of "legacy" digital content which is already in the hands of consumer (that is, digital content that was commercially distributed before the advent of watermarking systems) because legacy content will continue to be present in the future. Moreover, pirates who distribute unauthorized content will also complicate matters because such unauthorized copies are likely to be distributed in the same formats as legacy content. As it is unlikely that such unwatermarked content can ever be completely removed, the present system must try to accommodate such content.

Hardware can be configured to read old ROW content and extract the old ROW and insert in the content a new ROW.

Sample Embodiment – SPCS Audio Server

Tables 1, 2 and 3 depict a sample embodiment for an SPCS Audio Server, and in particular show how secured content packages are created as downloadable units (Table 1), how the LCS works on the input side for an SPCS Audio Server (Table 2), and how the LCS works on the output side (Table 3).

While the invention has been particularly shown and described by the foregoing detailed description, it will be understood by those skilled in the art that various other changes in form and detail may be made without departing from the spirit and scope of the invention.

Table 1

SAMPLE EMBODIMENT- SPCS Audio Server Stage

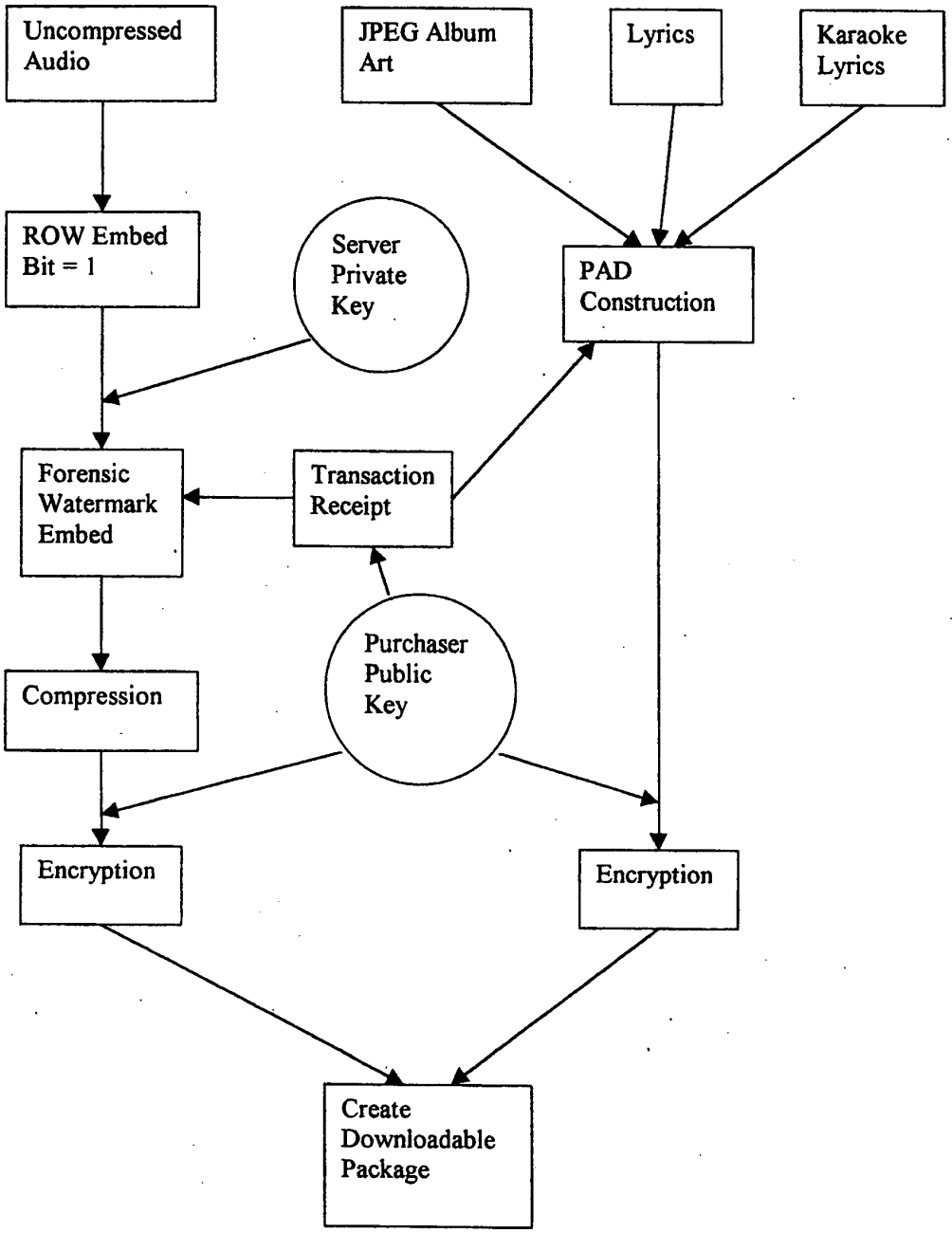


Table 2

SPCS Audio Player Input Stage

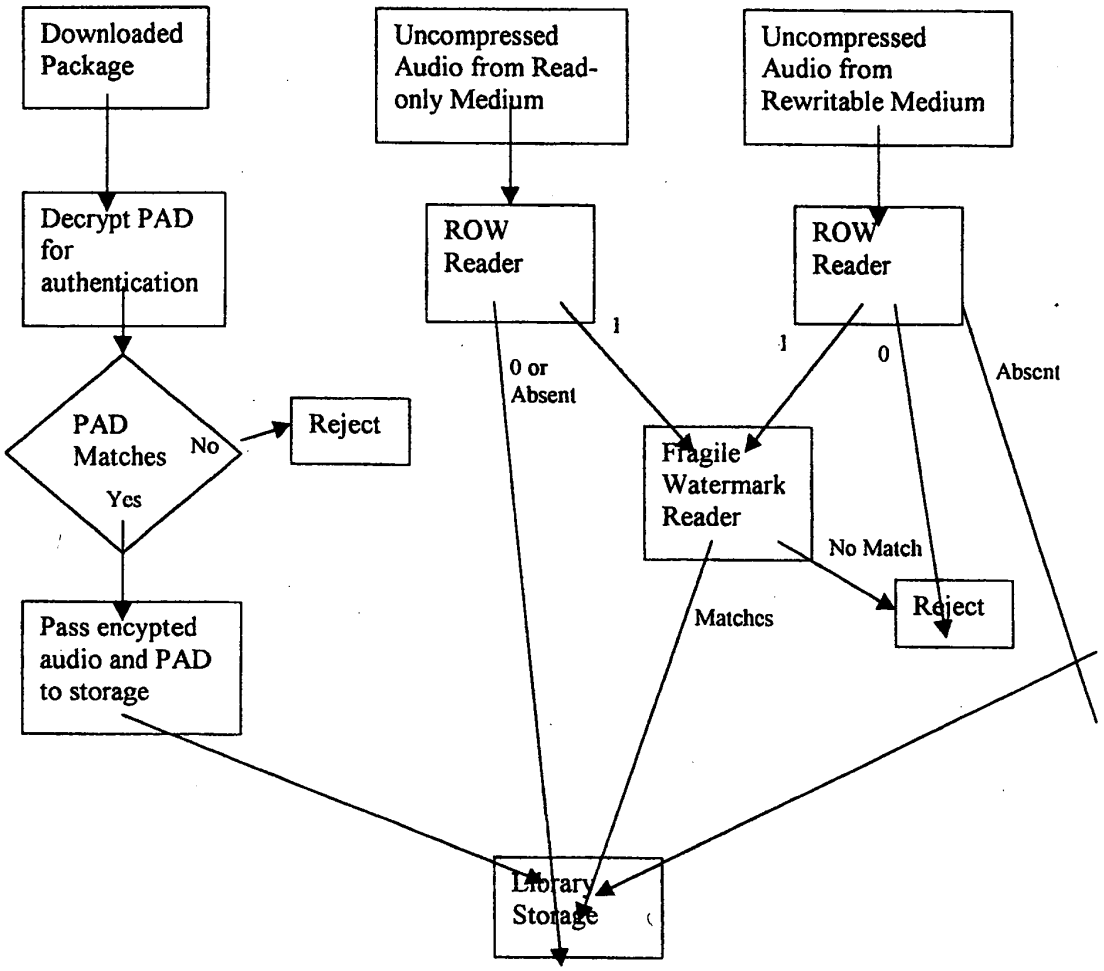
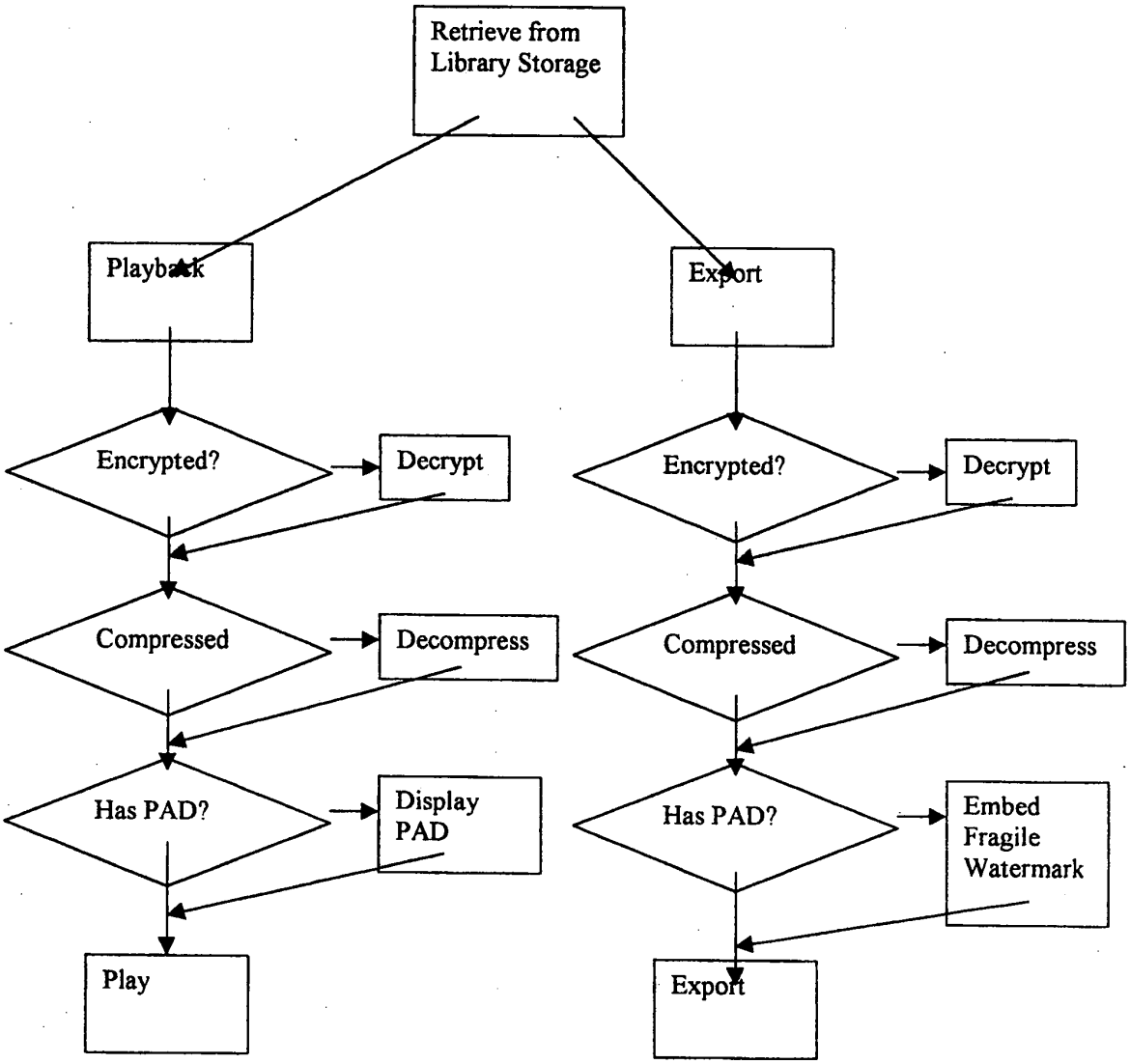


Table 3

SPCS Audio Player Output Stage



Claims:

1. A local content server system (LCS) for creating a secure environment for digital content, comprising:

a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD capable of storing a plurality of data sets, capable of receiving a request to transfer at least one content data set, and capable of transmitting the at least one content data set in a secured transmission;

b) a rewritable storage medium whereby content received from outside the LCS may be stored and retrieved;

c) a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS; and

d) a programmable address module which can be programmed with an identification code uniquely associated with the LCS; and

said domain processor permitting the LCS to receive digital content from outside the LCS provided the LCS first determines that the digital content being delivered to the LCS is authorized for use by the LCS.

2. The LCS of claim 1 further comprising

e) an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving and transmitting digital content;

and wherein said domain processor permits the LCS to receive digital content from an SECD that is connected to the LCS's communication port, provided the LCS first determines that digital content being received is authorized for use by the LCS,

and wherein said domain processor permits the LCS to deliver digital content to an SU that may be connected to the LCS's interface, provided the LCS first determines that digital content being received is authorized for use by the SU.

3. A local content server system (LCS) for creating a secure environment for digital content, comprising:

a) a communications port in communication for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD capable of storing a plurality of data sets, capable of receiving a request to transfer at least one content data set, and capable of transmitting the at least one content data set in a secured transmission;

b) an interface to permit the LCS to communicate with one or more Satellite Units (SU) which may be connected to the system through the interface, said SUs capable of receiving and transmitting digital content; and

c) a rewritable storage medium whereby content received from an SECD and from an SU may be stored and retrieved;

d) a domain processor that imposes rules and procedures for content being transferred between the LCS and the SECD and between the LCS and the SU; and

e) a programmable address module which can be programmed with an identification code uniquely associated with the LCS;

said domain processor permitting the LCS to deliver digital content to and receive digital content from an SU that is connected to the LCS's interface, provided the LCS first determines that the digital content being delivered to the SU is authorized for use by the SU or that the digital content being received is authorized for use by the LCS,

and said domain processor permitting the LCS to receive digital content from an SECD that is connected to the LCS's communication port, provided the LCS first determines that digital content being received is authorized for use by the LCS.

4. The system of claim 3, wherein said domain processor determines whether digital content is authorized for use by extracting a watermark from the digital content being transferred.

5. The system of claim 3, wherein said domain processor comprises:

means for obtaining an identification code from an SU connected to the LCS's interface;

an analyzer to analyze the identification code from the SU to determine if the SU is an authorized device for communicating with the LCS;

means for analyzing digital content received from an SU;

said system permitting the digital content to be stored in the LCS if i) an analysis of the digital content received from the SU concludes that the content is authenticated, or ii) an analysis of the digital content received from the SU concludes that the content cannot be authenticated because no authentication data is embedded in the content, and

said system preventing the digital content from being stored on the LCS if i) an analysis of the digital content received from the SU concludes that the content is unauthenticated.

6. The system of claim 4, wherein said analyzer of the domain processor comprises means for extracting digital watermarks from the digital content received from an SU, and means for analyzing the digital watermark to determine if the digital content has been previously marked with the unique identification code of the LCS.

7. The system of claim 4, wherein said system permits the digital content to be stored in the LCS at a degraded quality level if an analysis of the digital content received from the SU concludes that the digital content received from the SU cannot be authenticated because there is no authentication data embedded in the content.

8. The system of claim 4, further comprising at least one SU, each such SU being capable of communicating with the LCS.

9. The system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:

means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means to retrieve a copy of the requested content data set;

means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS; and

means to deliver the watermarked content data set to the SU for its use.

10. The system of claim 8, further comprising a SECD, said SECD capable of receiving a request to transfer at least one data set and capable of transmitting the at least one data set in a secured transmission.

11. The system of claim 10,

wherein the SU includes means to send a message to the LCS indicating that the SU is requesting a copy of a content data set that is not stored on the LCS, but which the LCS can obtain from an SECD, said message including information about the identity of the SU;

wherein the SECD comprises:

means to retrieve a copy of the requested content data set;

means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the LCS; and

means to deliver the watermarked content data set to the LCS for its use; and

wherein the LCS comprises:

means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means to receive a copy of the requested content data set as transmitted by the SECD;

means to extract at least one watermark to confirm that the content data is authorized for use by the LCS;

means to embed at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the SU and information about the LCS; and

means to deliver the watermarked content data set to the SU for its use.

12. The system of claim 8, wherein the SU has means to sending a message to the LCS indicating that the SU is requesting to store a copy of a content data set on a storage unit of the LCS, said message including information about the identity of the SU, and wherein the LCS comprises:

means to analyze the message from the SU to confirm that the SU is authorized to use the LCS;

means receive a copy of the content data set;

means to determine if a robust open watermark is embedded in the content data set, and to extract the robust open watermark if is it is determined that one exists;

means to analyze any extracted robust open watermarks to determine if the content data set can be authenticated;

means to permit the storage of the content data set on a storage unit of the LCS if i) the LCS authenticates the content data set, or ii) the LCS determines that no robust open watermark is embedded in the content signal.

13. The system of claim 4, further comprising at least one SU, each such SU being capable of communicating with the LCS, and being capable of using only data which has been authorized for use by the SU or which has been determined to be legacy content such the data contains no additional information to permit authentication.

14. The system of claim 5, wherein the LCS further comprises:

means to embed at least one robust open watermark into a copy of content data, said watermark indicating that the copy is authenticated;

means to embed a second watermark into the copy of content data, said second watermark being created based upon information comprising information uniquely associated with the LCS; and

means to embed a third watermark into the copy of content data, said third watermark being a fragile watermark created based upon information which can enhance the use of the content data on one or more SUs.

15. The system of claim 5, wherein the LCS further comprises:

means for encrypting or scrambling content data, such that content data may be encrypted or scrambled before it is stored in the rewritable storage medium.

16. A system for creating a secure environment for digital content, comprising:

a Secure Electronic Content Distributor (SECD);

a Local Content Server (LCS);

a communications network interconnecting the SECD to the LCS; and

a Satellite Unit (SU) capable of interfacing with the LCS;

said SECD comprising: a storage device for storing a plurality of data sets; an input for receiving a request from the LCS to purchase a selection of at least one of said plurality of data sets; a transaction processor for validating the request to purchase and for processing payment for the request; a security module for encrypting or otherwise securitizing the selected at least one data set; and an output for transmitting the selected at least one data set that has been encrypted or otherwise secured for transmission over the communications network to the LCS;

said LCS comprising: a domain processor; a first interface for connecting to a communications network; a second interface for communicating with the SU; a memory device for storing a plurality of data sets; and a programmable address module which can be programmed with an identification code uniquely associated with the LCS; and

said SU being a portable module comprising: a memory for accepting secure digital content from a LCS; an interface for communicating with the LCS; and a programmable address module which can be programmed with an identification code uniquely associated with the SU.

17. A Method for creating a secure environment for digital content for a consumer, comprising the following steps:

sending a message indicating that a user is requesting a copy of a content data set;

retrieving a copy of the requested content data set;

embedding at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;

embedding a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the requesting user;

transmitting the watermarked content data set to the requesting consumer via an electronic network;

receiving the transmitted watermarked content data set into a Local Content Server (LCS) of the user;

extracting at least one watermark from the transmitted watermarked content data set; and

permitting use of the content data set if the LCS determines that use is authorized.

18. The Method of claim 17, wherein the step of permitting use of the content data set if the LCS determines that use is authorized comprises:

checking to see if a watermark extracted from the content data set includes information which matches unique information which is associated with the user; and

permitting the storage of the content data set in a storage unit for the LCS.

19. The Method of claim 17, further comprising:

connecting a Satellite Unit (SU) to an LCS,

and wherein the step of permitting use of the content data set if the LCS determines that use is authorized comprises:

checking to see if a watermark extracted from the content data set includes information which matches unique information which is associated with the user; and

embedding a watermark into the content data set using information that is associated with the user and information that is associated with an SU;

delivering the content data set to the SU for its use.

20. A Method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit to an local content server (LCS),

sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU;

analyzing the message to confirm that the SU is authorized to use the LCS; and

retrieving a copy of the requested content data set;

assessing whether a secured connection exists between the LCS and the SU;

if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS; and

delivering the content data set to the SU for its use.

21. The Method of claim 20, further comprising:

embedding an open watermark into the content data to permit enhanced usage of the content data by the user.

22. The Method of claim 21, further comprising:

embedding at least one additional watermark into the content data, said at least one additional watermark being based on information about the user, the LCS and an origin of the content data, said watermark serving as a forensic watermark to permit forensic analysis to provide information on the history of the content data's use.

23. The method of claim 20, wherein the content data can be stored at a level of quality which is selected by a user.

24. A Method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit (SU) to an local content server (LCS),

sending a message indicating that the SU is requesting a copy of a content data set that is stored on the LCS, said message including information about the identity of the SU;

analyzing the message to confirm that the SU is authorized to use the LCS; and

retrieving a copy of the requested content data set;

assessing whether a secured connection exists between the LCS and the SU;

if a secured connection exists, embedding a watermark into the copy of the requested content data set, said watermark being created based upon information transmitted by the SU and information about the LCS; and

delivering the watermarked content data set to the SU for its use.

25. The method of claim 24, further comprising:

embedding at least one robust open watermark into the copy of the requested content data set before the requested content data is delivered to the SU, said watermark indicating that the copy is authenticated.

26. The method of claim 25, wherein the robust watermark is embedded using any one of a plurality of embedding algorithms.

26. The method of claim 24, further comprising:

embedding a watermark which includes a hash value from a one-way hash function generated using the content data.

27. The method of claim 25, wherein the robust watermark can be periodically replaced with a new robust watermark generated using a new algorithm with payload that is no greater than that utilized by the old robust watermark.

28. The method of claim 24, further comprising the step of:

embedding additional robust open watermarks into the copy of the requested content data set before the requested content data is delivered to the SU, using a new algorithm; and

re-saving the newly watermarked copy to the LCS.

29. The method of claim 24, further comprising the step of:

saving a copy of the requested content data with the robust watermark to the rewritable media of the LCS.

30. A Method for creating a secure environment for digital content for a consumer, comprising the following steps:

connecting a Satellite Unit (SU) to an local content server (LCS),

sending a message indicating that the SU is requesting to store a copy of a content data on the LCS, said message including information about the identity of the SU;

analyzing the message to confirm that the SU is authorized to use the LCS; and

receiving a copy of the content data set;

assessing whether the content data set is authenticated;

if the content data is unauthenticated, denying access to the LCS storage unit; and

if the content data is not capable of authentication, accepting the data at a predetermined quality level, said predetermined quality level having been set for legacy content.

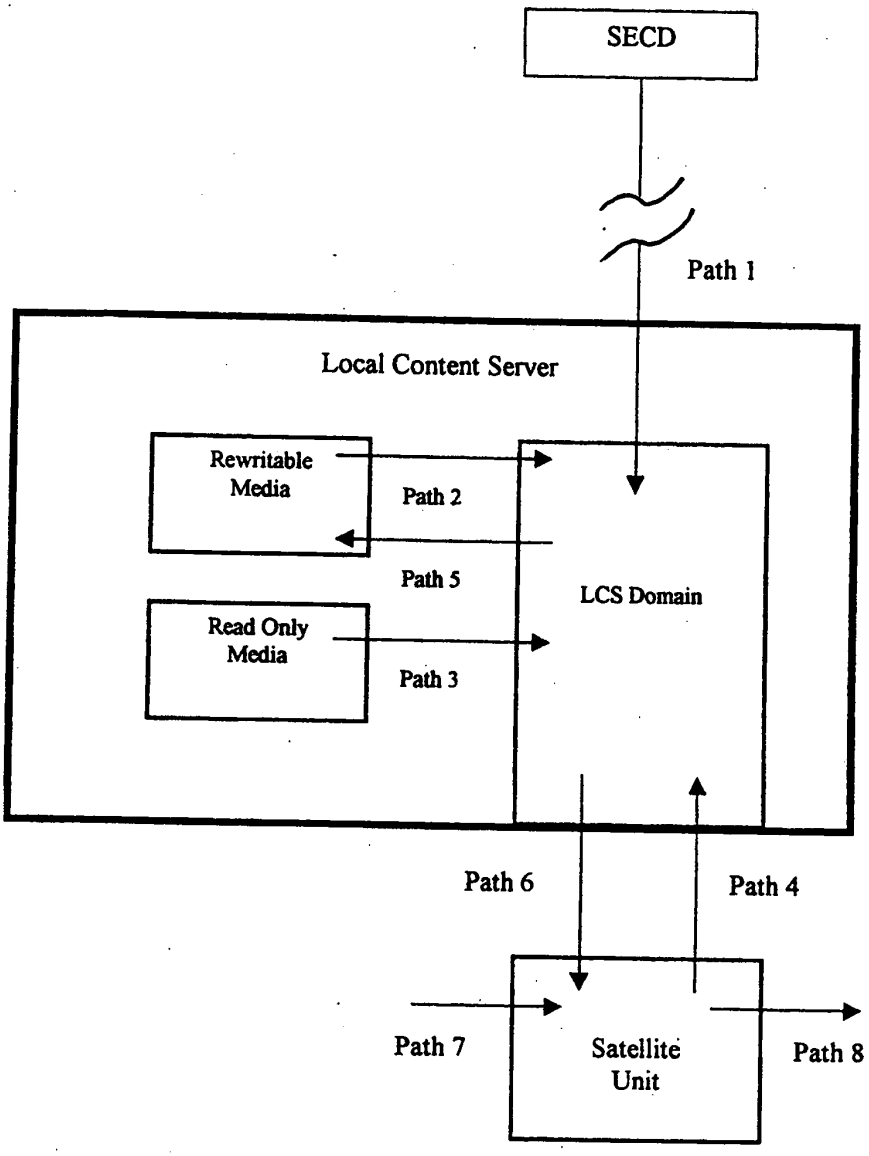

SECD
Path 1
Local Content Server
Rewritable Media
Path 2
Path 5
LCS Domain
Read Only Media
Path 3
Path 6
Path 4
Path 7
Satellite Unit
Path 8

FIG. 1

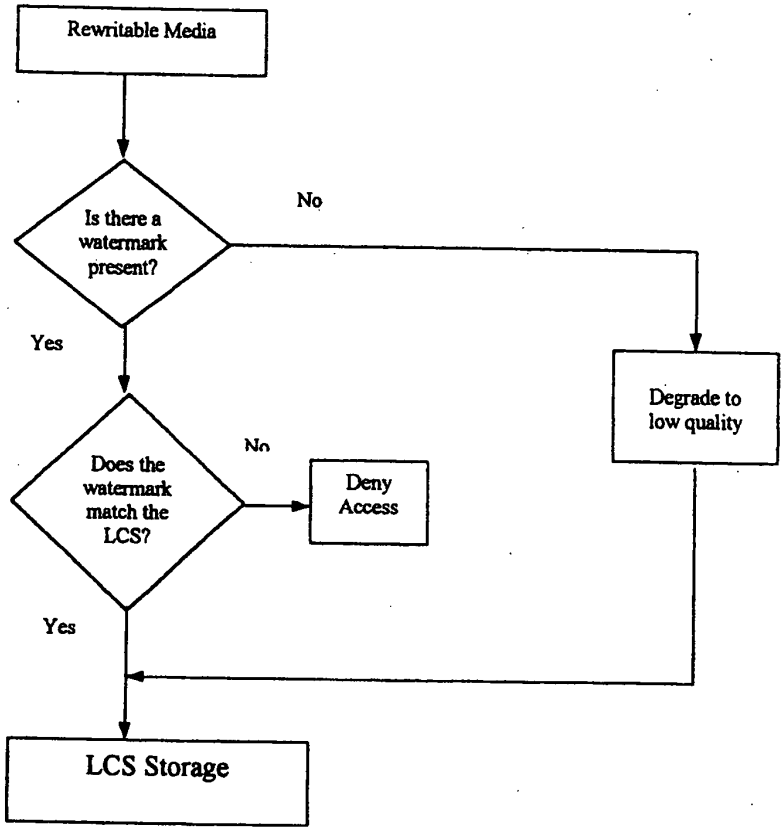

Rewritable Media
Is there a watermark present?
No
Yes
Degrade to low quality
Does the watermark match the LCS?
No
Deny Access
Yes
LCS Storage

FIG. 2

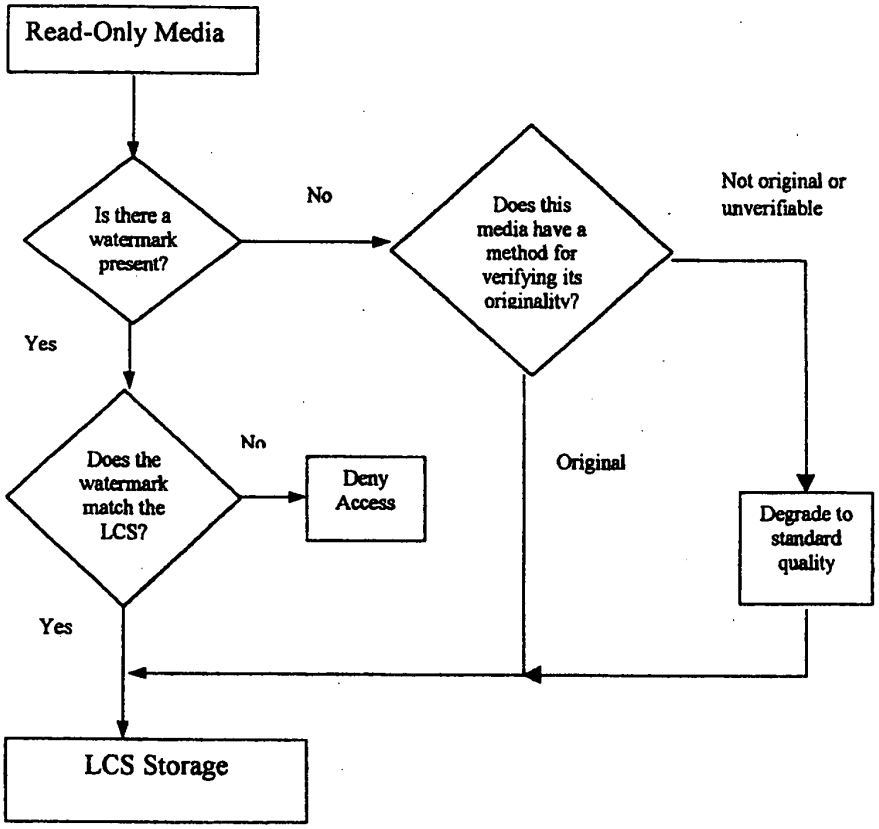

Read-Only Media
Is there a watermark present?
No
Does this media have a method for verifying its originality?
Not original or unverifiable
Yes
Does the watermark match the LCS?
No
Deny Access
Original
Degrade to standard quality
Yes
LCS Storage

FIG. 3

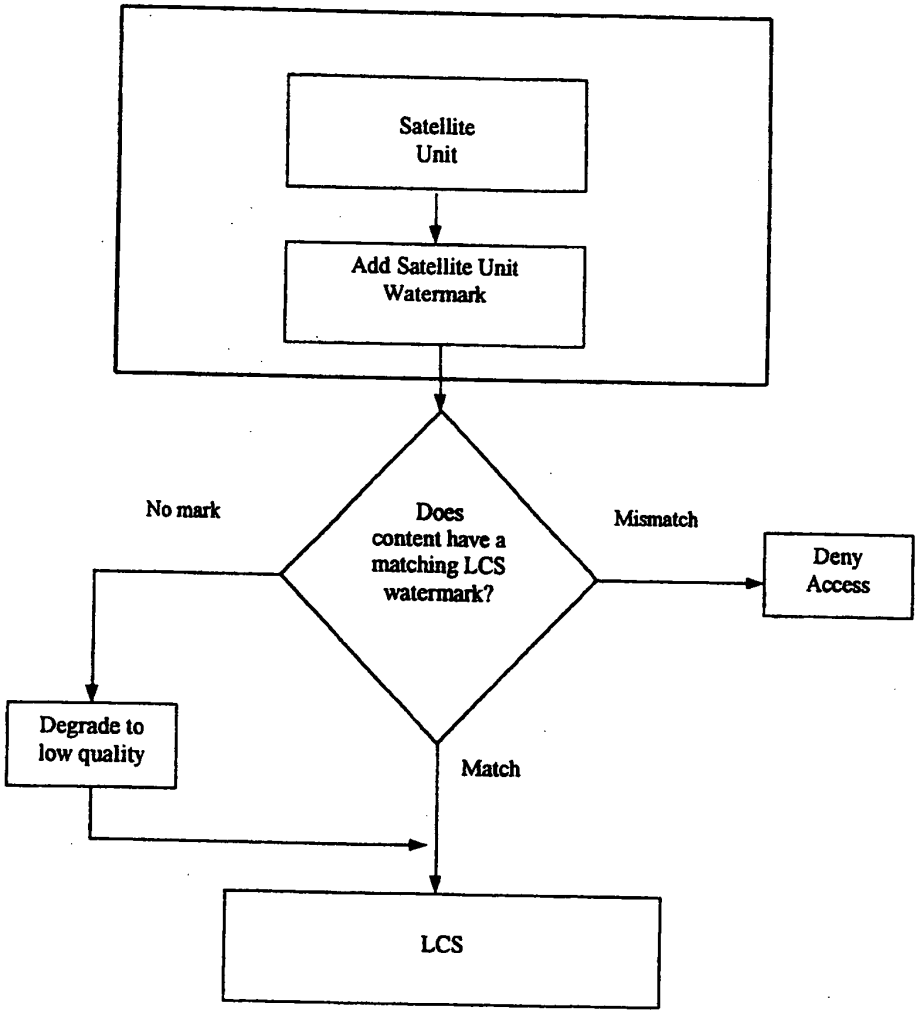

Satellite Unit
Add Satellite Unit Watermark
Does content have a matching LCS watermark?
No mark
Mismatch
Deny Access
Degrade to low quality
Match
LCS

FIG. 4

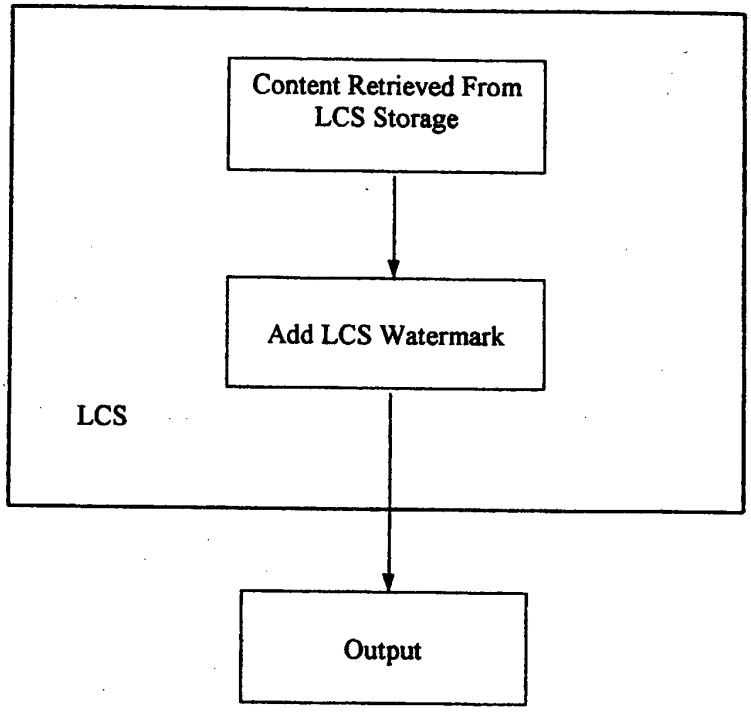

Content Retrieved From LCS Storage
Add LCS Watermark
LCS
Output

FIG. 5

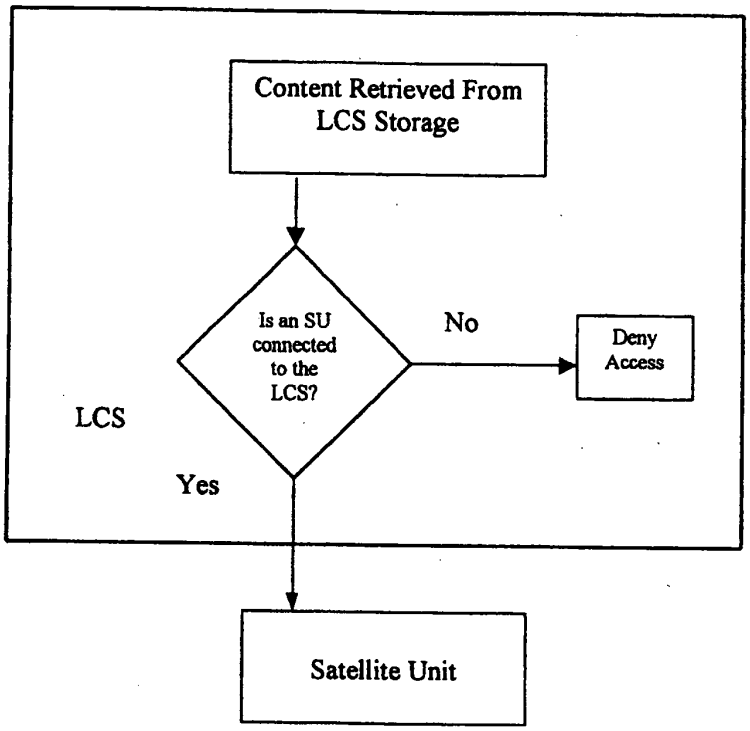

Content Retrieved From LCS Storage
Is an SU connected to the LCS?
No
Deny Access
LCS
Yes
Satellite Unit

FIG. 6

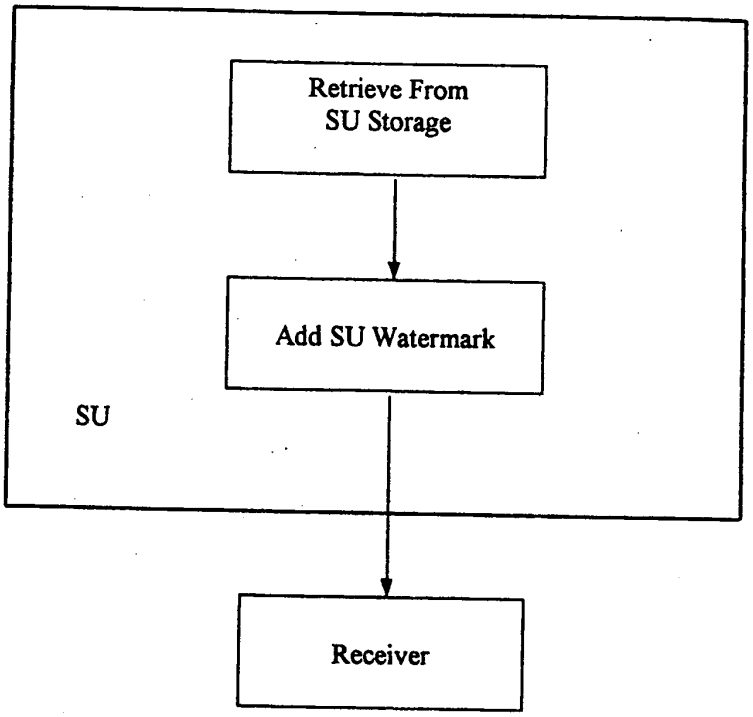


FIG. 7

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 June 2001 (14.06.2001)

PCT

(10) International Publication Number
WO 01/43026 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US00/33126

(22) International Filing Date: 7 December 2000 (07.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/169,274	7 December 1999 (07.12.1999)	US
09/456,319	8 December 1999 (08.12.1999)	US
09/545,589	7 April 2000 (07.04.2000)	US
09/594,719	16 June 2000 (16.06.2000)	US
PCT/US00/21189	4 August 2000 (04.08.2000)	US
09/657,181	7 September 2000 (07.09.2000)	US
60/234,199	20 September 2000 (20.09.2000)	US
09/671,739	29 September 2000 (29.09.2000)	US
Not furnished	7 December 2000 (07.12.2000)	US

(71) Applicant *(for all designated States except US)*: **BLUE SPIKE, INC.** [US/US]; 16711 Collins Avenue, #2505, Miami, FL 33160 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MOSKOWITZ, Scott, A.** [US/US]; 16711 Collins Avenue, #2505, Miami, FL 33160 (US).

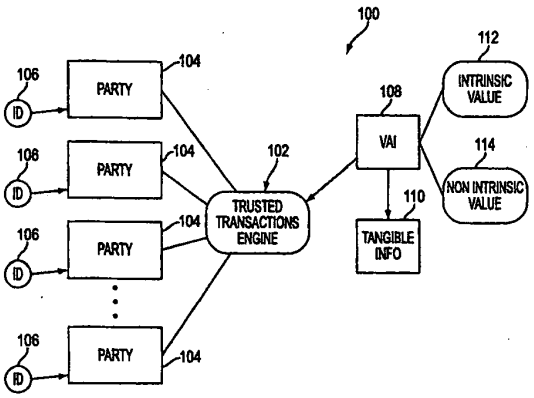
(74) Agents: **CHAPMAN, Floyd, B.** et al.; Intellectual Property Department, Brobeck, Phleger & Harrison LLP, Suite 800, 1333 H Street, N.W., Washington, DC 20005 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEMS, METHODS AND DEVICES FOR TRUSTED TRANSACTIONS



(57) Abstract: The invention discloses a system for enhancing trust in transactions, most particularly in remote transactions between a plurality of transactional parties, for instance a seller and buyer(s) of goods and/or services over a public computer network such as the internet. Trust is disclosed to be a multivalent commodity, in that the trust that is to be enhanced relates to information about the subject matter of the transactions (e.g., the suitability of the goods and services sold), the bona fides of the supplier of the goods and services, the appropriateness of a pricing structure for a particular transaction or series of transactions, a quantum of additional transactional value that may be imparted to the transactional relationship, security of information exchange, etc. An important contributor to trust for such aspects of the transaction is disclosed to be the use of highly-secure steganographic computer processing means for data identification, authentication, and transmission, such that confidence in the transaction components is enhanced. By providing an integrated multivalent system for enhancing trust across a variety of categories (for a variety of transaction species, including those in which the need for trust is greater on the part of one party than of another, as well as those in which both require substantial trust enhancement), the invention reduces barriers to forming and optimizing transactional relationships.

WO 01/43026 A1

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEMS, METHODS AND DEVICES FOR TRUSTED TRANSACTIONS

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to the transfer of information between parties; in particular, it relates to systems, methods, and devices for trusted transactions.

2. Description of the Related Art

Transactions are increasingly characterized by the amount and quality of information available to market participants. Whereas a seller seeks profit driven arrangements, which may vary over the course of a relationship with a particular buyer or consumer; buyers seek satisfaction of at least one of the following: price, selection or service. At any time the buyer or seeker of value-added information may lack recognition of the seller or provider of such information, even if coupled with a "manufactured" product or good. Sellers, or providers, similarly lack any information about individual buyers, buying groups or agents, and may only have information regarding potentially profitable transaction events defined by at least one of the following: existing market for goods or services, targeted projected market for new goods or services, or those consumers or buyers who currently engage in transactions with the provider. Transactions are the result of customer profiling, a form of recognizable pattern analysis for commerce.

Transactions conducted electronically, often in an online environment taking advantage of networks, such as the Internet and/or World Wide Web ("WWW"), form an increasingly-important subset of transactions. Most obviously, retail sales transactions in which individual customers purchase goods or services from a central web server using a WWW connection have become a prominent form of electronic transactions, though such transactions are by no means the only or even necessarily the predominant category of electronic transactions.

Electronic transactions pose special challenges for transaction parties. Some of these challenges relate to the difficulty of providing to a prospective acquirer (e.g., a purchaser) of goods or services full, accurate, and verifiable information regarding the nature, value, authenticity, and other suitability-related characteristics of the product in question. This is true in part, for instance, because the customer

cannot necessarily handle, sample, or evaluate at first hand the goods or services in question in an online transaction to the same extent to which he could evaluate them in an in-person transaction. It may also be true because of the fear of counterfeit, defective, or otherwise unsuitable products that may be viewed as more easily "passed off" (assuming a certain non-zero incidence of deceit and/or inadequate suitability verification among suppliers of products) in an electronic transaction than in an in-person transaction.

Further challenges in online transactions revolve around the serious concerns regarding security of such transactions. Such security-related concerns arise from the inherently-vulnerable nature of distributed public networks such as the internet, in which transaction parties cannot necessarily determine the path by which data travelling to and from them will take. Nor is it always possible to determine the identity of another transaction party, or to ensure that such other transaction party will take adequate precautions with sensitive data (for instance, data related to the identity or financial details (e.g., credit card number) of the first transaction party) transmitted during the course of proposing, evaluating, negotiating, executing, or fulfilling a transaction. Thus, concerns are raised about interception, inadequate safeguarding, or other unauthorized or inappropriate use of data generated or transmitted between transaction parties. Such concerns have raised the perceived need for security technologies adaptable for online transactions. Generically, these technologies have included encryption, scrambling, digital watermarking, and like methods of protecting transaction-related data.

Two conventional techniques for providing confidentiality and/or authentication currently in use involve reciprocal and non-reciprocal encrypting. Both systems use non-secret algorithms to provide encryption and decryption, and keys that are used by the algorithm.

In reciprocal algorithm systems, such as DES, the same key and algorithm is used to encrypt and decrypt a message. To assure confidentiality and authenticity, the key is preferably known only to the sending and receiving computers, and were traditionally provided to the systems by "secure" communication, such as courier.

In non-reciprocal systems, such as those described in U.S. Patent 4,218,582, a first party to a communication generates a numerical sequence and uses that -

sequence to generate non-reciprocal and different encrypting and decrypting keys. The encrypting key is then transferred to a second party in a non-secure communication. The second party uses the encrypting key (called a public key because it is no longer secure) to encrypt a message that can only be de-crypted by the decrypting key retained by the first party. The key generation algorithm is arranged such that the decrypting key cannot be derived from the public encrypting key. Similar methods are known for using non-reciprocal keys for authentication of a transmission. In the present invention, the non-secure "public" key is used to a message that has been encrypted using a secure "private" key known only to the originating party. In this method the receiving party has assurance that the origination of the message is the party who has supplied the "public" decrypting key.

SUMMARY OF THE INVENTION

Thus, a need has arisen for a system and method for enhancing trust on the part of participants in transaction. This may be with respect to all aspects of the transaction as to which trust may be an influential factor (or, viewed negatively, in which the lack of trust may be a potential bottleneck prohibiting consummation of the transaction, or of a more-optimal transaction, or of a series of transactions in a mutually-beneficial transactional relationship).

A need has also arisen for trust enhancement for transactions in connection with sophisticated security, scrambling, and encryption technology, for instance that provided by steganographic encryption, authentication, and security means.

A need has also arisen to provide these technologies in an integrated method and system, optimally requiring comparatively little processing resources so as to maximize its usefulness and minimize its cost.

The present invention represents a bridge between mathematically determinable security and analog or human measures of trust. These measures are typically perceptible or perceptual when evaluating value-added information. Additionally, a higher level of transparency between parties is assured, because information flow is recognizable and controllable by transacting parties at will.

According to one embodiment of the present invention, a method for trusted transactions is provided. The method includes the steps of (1) establishing an

agreement to exchange digitally-sampled information between a first and a second party; (2) exchanging the digitally-sampled information between the first and the second party; and (3) approving the digitally-sampled. The digitally-sampled information may be approved with an approval element, for example, a predetermined key, a predetermined message, or a predetermined cipher. The step of approving the digital information may include authorizing the digital information with the approval element, verifying the digital information with the approval element, or authenticating the digital information with the approval element. The predetermined cipher may be a steganographic cipher or a cryptographic cipher.

According to another embodiment of the present invention, a method for conducting a trusted transaction between two parties that have agreed to transact is provided. The method includes the steps of (1) establishing a secure transmission channel between the two parties; (2) verifying an identity of at least one of the parties; (3) determining an amount of value-added information to be exchanged between the parties; (4) verifying the agreement to transact; and (5) transmitting the value-added information. The value-added information may include value-adding components.

According to another embodiment of the present invention, a method for conducting at least one trusted transaction between two parties is provided. The method includes the steps of (1) authenticating the parties; (2) agreeing to a security of a transmission channel; (3) exchanging secondary value-added information; (4) determining at least one term for a primary value-added information exchange; and (5) facilitating payment for the transaction based on the terms.

According to another embodiment of the present invention, a method for conducting a trusted transaction between two parties is provided. The method includes the steps of (1) establishing a steganographic cipher; (2) exchanging secondary value-added information between the parties; (3) agreeing to terms for the exchange of primary value-added information; and (4) facilitating payment for the transaction.

According to another embodiment of the present invention, a method for conducting a trusted transaction between parties is provided. The method includes the steps of (1) identifying a unique identification for each of the parties, a unique

identification of the transaction, a unique identification of value-added information to be transacted, or a unique identification of a value-adding component; (2) applying a steganographic cipher; and (3) verifying an agreement to transact between the parties. Once the parties are identified by the unique identification, transaction identification, or the unique identification of the value-added information, secondary terms and conditions may be offered for acceptance. The transaction may take several additional steps and may include additional value-adding components to reach a legal agreement.

The agreement may cause a secondary term to be enabled for one of the parties. For example, the agreement may be related to the ability to choose ownership in the seller instead of some benefit in price, service or selection. This ownership may be priced according to traditional options pricing methodologies. Essentially the "discount" in cash value terms, may be the option price. So if there is a price, selection or service that can be equated to some cash equivalent amount, that amount can be used by the buyer as a right, but not obligation to purchase equity in the seller. Alternatively, the cash equivalent may have a direct equivalence in equity prices.

According to another embodiment of the present invention, a method for bi-directionally exchanging value-added information between parties is provided. The method includes the steps of (1) associating a plurality of unique identifiers with the value-added information, the value-added information including a digital watermark, a file header, a file attachment, and/or a file wrapper; (2) associating each of the parties with unique identifiers, the unique identifiers including a digital watermark, a file header, a file attachment, and/or a file wrapper; and (3) exchanging value-added information between the parties.

According to another embodiment of the present invention, a method for exchanging value-added information between parties is provided. The method includes the steps of (1) providing a data transmission means; (2) verifying the parties to the transaction; (3) negotiating a term. such as a price, a service, and/or a selection; and (4) binding the term to the information using a digital watermark, a file header, metadata, and/or a file wrapper. The bound transaction terms may include value-added information.

According to another embodiment of the present invention, a method for trusted transactions is provided. The method includes the steps of (1) receiving data to be processed; (2) determining a structure of the data; (3) determining if the data is authentic; and (4) determining an associated usage of the data based on the data structure and the authenticity of the data.

According to another embodiment of the present invention, a method for secure transaction is provided. The method includes the steps of (1) receiving a request to process a transaction; (2) uniquely identifying the source of the request; (3) uniquely identifying at least one term of the request; and (4) storing identification information for transaction negotiation.

According to another embodiment of the present invention, a method for the facilitation of the exchange of information data between at least a first party and a second party is provided. The method includes the steps of (1) receiving a rule governing information data from a first party; (2) receiving a request for the information data from a second party; (3) matching the predetermined rule with the request; and (4) uniquely identifying the information data and the first and second parties. The information data may include unstructured data or structured data.

According to another embodiment of the present invention, a method for the management of rights is provided. The method includes the steps of (1) receiving information; (2) determining whether the information is structured information or unstructured information; (3) identifying the information with a steganographic cipher; (4) authenticating the information with a digital signature or a digital watermark check; and (5) associating the identification and authentication results with a predetermined record, a predetermined rule, or a predetermined function.

According to another embodiment of the present invention, a method for risk management is provided. The method includes the steps of (1) receiving information; (2) determining whether the information is structured or unstructured; (3) identifying information with a predetermined ciphered key; (4) authenticating information with a digital signature, a digital watermark check, or a predetermined ciphered key; (5) associating identification and authentication results with a predetermined rule; and (6) limiting access based on a predetermined exposure of a decision maker.

According to another embodiment of the present invention, a method for securely exchanging information data between parties is provided. The method includes the steps of (1) creating a private key; (2) deriving a corresponding public key corresponding to the information data sought and at least one of (a) verifiable data associated with different versions of the information data, (b) verifiable data associated with a transmitting device, and (c) verifiable data associated with an identity of the party seeking the information data; (3) establishing a set of one time signatures relating to the information data; (4) establishing a hierarchy of access to the set of one time signatures; (5) creating a public key signature, the public key signature being verifiable with the public key, including the hierarchy of access to the set of one time signatures; (6) providing the information to a certification authority for verification; and (7) verifying the one time signature and the hierarchy of access to enable transfer of predetermined data.

According to another embodiment of the present invention, a method for authenticating an exchange of a plurality of sets of information data between parties is provided. The method includes the steps of (1) creating a plurality of hierarchical classes based on a perceptual quality of the information data; (2) assigning each set of information data to a corresponding hierarchical class; (3) defining access to each hierarchical classes and to each set of information data based on at least one recognizable feature of the information data to be exchanged; (4) predetermining access to the sets of information data by perceptually-based quality determinations; (5) establishing at least one connection between the exchanging parties; (6) perceptually recognizing at least one of the sets of information data dependent on user provided value-added information data; and (7) enabling a trusted transaction based on verification, and associated access, governing at least one of a set of information data sets.

According to another embodiment of the present invention, a method for authenticating the exchange of perceptual information data between parties over a networked system is provided. The method includes the steps of (1) creating a plurality of hierarchical classes based on a perceptual quality of the information data; (2) assigning each set of information data to a corresponding hierarchical class; (3) defining access to each hierarchical classes and to each set of information data

based on at least one recognizable feature of the information data to be exchanged; (4) perceptually recognizing at least one of the sets of information data dependent on user provided value-added information data; (5) enabling a trusted transaction of the information data based on verification of means of payment, and associated access, governing at least one copy of the information data sought; (6) associating the transaction event with the information data prior to transmission of the information data; and (7) transmitting and confirming delivery of the information data

According to another embodiment of the present invention, a device for conducting a trusted transaction between parties who have agreed to transact is provided. The device includes means for uniquely identifying unique identification information, such as a unique identification of one of the parties, a unique identification of the transaction, a unique identification of value-added information to be transacted, or a unique identification of a value-adding component; a steganographic cipher; and a means for verifying an agreement to transact between the parties.

According to another embodiment of the present invention, a device for conducting a trusted transaction between parties who have agreed to transact is provided. The device includes means for uniquely identifying unique identification information such as a unique identification of one of the parties, a unique identification of the transaction, a unique identification of value-added information to be transacted, or a unique identification of a value-adding component; and means for enabling a subsequent mutually agreed to at least one term.

According to another embodiment of the present invention, a device for conducting trusted transactions between parties us provided. The device includes a steganographic cipher; a controller for receiving input data or outputting output data; and an input/output connection. The device may have a unique identification code.

According to another embodiment of the present invention, a trusted transaction device for transmitting authentic value-added information data between parties is provided. The device includes a display; a unique identifier; means for ciphering information that is input and output; means for interacting with other similarly functional devices; and means for storing or retrieving value-added information and a value-adding component.

According to another embodiment of the present invention, a device for securely exchanging information data is provided. The device includes means for creating a private key by the party seeking information; means for deriving a corresponding public key based on the predetermined data and verifiable data associated with different versions of the information, verifiable data associated with a transmitting device, or verifiable data associated with the identity of the party seeking information; means for creating a set of one-time signatures relating to the predetermined data; means for validating a predetermined hierarchy of access of the set of one-time signatures; means for creating a public key signature, verifiable with the public key, including the access hierarchy of one time signatures; means for securely transacting predetermined data by providing information relating to a proposed transaction; and means for verifying the one time signature and the hierarchy of access to enable transfer of predetermined data.

According to one embodiment of the present invention, a system for the secure exchange of predetermined, verifiable information data between parties is provided. The system includes at least one condition for the use of the information; means for differentiating between predetermined information and other seemingly identical information based on an authentication protocol; means for associating authenticity of verifiable information data with at least one condition for use; a storage unit for storing the predetermined, verifiable information; and means for communicating with the predetermined, verifiable information storage.

According to one embodiment of the present invention, a system for the exchange of information is provided. The system includes at least one sender; at least a receiver; a verifiable message; and a verification of the message by at least one of the senders and the receivers. A verification of the message may enable a decision over receiving additional related information.

According to one embodiment of the present invention, a system for computer based decision protocol is provided. The system includes a means for identifying between structured and unstructured information; a means for authenticating structured information; and a means for enabling a decision rule based on the identity and authenticity of the information.

According to one embodiment of the present invention, a system for computer-based decision protocol is provided. The system includes means for identifying between structured and unstructured information; means for identifying structured information; and means for enabling a predetermined decision rule based on the identity of the information.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, the objects and advantages thereof, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

Fig. 1 is a block diagram of a system for trusted transactions according to one embodiment of the present invention;

Fig. 2 is a schematic of a local content server environment according to one embodiment of the present invention;

Fig. 3 is a flowchart depicting an example of an authentication according to one embodiment of the present invention;

Fig. 4 is a flowchart depicting an example of content flow according to one embodiment of the present invention;

Fig. 5 is a flowchart depicting an example of content flow according to one embodiment of the present invention;

Fig. 6 is a flowchart depicting an example of content flow according to one embodiment of the present invention;

Fig. 7 is a flowchart depicting an example of content flow according to one embodiment of the present invention;

Fig. 8 is a flowchart depicting an example of content flow according to one embodiment of the present invention;

Fig. 9 is a flowchart of a method for trusted transactions according to one embodiment of the present invention;

Fig. 10 depicts a device for trusted transactions according to one embodiment of the present invention.

Fig. 11 is a block diagram of a person information device according to one embodiment of the present invention;

Fig. 12 is a block diagram of an authentication device according to one embodiment of the present invention; and

Fig. 13 is a flowchart depicting an authentication process according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In order to assist in the understanding of the present invention, the following definitions are provided and are intended to supplement the ordinary and customary meaning of the terms:

Authentication: A receiver of a "message" (embedded or otherwise within the value-added information) preferably is able to ascertain the origin of the message (or by effects, the origin of the carrier within which the message is stored). An intruder preferably cannot successfully represent someone else. Additional functionality, such as message authentication codes, may be incorporated (a one-way hash function with a secret key) to ensure limited verification or subsequent processing of value-added data.

Authorization: A term which is used broadly to cover the acts of conveying official sanction, permitting access or granting legal power to an entity.

Encryption: Encryption is a method of securitizing data. For example, encryption may be data scrambling using keys. For value-added or information rich data with content characteristics, encryption is typically slow or inefficient because content file sizes tend to be generally large. Encrypted data is sometimes referred to as "ciphertext."

High Quality: A transfer path into the LCS Domain that allows digital content of any quality level to pass unaltered. "High Quality" can also mean unfettered access to all VACs.

Local Content Server (LCS): A device or software application that can securely store a collection of value-added digital information, such as entertainment media. The LCS has a unique ID.

LCS Domain: A secure medium or area where digital content can be stored, with an accompanying rule system for transfer into and out of itself.

Low Quality: A transfer path into the LCS Domain that degrades the digital content to a sub-reference level. In an audio implementation, this might be defined

as below CD Quality. Low Quality can also mean no VACs are allowed in to the system.

One way hash function: One-way hash functions are known in the art. A hash function is a function which converts an input into an output, which is usually a fixed-sized output. For example, a simple hash function may be a function which accepts a digital stream of bytes and returns a byte consisting of the XOR function of all of the bytes in the digital stream of input data Roughly speaking, the hash function may be used to generate a "fingerprint" for the input data. The hash function need not be chosen based on the characteristics of the input. Moreover, the output produced by the hash function (i.e., the "hash") need not be secret, because in most instances it is not computationally feasible to reconstruct the input which yielded the hash. This is especially true for a "one-way" hash function--one that can be used to generate a hash value for a given input string, but which hash cannot be used (at least, not without great effort) to create an input string that could generate the same hash value.

Read-Only Media: A mass storage device that can only be written once (e.g., CD-ROM, CD-R, DVD, DVD-R, etc.) Note: pre-recorded music, video, game software, or images, etc. are all "read only" media.

Re-writable Media: An mass storage device that can be rewritten (e.g., hard drive, CD-RW, Zip cartridge, M-O drive, etc.).

Satellite Unit: A portable medium or device that can accept secure digital content from a LCS through a physical, local connection and that can either play or make playable the digital content. The satellite unit may have other functionality as it relates to manipulating the content, such as recording. The satellite unit has a Unique ID.

Scrambling: For digitally-sampled data, scrambling refers to manipulations of the data. Value-added or information rich data may be manipulated at the inherent granularity of the file format, essentially through the use of a transfer function. The manipulations are associated with a key, which may be made cryptographically secure or broken into key pairs. The manipulation may be associated with a predetermined key, which may be made cryptographically secure or made into asymmetric key pairs. Scrambling is efficient for larger media files

and can be used to provide content in less than commercially viable or referenced quality levels. Scrambling is not as secure as encryption for these applications, but provides more fitting manipulation of media rich content in the context of secured distribution. Scrambled data is also called "ciphertext" for the purposes of this invention.

Encryption generally acts on the data as a whole, whereas scrambling is applied often to a particular subset of the data concerned with the granularity of the data, for instance the file formatting. The result is that a smaller amount of data is "encoded" or "processed" versus strict encryption, where all of the data is "encoded" or "processed." By way of example, a cable TV signal can be scrambled by altering the signal which provides for horizontal and vertical tracking, which would alter only a subset of the data, but not all of the data—which is why the audio signal is often untouched. Encryption, however, generally alters the data such that no recognizable signal would be perceptually appreciated. Further, the scrambled data can be compared with the unscrambled data to yield the scrambling key. The difference with encryption is that the ciphertext is not completely random, that is, the scrambled data is still perceptible albeit in a lessened quality. Unlike watermarking, which maps a change to the data set, scrambling is a transfer function which does not alter or modify the data set.

Secure Electronic Content Distributor (SECD): An entity that can validate a transaction with a LCS, process a payment, and deliver digital content securely to a LCS. This may be referred to as a "certification authority." SECDs may have differing arrangements with consumers and providers of value-added information or other parties that may conduct transactions, such as business to business relationships. The level of trust place into an SECD can be dynamically adjusted as transactions warrant or parties agree.

Standard Quality: A transfer path into the LCS Domain that maintains the digital content at a predetermined reference level or degrades the content if it is at a higher quality level. In an audio implementation, this might be defined as Red Book CD Quality. Standard Quality may also refer to a particular set of VACs that are allowed into the system.

Unique Identification, or Unique ID: A Unique ID is created for a particular transaction and is unique to that transaction (roughly analogous to a human fingerprint). One way to generate a Unique ID is with a one-way hash function. Another way is by incorporating the hash result with a message into a signing algorithm will create a signature scheme. For example, the hash result may be concatenated to the digitized, value-added information which is the subject of a transaction. Additional uniqueness may be observed in a hardware device so as to differentiate that device, which may be used in a plurality of transactions, from other similar devices.

Value-Adding Component (VAC): An attachment to the content that enhances the user's experience of the content. VACs may be metadata, headers, usage rules, etc. For music, some examples are: album art, lyrics, promotional material, specialized playback instructions. For other embodiments, the value-adding component may relate to the consumer's personal information, preferences, payment options, membership, or expectations over a transaction.

The agglomeration of value-adding components is "value-added information." In the aggregate, value creation on an informational level can be observed and measured.

Value-added Information: Value-added information is generally differentiated from non-commoditized information in terms of its marketability or demand, which can vary, obviously, from each market that is created for the information. By way of example, information in the abstract has no value until a market is created for the information (i.e., the information becomes a commodity). The same information can be packaged in many different forms, each of which may have different values. Because information is easily digitized, one way to package the "same" information differently is by different levels of fidelity and discreteness. Value is typically bounded by context and consideration.

Verification: Called "integrity," in cryptography, an intruder preferably cannot substitute false messages for legitimate ones; the receiver of the message (embedded or otherwise within the value-added information) preferably is assured that the message (or by effects, the origin of the carrier within which the message is stored) that the message was not modified or altered in transit.

Note: The above definitions may be interchanged in different embodiments of the present invention and serve as parameters in breaking down value-added information exchange and trusted transactions.

Embodiments of the present invention and their technical advantages may be better understood by referring to **Figs. 1** through **13**, like numerals referring to like and corresponding parts of the various drawings.

Increasingly, a premium is being placed on both recognition and trust. These intangible elements are both expensive to create and to maintain given the ever-decreasing amount of human contact during transactions. To the extent that many transactions are now possible without any human contact, the present invention is a unique improvement over the art in enabling bi-directional authentication of information between parties to enable "trusted transactions" between those parties

For anonymous market exchanges, transparency and data integrity, as well as confidence, serve to promote confidence and growth in product, goods and service offerings. Perception is an expensive trigger to trusted transactions reinforced by the experience of market participants.

Confidence as well as experience enable trust: in an anonymous marketplace, it is desirable for the authenticity of value-added information and value-added components to be made more transparent and independently verifiable by all concerned parties. Transparency is valued in education and experience.

A purchase decision between a buyer and a seller is equivalent to the temporal establishment of a mutually agreed "abstraction of value" in the information sought or exchanged, which may be represented in both tangible and intangible forms. Perception is the natural limit of "fair pricing," and drives value determination of a particular good or service. Perception may be structured by context, history, and/or condition. The "value" of a particular transaction has an intrinsic meaning (financial, economic, legal, political, social, statistical or actuarial meaning), temporally (at the instant of the transaction), for both the buyer and seller (reached an agreement including offer acceptance and consideration), with any inclusive terms and conditions (hereinafter, "terms") governing the transaction (price, credit terms, delivery options, and other parameters concerning the good or service with respect to which the transaction takes place). As a result of such trusted

transactions, the parties gain confidence. Even parties who may be anonymous benefit from the contemplated improvements over the art.

Referring to **Fig. 1**, a block diagram of a system for trusted transactions is provided. System 100 includes trusted transaction engine 102, which interacts with a plurality of parties 104. Each party 104 has a unique identity 106.

Value-added information 108, as defined above, includes both intrinsic value 112 and nonintrinsic value 114. A vendor (who may be a party 104) may decide what information has value (i.e., should be considered to have intrinsic value or not), and this decision may be made on a per transaction basis.

The present invention may provide advantages to all parties involved, including pricing flexibility, a reduction (or optimization) of transaction costs, a recognition of value-adding components, and the ability to provide provable security and trust among parties. Each will be discussed in greater detail, below.

1. Pricing flexibility for parties

Because buyers and sellers have complementary but competitive goals in consummating a transaction, variable pricing in the present invention is supported without any detrimental affect on the potential relationship between the buyer and the seller, or their agents. Known systems depend primarily on securing payment; payment alone, however, does not ensure the buyer and the seller of lasting protection of their respective "intangible assets," especially those that are increasingly based on value-adding information (e.g., trademarks, copyright, patents, credit history, health condition, etc.). The buyer fears identity theft ("first party," or "sentimental" piracy), while the seller fears piracy of valuable information assets ("third party," or "positional" piracy). The separation of authentication of perceptually-represented goods and services and value-adding information, from payment security, is an important novel feature of the present invention.

Known systems specify a number of methods for ensuring "security." However, the primary feature of these approaches is access control based solely on proof that a purchase has been completed. This means that if a purchase can be enabled only by determinations that a transaction was successful, the ability to entice more transactions or otherwise increase the development of maintainable trusted transactions is undermined. Simply, the fact that a purchase was completed does not

mean that a trusted transaction has, in fact, been enabled. No provision for establishing a trusted relationship between the buyer and the seller takes place absent some authenticable exchange of additional value-adding information. The present invention increases the likelihood of a successful trusted transaction and extends beyond the ability to pay (assuming no "identity theft" has occurred). The present invention provides additional means for verifiable information exchange that enhance the experience of the buyer and the seller in seeking trusted transactions.

Because many manufactured goods are likely to have similar costs from a strict manufacturing standpoint, the value-added service, or services, that are provided to the buyer are likely to encourage additional opportunities for trusted transaction. The seller can benefit by leveraging a single purchase into a profitable relationship. Even distribution costs may be commoditized for all similar tangible goods. A series of non-contiguous or non-temporal transactions alone would constitute a profitable relationship if the buyer is satisfied and the seller is profiting. That pricing, and its terms, may be varied dynamically or supported flexibly (based on information exchange at the time or leading to a transaction), is another improvement over the art. The incorporation of micropayments becomes more feasible as the cost of trust has been reduced and thus smaller discrete increments of monetary consideration are easier to support to the benefit of buyers and sellers seeking higher granularity or discreteness over the information or tangible goods they transact. Simply put, identification and authentication of specific information and value-added components is inherently important to further segmentation of units of payment (e.g., micropayments). Micropayments may be interpreted as a value-added component in facilitating transactions.

Pricing may also be bi-directional and asymmetric, and is preferably determined by the seller in order to define "profitability." Some sellers may choose to maintain fixed pricing for their goods or services, but may incorporate variable pricing in the value-added component. For instance, while the price of a given good or service may be fixed, the value-added component may be the terms of the pricing as it effects the buyer. The seller may also entice the buyer to provide demographic value-added components, or related data, which has intrinsic, sentimental value to the buyer. To the seller, the pattern, or structure, of demographic datum serves as a

valuable filter in which to position its offerings. Simply put, while barter is relatively inefficient, cash, being anonymous, may not reveal enough information to provide an incentive for the seller to vary credit terms or offer a greater variety of goods and services, even if there is a single underlying value-added information good (the seller can still offer perceptually similar but nonequivalent versions of the information without threatening secure, higher quality, limited, or more expensive versions).

The ability to offer both secure and unsecure, or legacy, versions of the same information based on a mutual disclosure and mutual understanding of both the buyer and the seller is particularly novel in the art. Moreover, privacy can be enhanced and new, unproven and yet unsecure information can be offered without jeopardizing the security of any pre-existing primary value-added information whether it be music, images, currency, electronic documents, chip designs, source code, legacy versions, prior art, etc.

The period of payment, like the discreteness of the actual payment, interest rate relating to a payment period, grace periods, early payment benefits, variable interest rate based on the seller's ability to assess the credit risk/worthiness of the buyer or its agent, etc. is an element or component (a value-added component) that may be changed to affect a transaction. Making these components more transparent to buyers improves the opportunity for enhancing and maintaining trust. It also enables buyers and sellers to make mutually beneficial decisions based on transparent, verifiable information or value-added components. Moreover, buyer-driven pricing, as with Dutch auctions, or market-based pricing, are not possible without compromising the access-based security in known systems. With the present invention, goods and services are better able to realize full market value because access to the good or service is not restricted (such as with new music or new endeavors by "unknown" or "unrecognized" artists, designers, creators or engineers). The market participants are better able to assess the good or service in question, and/or the related value-adding information/component, when experience and information sharing is encouraged. The prior art is restrictive by necessity in information sharing precisely because security cannot be maintained by prior art systems with such open access to information.

For goods or services that are difficult to value (e.g., media content, legal advice, design, non-commodity items, etc.) and decision-intensive, pricing becomes a barrier to entry in a marketplace that puts a premium on recognition. Highly recognized artists, lawyers, designers, retailers, etc. have a competitive advantage over their unrecognized competitors. One approach to gaining recognition is freely distributing or providing goods or services. Ultimately, the seller still needs to profit from this initial positioning to the extent that financing of operations is available (the seller can stay in business as long as investors or financing is available to enable such operations). The same goods or services may be offered in a "tiered" manner, which relates to the purchase price or to the quality of the underlying good or service to be exchanged. Examples of this include providing music in MP3 quality audio instead of CD quality; providing 10 hours of customer support instead of charging per hour; charging service charges instead of free checking or ATM access; charging a price per bit or bandwidth; etc.

Segmenting also plays a role in the "freshness" or "newness" of the information good or service. Live concerts or lectures may be worth more to the buyer than pre-recorded versions offered later or separately. The performer or creator of the information to be performed, or conveyed live, can only be at one place at a time, and may be a premium for that time. Live broadcasts may similarly have a higher value. Physical advice may be worth more than printed literature to the buyer as well. These dynamics create an impetus for flexible and dynamic pricing that does not undercut the security of the overall "trusted transaction" methods and systems envisioned in the present invention.

In known systems, legacy information, relationships, etc. systemically undermine the ability to ensure a "trusted system." The buyer and the seller in the art have no means for differentiating between the secure and unsecure versions of a good, service, or value-adding component. The present invention provides such protocols by incorporating additional bits of data, which do not necessarily represent added data, but imperceptibly replace data with identifying or authenticating data, enabling market participants to determine whether a value-added information "package" is secure. This also enables uniqueness of information packages to be consistently created and checked or maintained for later reference. The prior art

relies on the denial of access or access restriction, a clear disadvantage in increasing the availability of value-added information. With trusted transactions market participants are able to verify, identify, and price information and then decide which versions are appropriate for a given or existing demand.

Pricing may be better understood if the cost or time of computation is measured as a tangible asset. Similarly, the natural limit to theft of tangible assets has always been in the cost of the tangible assets. As information can increasingly be traded for value in excess of the cost of its storage or transmission, pricing becomes less tangible and more subjective. Delivery of information accurately and quickly becomes a valued service. Measuring such value is based on the same principles that allow cost estimates of the delivery of fixed weight parcel packages. The existence of hackers indicates a lowered economic barrier to entry for informational crime, including identity theft and piracy. Dissemination of binary code, which is similarly detrimental, at little or no cost to the originator of the valuable information, introduces novel concepts to the approaches of information pricing. Tangible goods become substitutes for cash payment.

An example of pricing based on effort is illustrated by a watchmaker who takes six months to finish a watch that he prices at $70,000. This includes a "reasonable" profit and the cost of materials. The buyer is a watch fanatic and earns $140,000 a year. The exchange of a tangible good that has intrinsic value, which is converted into monetary terms for negotiation, as agreed by the parties in the exchange, becomes more prominent if information concerning value is transparent or fluid for all market participants. Transparency is inherently favored by markets seeking to appropriately price goods or services based on all available information at the moment of pricing. Conversely, risk can be priced based on the financial context or structure of an organization. Those who earn $20,000 should have to have confirmation by others with additional financial or fiduciary responsibilities before validating or approving transactions that exceed an individual's earnings for the period in question. At any time responsibility can be linked to authority, as a pricing mechanism for decisions concerning similar amounts of monetary consideration. With pricing mechanisms and use rules, trusted transactions offer flexible pricing not possible with current systems.

Value-adding components, which may include pricing, is preferably viewed as a separate and distinct means for the buyer and the seller to separate information that may or may not be essential to any given transaction and may also be viewed as nonessential unless both parties can stipulate such information exchange. This is invaluable as multiple channel distribution of the "same" goods (e.g., download music over the Internet versus purchasing a CD from a store) or services (obtaining a mortgage online versus processing physical loan documents) can be offered by the seller. Determinations of which channel, or channels, are profitable requires verification of unsecure and secure versions of these "same" goods.

Value-adding components may also include an offer, an acceptance, a bid, a purchase, and a sale of a securities instrument, including an option, a warrant, or equity.

Security is inherently intended for the party seeking value or authentication over the information or transaction and conversely protecting sentimental information or identity from being stolen or defrauded. For the long term, buyers are able to differentiate that personal information value-added components are appropriate for dissemination to a seller to affect a transaction, or to get better terms. Either the buyer or the seller, or both, are better able to determine that transactions or relationships are favorable on a transaction to transaction basis, and thus "transact" accordingly.

Pricing of the value-added information may include a value-adding component relating to the present value of recognition/non-cash equivalent cost/service that is handled in a separate negotiation or transaction, or a subsequent negotiation or transaction

The present invention may include limits of liability, or may consider the time value of money when determining a limit of liability threshold. The present invention may enable rules/access/authorization based on the result of that operation. In one embodiment, an actuarial estimate of liability (future time) or cost (present time) may serve as a rule for enabling another rule.

2. Reduction or optimization of transaction costs

In instances where the buyer and the seller, or their agents, seek to transact products or services that include value-added information, the seller generally seeks

to maximize profit, but may forego profit in the short term to ensure recognition or market share in the short term. The buyer seeks "satisfaction," which is dependent on one or more of the following product/service determinants: 1) price; 2) service; and 3) selection. These determinants may be quantitatively or qualitatively assessed and may be based on available bandwidth, time of transaction, and transaction event conditions.

A priori, the buyer may not recognize the seller. In an information economy, such events are not a disincentive to pursuing a trusted transaction, but instead present market opportunities for valuing, authenticating, and verifying information (all may be value-added components) concerning potential transactions are inefficient. Conversely, the seller may not have enough information about the buyer to determine what type of potential transaction can be enabled, based on the buyer's ability to purchase now, or at any point in the future. The seller may be inclined to make a sale with the buyer (or the buyer's agents) with or without confidence that the initial transaction will lead to further transactions or trusted relationships that are profitable for the seller. The seller may use purchasing options (e.g., barter, cash or its equivalent, or credit) to enable a purchase by the buyer. According to one embodiment of the present invention, because value-adding information and its components may be bi-directional, both the buyer and the seller may chose to negotiate the transaction, including variable terms for payment, as one form of value-added component or service and support for the information to be transacted.

Transactions, as defined by a purchase event (payment can be preliminarily assured), may happen before or after the buyer and the seller have "agreed" to transact. When the seller requires value-adding components/information about the buyer before entering the transaction, the seller generally has higher risks than the buyer, which may affect its profitability. Where there is a high risk for piracy, such as the digital copy problem (that can render individual copies of value-added information worthless), the seller may not be able to establish trust with an unknown buyer. The seller is not assured of any potential profitable transactions or long-term relationship with the buyer, which poses a significant risk to the seller if the buyer pirates information goods or services. A lack of dynamic authentication, even in

real time, at least initially, and adjusted as needs arise over time, and flexibility in negotiable terms, may cause the seller's assets to be economically undervalued.

Conversely, in those events where the buyer requires value-adding components/information about the seller in advance of entering a transaction, the buyer generally has higher risks than the seller with regard to its ability to enter into transactions. "Identity theft" is an example of a risk that is higher for the buyer than the seller in these types of transactions. Additional transactions include on-line brokering, auctions, searches, bots, webcrawlers, recognition, and determination of goods or services absent proof of privacy guarantees. This applies to noncommercial information as well (e.g. the FDIC logo, currency, driver's license, etc.)

The establishment of mutual trust may be asymmetric depending on the risk profile of the buyer and the seller. Risk/reward tradeoffs are implicit to some transactions, while the time required to establish a trusted transaction or eventual profitable relationship may not be contiguous. In many on-line transactions, the per transaction risk is generally higher to the buyer, who may suffer fraud and may need to be more diligent about what value-adding information it chooses to exchange in the interests of enabling a trusted transaction. It is true, however, that in business to business transactions ("B2B"), or in financial information exchange, the relative risks to each party are relatively equivalent, and requiring a more symmetric exchange of value-adding components relating to verification and purchasing power (in the form of barter, cash, cash equivalents or financing that would also constitute value-adding components) is not as necessary. Reducing the cost of creating and maintaining trust is an advantage of the present invention over known systems.

3. <u>"Reintermediation": recognition as a Value-added Component</u>

Asymmetry exists in recognition as well. Where word-of-mouth may constitute an acceptable means for creating recognition for a particular good or service, the buyer and the seller may wish to expand their respective abilities to capture more of the increasingly available goods and services, or value-adding information (about themselves, or terms for a trusted transaction). With advertising and other forms of marketing, the push and pull of value-adding information between the buyer and the seller also contributes to potential purchase decisions by

both parties or their agents. The buyer may control certain criteria it seeks, such as price, selection, and/or service. The seller, conversely, seeks the highest profits from a given potential buyer or his agents, which may not be quantifiable from the first transaction or may not be the primary focus of the seller (such as seeking a valuable, marquis client). Both the buyer and seller may compare patterns or structure that, when recognized, help in forming opinions about the history, condition or context of the information.

In general, recognition serves to encourage more recognition. The seller will likely seek trusted transactions in the interests of profitably leveraging the time, cost and expense of generating the initial exchange of goods and services with the buyer. Over the longer term (defined as any additional transactions beyond the initial transaction), a profitable relationship is sought by the seller. The buyer and the seller may still maintain flexibility as expectations or needs concerning the relationship change. The present invention allows for such variability and flexibility by enabling real time adjustments to the terms that prevail between market participants. While terms are conditions are negotiatiable, security of the overall system is not jeopardized because secure and unsecure versions of the "same" value-added information and value-added components can be adjusted bi-directionally. In an information-based transaction, there is value in reintermediation by sellers seeking to ensure that their information is provably identifiable and verifiable.

The buyer and the seller may seek recognition or use means for increasing visibility of their respective interests. The buyer ultimately seeks to satisfy itself through a trusted transaction preserving private or financial information for select transactions requiring higher amounts of information exchange or verification (real time references, "membership reward programs" such as frequent flier airline points, or financing options that can be dynamically offered, are two incentives to the buyer and are likely to differentiate vendors, large and small, really or perceptually); the seller ultimately seeks to profit from the trusted transaction. Recognition of this potential exchange between the parties is not assumed to be high enough to enable a transaction, but high enough to create exposure for the buyer or the seller. Trust is assumed to not be pre-existing, or it may be variable between the buyer and/or the seller, requiring additional exchanges of value-adding information to enable a

trusted transaction. The seller, in the extreme, seeks the highest profit for each transaction. The buyer, in the extreme, seeks the highest satisfaction for each transaction. As discussed above, both goals are complementary and competitive, thereby increasing the need for dynamic exchange of value-adding information. Recognition can enhance the potential for a successful trusted transactions and serves as a form of abstract experience for both parties to efficiently make decisions. With experience, value assessments become possible. Abstractions of value become experience as trusted transactions beget more trusted transactions.

4. Provable security and trust

Trusted transactions are characterized primarily by bridging the gap between "provable security" and the imprecise nature of trust. Encryption, cryptographic containers, digital watermarks and other forms of electronic data security can be mathematically demonstrated -- discrete algorithms can be designed to meet certain pre-defined specifications or pre-defined expectations.

Encryption and secure digital watermarking (e.g., steganographic ciphering) offer tools for determining data integrity, authenticity and confidence. Transactions, however, still require human decision-making. Known systems describe a number of approaches for ensuring transactional security based solely on transmission security and fail to differentiate between what could be called "positional piracy" (e.g., the fraud or theft of universally recognized goods, products, and services) and "sentimental piracy" (e.g., the fraud or theft of personal, private or financial information).

For the purposes of this disclosure, the extreme case of sentimental piracy is identity theft. So long as information can be represented in binary digits (0s and 1s), and can be easily copied, stored or transferred, identity fraud becomes an increasingly insidious problem. There is a temporal limit whereby the actual person is able to "reclaim" their identity at some point in time. The extreme case of positional piracy is zero returns on an intangible asset that has been pirated. As well, the present invention offers advantages over known systems for positional piracy that enable the continuation of legacy business, customer relations and existing information formats, without sufficiently weakening any overall system security for trusted transactions. Simply, unlike known systems, access restriction is

not an adequate or appropriate means for ensuring the security of information data for a wide variety of applications.

To the extent that "security by obscurity" is typically representative of weak security to those skilled in the art of cryptography, more transparency for parties to a transaction over security protocols and information transfer are inherently necessary to ensure trusted transactions. Although information between parties may be asymmetrically exchanged (i.e., the value-added information or value-adding components is not equivalent in quality or quantity between parties, such as a difference in the amount of information exchanged, the identification of the parties, etc.), the level and degree of authenticity or verification only differs among the goods, products or services to be transacted, as well as the demands of the market participants. For the purposes of this disclosure, the value-added information is the fundamental good to be transacted between parties, while value-added components represent an atomic unit of data that is defined as the least amount of data that can either add functionality or be perceptibly recognized to a system for trusted transactions. Data may be represented in analog or binary terms in order to establish uniqueness and assist in identification and authentication. Value-added components may be added, subtracted, or changed to vary the underlying value-added information sought.

Because humans have difficulty remembering passwords, personal identification numbers (PINs), and the like, dependence on such datum is increasingly problematic as more anonymous transactions are enabled between parties over electronic networks, such as the Internet, or between businesses in private networks. While passwords, or PINs, are commonly thought to be secure, the ability to check all combinations of numbers or crack passwords becomes less computationally expensive with increases in both processing speed and availability of bandwidth. Cost is reduced to the detriment of security if any individual has the means for high order computation or network-based bandwidth in discovering or hacking any given secret. Quantum computing speeds up the ability to test and discover such data at even greater speeds, and presents unique problems to security systems described in the art. Quantum computing also enables the definition or predetermination of the physical limitations of communicating or securing

information. Where difference between binary or digital signal processing and quantum mechanical limits is higher, better security is enabled.

Biometrics have been suggested to remedy this problem, but do not offer any way to create truly cryptographic secrets to be shared between parties. Iris scans, fingerprints, and the like, are easily stolen because they are easily perceptible to those seeking to defraud. Once stored electronically, biometrics be stolen for unauthorized use. Combining a biometric with a digital signature may provide a means to ensure that a given representation of a fingerprint or iris is fixed, temporally at the time the certificate is created, but does not prevent dedicated attacks at determining the fingerprint or iris to be used at some subsequent time. Real time authentication and verification are improvements envisioned with the present invention. Assuring that a particular fingerprint, signature or iris "data set" is that of the intended user, is fundamentally important to embodiments described herein. This becomes especially invaluable with increasing number of anonymous transactions. Although uniqueness may be enhanced with digital signatures and digital iris or fingerprint records, the advantage with the present invention is that more secure forms of uniqueness based on a predetermination of the discreteness of time and a predetermination of the limits of information conversion and transfer are absent in the art.

Moreover, real time authentication is not enhanced with systems described in the art, since such biometric data is easily stored or transferred, and thus suffers the same pitfalls for any binary data that is sought by a party seeking to defraud. Biometrics may be great for forensics (e.g., to determine after the fact who is responsible for a particular act), but they do not effectively address an inherent problem in enabling trusted transactions; that is, real time verification of parties or real time association of parties with information being transacted (in an auction, for instance). They are also not representative of a cryptographic key, which, as is well-known in the art, requires secrecy, randomness, and an ability to update or destroy the cryptographic key.

Another advantage of the present invention is the ability to serialize or individualize "personal secrets" that are shared between parties to boost confidence and transparency of transactions. That control, and the inherent uniqueness of

personal entropy, constructed from such information as a hometown, favorite restaurant, or high school sweetheart, is a means for perceptible representations of "secret data" that enhances the ease-of-use and application of appropriate shared secrets to be exchanged in conducting trusted transactions. Associating such secrets with primary value-added information or value-added components being transacted is an additional novel feature of the present invention. Essentially, the present invention provides the ability to personalize or serialize, informationally, an actual "transaction event," including: the buyer; the seller; primary information; value-added components and tangible assets created, manufactured, or manipulated; and any additional reference that can be made perceptible and secure to any observer. Bridging cryptographic with real world perception is a benefit over the prior art.

Essentially, randomness alone, whether pre-determined or not, is not sufficient for the creation of a "secret" that may be used with high levels of confidence repeatedly in assuring the validity of information or verify the identity of a party. Encryption systems cipher the randomness according to available data capacity; digital watermarking ciphers the randomness according to perceptible features or characteristics of the carrier signal (a humanly-perceptible measure of data capacity, which distinguishes applications for encryption from secure watermarking). That such information can be made more computationally difficult to discover, even by brute force attacks (since such experience is only limited by the experience of individuals) is of particular benefit to the art. The computational complexity added by use of a steganographic cipher is discussed in the U.S. Patent No. 5,613,004, the disclosure of which is incorporated by reference in its entirety, and offers a means for human observers to see the actual tampering of information represented perceptibly. This proof is self-similar to that which is obvious in the real world, i.e., the ease at which one can observe that a watermark is missing from currency. Handling information as contemplated by the present invention for trusted transactions is unique in bridging computational benefits from both digital signal processing and cryptography to the benefits of all parties to a transaction. The present invention is the enhancement of transactions through bi-directional verification of parties and verification of primary or secondary information exchanged.

An additional advantage of the present invention is the ability to continue to offer legacy business relationships, legacy products, legacy services and other means that will not reduce the overall security maintained by a system for trusted transactions. Known applications lack this feature, and instead rely on denial of access or authorized access to information. Information need not be restricted, and is preferably freely exchanged to widen the opportunities for transactions with a greater potential number of parties. The present invention is an improvement, in that the elements necessary for generating trusted transactions may be made more flexible, and those elements that are "secret," those elements that will be available at predetermined times, as well as those elements that are made more obscure to unintended parties, increase the overall computational difficulties in defeating a system for trusted transactions.

An additional consequence is improvements in enterprise resource planning and data mining. To the extent that transactions are made unique and may be atomized into data, functions, value-added components and any associated information, the cost of maintaining or referencing stored data, a goal in data mining technologies, can be made more efficient and effective in assisting with an optimized appropriation of resources, individual or corporate. Without such uniqueness, serialization, authentication, verification or identification, particular transaction events cannot be analyzed, manipulated or optimally used to create additional trusted transaction opportunities. Caching technologies are similarly effected by the present invention. The choice about what information should be maintained locally based on identification or authentication of that information available on a network, such as the World Wide Web, enables higher efficiency in sorting and referencing data for repeated use without increased demands on the network.

The ability to serialize individual transactions by particularizing trusted transaction elements between parties is handled more consistently than in known systems. Access is not denied, and rules for access are not pre-determined for goods or services that require exposure, testing or additional information for consummating a transaction. Ease-of-use, maintenance of more human-like and physical world expectations of trust are made more transparent. Identity and authentication risk is

reduced, and confidence is increased. Overall expectations are handled according to the needs of individual parties to any number of transactions. What results from trusted transactions is a more vibrant and competitive marketplace for information, value-added or not. Anonymity and legacy relationships may be maintained, unlike requirements in known systems.

The application of steganographic ciphers enables an "optimized envelope" for securely inserting, detecting, and protecting informational signals, or data, or digital watermarks (predetermined messages) in a given digitized sample stream (e.g., a predetermined carrier signal, such as audio, video, image, multimedia, virtual reality, etc.). As the perceptible qualities of the content stream have a basis as analog waveforms, steganographic ciphering increases the computational difficulty of crypto-analysis and makes unauthorized removal or tampering of the watermark a costly operation. With perceptible damage to a carrier signal a result of such tampering, tampering is more easily observable by parties, including those who are involved in a particular transaction event. Moreover, such tampering enables higher transparency and verification of carrier signals of datum that are marked for secure exchange, even if over unsecure transmission channels. The prior art relies overly on secure transmission channels while ignoring the potential benefits of securing datum (with secure watermarking, scrambling, or chaffing, for instance) over any available transmission channel. Such tampering is also transparent to vendors handling or accepting the information that enables less costly validation of claims made after some event must be confirmed and verified to the satisfaction of transacting parties. These unique features are an improvement over the art.

What differentiates the "digital marketplace" from the physical marketplace is the absence of any scheme that establishes rights and responsibility, or trust, in the authenticity of digitized goods, services or value-added information. For physical products, corporations and governments watermark "goods" and monitor manufacturing capacity and sales to estimate loss from piracy. Reinforcement mechanisms, including legal, electronic, and informational campaigns also exist to better educate consumers. Evidentiary levels of confidence must exist to support claims that are typically competitive between parties to a transaction.

Currently, security parameters may be coded into the actual physical transaction system or instrument. Similar to the security inherent in the randomness of the magnetic strip on most credit cards, these security parameters are designed to be tamper-resistant. Cracking such codes would not present insurmountable barriers to a dedicated effort at cracking a PIN. Access authorization is easily compromised by fraudulent reconstruction of an instrument, such as a credit card. Although storage of the security parameters in volatile, or nonpermanent, memory appears to offer advantages, including higher security required for many transactions, absent this higher level of security, real time authentication becomes a crucial benefit to parties in ensuring the validity of many forms of transactions. Insurance, identity, and purchases of expensive items or services are not generally confidently handled. Use of trusted transactions to process value-added information is unique and beneficial.

Several components may be used for separation of "trusted elements" for a given device or method for ensuring "trust" according to one embodiment of the present invention. First, a general purpose computing device is comprised of a CPU, a memory or storage, input and output devices, and a power supply. A device or card holder decides whether and when to use the device. For additional benefits described herein, personal information or privacy data may be controlled by the user in sample embodiments envisioned, unlike other pre-determinations of data in non-trusted transaction smart cards (e.g., a credit card).

A data owner, who may or may not be the device holder, is provided. Where the device holder and data owner are the same, as contemplated by some embodiments of the present invention, such data as digital certificates, time stamps, Unique IDs of data coming into and out of the device (personal or financial information being a large class of such data), etc. can be authenticated in a humanly-perceptible manner. This may be accomplished by a transducer, or a screen, that can transfer analog-based information of device holder, or be inputted and transmitted by the device holder for secure watermarking, or hashing of data to be exchanged.

A terminal, controlling input and output to and from the device (e.g., phone cards are controlled by the phone service provider's terminals, ATMs are controlled by financial institutions, set-top boxes controlled or owned by entertainment

distribution providers, etc. that may be made physically secure by separate means) or a system that may interact with a device, such as that contemplated in embodiments herein, to enable real time authentication or verification where such checks may fail from time-to-time with existing pre-defined trust arrangements or pre-determined protocols that require inefficient updating by one or both parties. In lieu of a physical visit to a vendor, the present invention anticipates more convenient anonymous updates, in those markets where it is possible to the benefit of both buyers and seller -- both parties have a market demand or need and are able to agree to such arrangements.

Embodiments of the present invention may include a simple Internet browser plug-in, with complementary system software for the provider of "information goods or services," that would identity, verify, authenticate, enable transfer, enable copying or other manipulations of the various primary value-added information and value-added components. Some of the functionality may strictly indicate what, if any, security exists within a particular primary value-added information set. This need not be settled within a system of trust, but be inherently imperceptible to any casual observer or market participant interested in the information or the transaction events that can be observed. Essentially, encouragement of provable differentiation between different classes of primary value-added information (secure, unsecure, legacy, etc.), value-added components (not the primary information but value-adding to the transaction event, and any information concerning market participants (private, history, condition, or financial) is enabled, using simple steganographic ciphers with mapping and transfer functions without compromising the underlying security.

A device issuer controls the operation of the device according to mutually agreed to terms between parties. The device issuer may limit the use or functionality of the device.

For the device hardware manufacturer, fraud may be attempted by the various parties, subcontractors, etc, who are involved in the manufacture of the devices. The device issuer requires protocols that cannot be defeated by typical "rogue engineer" attacks, where security is dependent on an understanding of the methodologies, device, or system design. In fact, the ability to transparently and

provably manufacture secure smart devices may be accomplished with such protocols as digital time stamping (using successive temporally related hashes that seed other hashes to create a universally acceptable means for establishing the time of manufacturer, with time being the universal constant), or digital watermarking (where instead of time, other predetermined data is concatenated with data for provably establishing ownership, over the device). Tampering must be provably perceptibly evident upon tamper detection of the device (as with device used for limiting theft of clothing or physical items in retail stores). Prevention of the rogue engineer problem is not anticipated by known systems.

A software manufacturer usually requires clear specifications or transparency such as open source code, providing the underlying ciphering algorithms and other specifications for analysis. Similar trust issues as with device hardware manufacturing exist. Stega-ciphering the operating system, the simple system or engine for determining authenticity and identification of available data, to prevent memory capture, cloning, write once memory specific to the device holder provide additional benefits of security. A discussion of such is provided in U.S. Patent No. 5,745,569, the disclosure of which is incorporated by reference in its entirety. As well, using transfer functions with associated predetermined keys is also a means for accomplishing confidence and authenticity in transaction. This is described in U.S. Patent Application Serial No. 09/046,627, entitled "Method for Combining Transfer Functions with Predetermined Key Creation," the disclosure of which is incorporated by reference in its entirety.

In general, security requires: fewer splits of trust (poor tying arrangements that may encourage fraud or piracy), better transparency of data (it should be perceptibly apparent, or mathematically, or actuarially possible to observe risks and quantify them to enable security design with a clear understanding of potential threats for each system, method or device), and use of cryptographically strong protocols, where security is both provable and perceptible such that market-driven features are both fundamental at the earliest development and design of appropriate systems and devices, in order to build confidence and trust that is acceptable and transparent to all parties to a transaction.

Application of a steganographic cipher to the operating system or operation of the contemplated systems and devices ensures further security from tampering. Such methods are disclosed in U.S. Patent No. 5,745,569, and offer additional benefits when coupled with the embodiments disclosed herein. System or device operations may be controlled with minimum functionality, objects or executable code. As value-added information is checked for authenticity, decoding any embedded operation objects or code, executing the operation of the system, and deleting the object or code from memory, or randomizing it in memory to avoid capture, would greatly increase the security of both value-added information and the systems or devices intended for manipulation of the value-added information. Alternatively, certain base functions, such as play, record, copy, manipulate, and transfer data, may be problematic. These functions may be atomized into objects that must be first authenticated by the trusted transaction device before they are operable for the given format, or before they provide additional information.

Time of use has traditionally been a typical constraint for securing smart cards and similar devices, but may become ineffective and inconvenient to users. Enabling a smart card to capture or transduce information (even converting analog information or input into secure digitally-sampled representations of the analog information for analysis and authorization, as with a stega-ciphered digital watermark) about the time, location, identity or any number of specific datum greatly enhances smart card and similar device security, trust and confidence. Such benefits over known systems are valuable contemplated with the present invention.

Valuations of trust also enables the described sample embodiment of a trusted transaction system or device to compare private information with financial information, essentially bridging determinations of risk in financial transactions and insurability. Private, or sentimental, information disclosure is more highly sought in determining insurance risk. The ability to pay, and other financial information, are being commoditized. Insofar as the described method and device for such deployment of trusted transaction technology can be assessed for different products and markets, the example of an insurance device could easily be called a trusted transaction privacy/financial information device or card. Users can control what information they disclose given the risk coverage or credit they seek, and providers

being able to decide, with more current and transparent information disclosure possible, what to underwrite or what to finance.

For the authentication or identification device, there is a risk of identity theft to both buyers and sellers, or information that is limited by law. Examples include Medicare-covered drugs, local legal constraints, etc. Risk may be predetermined or limited by a government agency (FDIC, FBI, Social Security, IRS, DMV, Federal Reserve, etc.), a similarly outfitted organization (trust is held in perceived and observable representations of the organization, food stamps, stamps), or an equivalent transaction event enabler (traveler's check provider, medication, etc.). In these cases, systemic risk is limited by enforcement agencies held in trust by a government or body politic. The restrictions are predetermined and dependent on successful authentication or identification of a product, label, or other similar item. Laws may differ between localities and may be dependent on some form of identification, proof of age, or proof of residency. To properly serve local residents becomes a data security issue. This embodiment offers advantages over the art in its flexibility and real time, perceptible authentication properties.

Both the provider and the agency involved may have higher levels of risk, because the nature of the information is characterized by high value, general or universal recognizability, and a genuine threat of fraud. Most people casually accept that $10 and $20 bills are real even if they prove not to be later. Governments try to limit such liability without damaging the overall trust in the currency. As abstractions of value are exchanged, a smart identifying device, instead of value replacement device (predetermined, fixed spending or authorization in a device), is necessary to capture "personal entropy," or information about oneself that can be more closely guarded and less open to theft versus a password or pass phrase. Secrets must differ from identification. The larger body of data to search to discover these secrets act as a higher form of secrecy. These datum may be converted to readable text in some embodiments or maintained in digitally-sampled but humanly perceptible form in other embodiments (favorite restaurant is represented as an actual image of the restaurant, mother's maiden name is actually the voice of an individual's maternal grandparents, highly specialized forms of personal information

that may be dynamically changed or checked quickly and conveniently without undue risk exposure to the system).

For governments and individuals, piracy of identity is the most insidious risk exposure. Identity theft may be curtailed with devices that can transduce, in real time, an iris scan, fingerprint or other biometric and compare securely transmitted results with a secured stored record at the time of initialization. Alternatively, this may be accomplished with an unrelated Unique ID that confirms the identity of the user, and may be created and stored on the device. Because governments are arbiters of trust in markets (their actions in the collective affect trust and confidence in products and markets), these devices are able to alert consumers to potential risk for a given product or service (represented by some ruling or law that is important to convey to the consumer, such as with alcohol, medications, or tobacco). These devices could, at the discretion of the user, indicate related warnings for which the government has an interest in safety. In one embodiment, by checking an actual cigarette carton, or drug packaging, with the enabled device, counterfeit packaging may also be detected. In one embodiment of the present invention, bar code scanners may be "required" to also check for embedded or associated signals indicating authenticity. The devices may also check if supposedly "real" prescription drugs are authentic. Such a check may occur when using the device to communicate with a vendor and check to see if any complaints or problems exist in stored records; again the packaging may be checked for authenticity in cases where counterfeits are high and difficult to check without some form of secure watermarking or perception-based authentication that can be efficiently handled by an enabled device.

According to one embodiment of the present invention, digital content may be distributed through a local content sever, or LCS. In general, the LCS environment is a logical area inside which a set of rules governing content use may be strictly enforced. The exact rules may vary between implementations, but in general, unrestricted access to the content inside the LCS environment is disallowed. The LCS environment has a set of paths, or paths that allow content to enter the domain under different circumstances. The LCS environment also has paths that allow the content to exit the domain.

The act of entering the LCS environment may include a verification of the content (an authentication check). Depending upon the source of the content, such verification may be easy or hard. Invalidatable content may be subjected to a quality degradation. This degradation may be to the content itself, or it may be removal of value-added components. Content that can be validated, but that belongs to a different LCS environment may be excluded. The primary purpose of the validation is to prevent unauthorized, high-quality, sharing of content between environments.

When content leaves the LCS environment, it may be watermarked as belonging to that environment. It is allowed to leave the LCS environment at the quality level at which it was stored (i.e., the quality level determined by the path). The watermark on the exiting content may be both an embedded digital watermark and an attached hash or digital signature (it may also include a secure time stamp). Content cannot return into the environment unless both the watermark and hash can be verified as belonging to this environment. The presence of one or the other is generally sufficient to allow re-entry.

This system may allow a certifiable level of security for high-quality content, and may allow the use of unsecure content at a degraded quality level. The security measures are such that a removal of the watermark constitutes only a partial failure of the system. The "wiped" content may be allowed back into the LCS environment, but only at a degraded quality level, a result of the watermark destruction and subsequent obscurity to the system. Consumers will not be affected to the extent that the unauthorized content has only been degraded, but access has not been denied to the content. Only a complete forgery of a cryptographically-secure watermark will constitute a complete failure of the system. For a discussion on such implementations please see U.S. Patent No. 5,613,004; U.S. Patent No. 5,687,236; U.S. Patent No. 5,745,569; U.S. Patent No. 5,822,432; U.S. Patent No. 5,889,868; U.S. Patent No. 5,905,800, U.S. Patent No. 6,078,664, U.S. Patent Application No. 09/046,627 U.S. Patent Application No. 09/053,628, and U.S. Patent Application No. 09/594,719

Provable security protocols may minimize this risk. Thus, the embedding system that embeds the watermark does not need to be optimized for robustness, only for imperceptibility (important to publishers and consumers alike) and security

(more important to publishers and commercial interests in the content than to consumers). Ideally, as previously disclosed, security preferably does not obscure the content, nor prevent market participants from accessing information contained therein, and for the longer term, developing trust or creating relationships.

The system can flexibly support "robust" watermarks as a method for screening content to speed processing. Final validation, however, is relied upon the fragile, secure watermark and its hash or digital signature (a secure time stamp may also be incorporated).

The LCS provides storage for content, authentication of content, enforcement of export rules, and watermarking and hashing of exported content. Stored content may be on an accessible rewritable medium, but is preferably stored as ciphertext (encrypted or scrambled), not plain text, to prevent system-level extraction of the content. This is in contrast to known systems, which affix or otherwise attach meta-data to the content for access control by the variously proposed systems.

The LCS may be able to receive content from a secure electronic content distributor, or SECD, and may be able to authenticate content received via any of the plurality of implemented paths. The LCS may monitor and enforce any rules that accompany received content, such as number of available copies. Finally, unless being transmitted to a satellite unit, the LCS may watermark all exported material and supply a hash made from the Unique ID and the content characteristics (so as to be maintained perceptually within the information and increase the level of security of the watermark).

The satellite unit enables the content to be usable apart from the LCS. The satellite unit is partially within the LCS environment. A protocol may exist for the satellite unit and LCS to authenticate any path made between them. This path may have various levels of confidence set by the level of security between the satellite unit and LCS, and determinable by a certification authority or its equivalent, such as an authorized site for the content. The transfer of content from the satellite unit to the LCS without watermarking may be allowed. However, all content leaving the satellite unit is preferably watermarked. The satellite unit watermark may contain a hash generated from the satellite unit Unique ID and the content characteristics. If the content came from a LCS, the satellite unit may also add the hash received from

the LCS to the watermark. The LCS and satellite unit watermarking procedures do not need to be the same. However, the LCS is preferably able to read the satellite unit watermarks for all different types of satellite units with which it can connect. The satellite unit does not need to be able to read any LCS watermarks. Each LCS and satellite unit preferably has a separate Unique ID.

Referring to **Fig. 2**, a schematic of a local content server environment according to one embodiment of the present invention is provided. LCS 202 may be a software device running on a general purpose computing device, such as a personal computer (including, in general, a central processing unit, an input, an output, a memory, and a power supply). LCS 202 may include local content server domain 204, rewritable media 206 (such as a hard disk drive, a CD-R/W, etc), and read-only media 208 (such as a CD-ROM). LCS 202 may communicate with at least one satellite unit 210 via an interface.

In one embodiment, LCS 202 may have a Unique ID. Similarly, in one embodiment, satellite unit 210 may have a Unique ID.

LCS 202 may communicate with SECD 212 via a network, including a local area network, a wide area network, an intranet, and the Internet. This communication may also be established by a telephone link, a cable connection, a satellite connection, a wireless connection, etc.

In one embodiment, a single LCS 202 may interface with more than one SECD 212.

A plurality of paths 220, 222, 224, 226, 228, 230, 232, and 234 may exist among LCS 202, SECD 212, Satellite unit 210, LCS domain 204, rewritable media 206, and read-only media 208. Each will be discussed in greater detail, below.

Digital content may be securely distributed to LCS 202 from SECD via path 220. The content may be secured during the transmission using one or more security protocols (e.g., encryption or scrambling of the content). In one embodiment, if LCS 202 interfaces with multiple SECDs 212, each path may use a different security protocol.

The security protocol may use an asymmetric cryptographic system. An example of such a system includes a public key cryptography system. The private and public key pairs allow LCS 202 to authenticate and accept the received content.

Referring to **Fig. 3**, a flowchart depicting an example of an authentication by LCS 202 is provided. In step 302, the user connects to the SECD, makes a selection, and completes a sale.

In step 304, the LCS provides its public key to the SECD.

In step 306, the SECD uses the LCS public key to initiate transmission security.

In step 308, the SECD transmits the secured digital content to the LCS.

In step 310, the LCS receives the digital content, authenticates that the digital content was unchanged during transmission, and unpacks it from its security wrapper (that may include a secured transmission line, such as SSL). In one embodiment, the digital content may be authenticated by a watermark and hash check. If the content can be authenticated, the content is accepted into the LCS domain. If the content cannot be authenticated, it is rejected.

Referring again to **Fig. 2**, path 222 connects LCS domain 204 with rewritable media 206. Referring to **Fig. 4**, a flowchart depicting the process for content entering LCS domain 204 from rewritable media 206 is provided. In step 402, the content is provided. In step 404, the content is checked for the presence of a watermark, such as a watermark for the particular LCS. If there is not a watermark, in step 406, the content is degraded to Low Quality and, in step 408, the content is stored in the LCS domain.

If, in step 404, a watermark is present, in step 410, the watermark is checked to determine if it matches the LCS. This may be achieved by a hash. If the watermark is verified, in step 408, the content is stored in the LCS. If the hash does not match, the content is rejected.

Referring again to **Fig. 2**, LCS domain 204 may export content to any receiver (other than satellite unit 210) through path 224. This may include copying content to a rewritable media, creating a read-only media, rendering the content for use (e.g., playing, viewing, etc), etc.

Referring to **Fig. 5**, a flowchart depicting the process for content leaving LCS domain 204 is provided. In step 502, the content is retrieved from storage within the LCS. In step 504, the content is embedded with a watermark. In one embodiment, the watermark may be unique to the particular LCS, as determined by

the LCS Unique ID. The watermark may contain a hash that is created from the combination of the content characteristics (such as signal features, etc.) and the Unique ID. The watermark may optionally contain other data, such as a timestamp, a number of allowable copies, etc. This would be described as parameters of use, usage data, etc. which could be referenced when content is exported. If the export is to a storage medium, the LCS optionally can add a second hash to the file, external to the content, which can be used for further authentication. For security purposes, in one embodiment, the external hash may be created in a different manner from the embedded, watermark hash.

In step 506, the content is output from the LCS to the receiver.

Referring again to **Fig. 2**, path 226 connects LCS domain 204 with read-only media 208. Referring to **Fig. 6**, a flowchart depicting the process for content entering LCS domain 204 from read-only media 208 is provided. In step 602, the content is provided. In step 604, the content is checked for the presence of a watermark, such as a watermark for the particular LCS. If there is no watermark, a check is made in step 610 to see if the originality of the content can be determined. An example of such includes a media-based identifier that identifies the content as original.

If the content can be verified as an original, in step 608, it is stored as High Quality in the LCS domain. If the originality cannot be verified, in step 610, the quality is degraded to Standard Quality, and, in step 608, the content is stored in the LCS domain.

If a watermark is identified in step 604, in step 612, the hash is checked to verify that the content matches this LCS. If it matches, in step 608, the content is stored in LCS domain at High Quality. If it does not match, in step 614, the content is rejected.

Referring again to **Fig. 2**, path 228 connects LCS 202 with satellite unit 210. Referring to **Fig. 7**, a flowchart depicting the process for content entering LCS 202 from satellite unit 210 is provided. In step 702, the content may be watermarked before it is transmitted to the LCS. In step 704, the content is transmitted to the LCS.

In step 706, the content is checked by the LCS. This may include checking the LCS hash. If the hash matches, in step 708, the content is stored in the LCS domain as High Quality. If there is no hash, in step 710, the content is degraded to Low Quality, and in step 708, the content is stored in the LCS domain. If the hash does not match, in step 712, the content is rejected.

Referring again to **Fig. 2**, path 230 connects LCS 202 with satellite unit 210. Referring to **Fig. 8**, a flowchart depicting the process for exporting data from the LCS 202 to satellite unit 210 is provided. In step 802, the content is retrieved from storage within the LCS. In step 804, the security of the path between the LCS and the satellite unit is verified. Once the security is verified, in step 806, the content is exported to the satellite unit without a watermark.

If the security of the path cannot be verified, the export process mirrors that of an export to a receiver, depicted in **Fig. 5**.

Referring again to **Fig. 2**, path 232 is a path for content to be stored in satellite unit 210. In one embodiment, all content may be allowed to be imported into satellite unit 210, but may be automatically degraded to Low Quality when it is stored.

Path 234 is an export path for content rendered by satellite unit 210. In one embodiment, this content may be marked with a satellite unit watermark that contains a hash from the satellite unit Unique ID and any hash that is associated with the content from an LCS .

It should be noted that a hash function may be converted into a digital signature by performing a hash and encrypting the result of the hash. The uniqueness of the hash can vary with the hash function, while the digital signature adds a layer of confidence to the integrity of the data.

Other types of encryption, including transfer functions, may also be used.

Referring to **Fig. 9**, a flowchart of a method for trusted transactions according to one embodiment of the present invention is provided. In step 902, value-added information, or its tangible equivalent, is provided. This may be provided by a user that wishes to verify the value-added information.

In step 904, the perceptible data for verification may be maintained by a vendor or provider, and may be updated by a public-key secure digital watermark in

the observable packaging (if applicable). In those cases where security must be high, real time, or simply faster, key generation or signature generation functions may be enabled with embodiments of the present invention.

In step 906, the user provides a public key based on the identify held in the device to enable an authentication check.

In step 908, a response may be sent to the user.

Steps 906 and 908 may be repeated with further prompting for higher levels of authentication, or for additional checks. If the remote location provides the confirmation, or if a certification authority is involved, the response may be sent via secure transmission lines (e.g., encrypted transmission that can only be decrypted with the user's device and access to the user's stored private key). Alternatively, information may not need to be sent in a secure manner and may be checked upon delivery to the device to limit any remote communications breaches by unintended third parties.

Referring to **Fig. 10**, a device for trusted transactions according to one embodiment of the present invention is provided. Device 1000 may include steganographic cipher 1002. Steganographic cipher 1002 may be governed by at least the following elements: (1) a predetermined message; (2) a predetermined key/key pair; and (3) a predetermined carrier signal (image data, so images will be the primary data represented and ciphered).

Transducer 1004 may be provided. Transducer 1004 may include a charged coupled device (CCD), a personal entropy capture device (e.g., a retinal scanner, a thumbprint scanner, etc.), a touch pad (e.g., a pad for receiving a signature), an image capture device, a bar code reader, a magnetic card reader, etc. Transducer 904 receives the data in a physical format and converts it to an analog or digital format.

In one embodiment, the data from transducer 1004 may be marked with a timestamp for time-critical input.

Analog/digital converter 1006 may be provided. A/D converter 1004 may be used to convert analog information from transducer 1004 into predetermined digital format. In one embodiment, signatures may be converted in one format, images that

are captured in another format, and fingerprint/iris scans may be converted in another format.

A memory may be provided. The memory may include both volatile memory, and re-writable memory, such as DataSlim™.

A volatile device may be provided, such as a one time pad (private key of card holder/user), a one time memory or floating in the volatile memory to evade capture (stega-cipher computer code). This may be provided in a tamperproof casing.

Device 1000 may also include output 1020. Output 1020 may be any suitable output, including a connection port, a wireless port, a radio transmitter, etc. Before information is output from device 1000, it may be encrypted. In one embodiment, the information may be digitally watermarked. In another embodiment, the information may be digitally signed. In another embodiment, the information is not encrypted, and instead is transmitted over a secure transmission channel. Number generator 1008 may be provided. Number generator may be a random number generator, or it may be a pseudo-random number generator.

In addition, the device may include a controller, a power source, and an input and an output.

Information may be converted into a humanly perceptible form (chemical/electrical/magnetic such as a humanly visible chemical test result, as with a pregnancy tests, an EKC, an MRI or CatScan image, are all converted into "humanly perceptible form for "human" analysis) prior to authorization of a transaction/decision event.

EXAMPLES

In order to better understand the present invention, several examples are provided. These example do not limit the present invention in any way, and are intended to illustrate embodiments of the present invention.

1. Smart Telecommunications

At present, large volumes of commerce and commerce-related activities are performed using telephone connections. Authentication of identity is an ongoing concern in such transactions. Present technology allows the verification of the

origin of a landline phone call (POT), but offers no assurances as to the identity of the user. Furthermore, simple identification of the origin of the call is only useful insofar as that phone number can be used to index a database of callers. The present invention allows for bi-directional verification of identity during a phone call, with the option of partial or full concealment of identity.

A consumer may wish to make a purchase on the phone. Presently, the consumer's identity is established by the seller using personal information from the consumer, such as a credit card number, an address, a phone number, etc. However, all of this information may be known by an imposter. A smart phone transmits identity information (perhaps embedded as a watermark in the audio connection), in response to a query from the seller. The receiver verifies the buyer's identity with a certification authority. Furthermore, the consumer may also verify the authenticity of the seller's identity at the same time, by the same method. The consumer may choose not to respond to certain queries in real time.

The smart phone may require a level of identity disclosure before it accepts an incoming call. For instance, telemarketers may be required to reveal the name of their company before the call is accepted by the smart phone. Consumers may protect themselves from fraudulent sellers by requiring such identification. Further, legitimate sellers may be assured that their customers know that they are legitimate. The certification authority assures the consumer and seller that they are receiving authentic identifications.

2. Equity Programs As A Value-added Component

Another embodiment of the present invention relates to methods and means of payment includes a novel means for encouraging alignment of buyer and seller interests. Similar to cooperatives, membership programs (in proprietary form, co-branded with a financial institution, or implemented as a specialty device that can handle these equity transactions) may be enhanced to offer buyers the opportunity to purchase options in equity of the seller's company or related institution. Instead of being given cash or points, at some fixed point in time, consumers and sellers may be provided with the opportunity to purchase equity as available on some public or private market or exchange.

These options may be built into the functionality of the actual transaction device and may be coupled with both trusted transactions or general transaction systems. Settlement of the option may be based on any known option pricing mechanism (such as the well-known Black-Scholes model) and predetermination of terms for settlement and conversion of the option. This approach incentivizes and encourages clearer alignment of all market participants in the value and condition of the equity of the entity with which transactions are being handled or negotiated. Independent certification authorities, or infomediaries that are able to ensure or verify a transaction or related information, may be used to ensure that such equity programs can be trusted. Any relevant disclosures concerning legal or financial restrictions are simply additional value-added components for consideration.

3. More security - body movements for entropy and pharmaceutical use control

A related embodiment according to another embodiment of the present invention includes an interface for detection of body movements (eye movements, blinks, voice pass phrases, etc.). These movements may include predetermined sequences of movements that may be ciphered in a manner similar to encrypting ASCII pass phrases. This is a novel implementation of human movement in generating symmetric or asymmetric cryptographic keys. The transducer may include any number of means of capturing human-based body movements in real time for instantaneous verification of an authorized user. Moreover, unlike simple biometrics, a series of body movements (similar to the act of signing in writing, but likely to be more difficult to capture for unauthorized misuse -- a signature, like a fingerprint, is able to be observed and copied without permission or knowledge of the signature author) is difficult to copy.

The movements or similar biological entropy (transduced from biomedical, bioengineered, biochemical or biophysical information that may be made perceptible and encrypted or securely watermarked for later comparison or real time verification) may be captured by a transducer of analog signals and converted into digital binary information used for comparison with any number of stored corresponding instructions or messages to be decrypted. These signals may be multidimensional (2D, 3D, 4D- with a time component, etc.) to increase the information space and make discovery of hidden secrets more computationally

difficult. Images, medical or human-condition based, audio signals, video, virtual reality, multimedia, etc. all provide rich media information in which to enhance the security of any embodiment contemplated by the present invention. Combinations of multidimensional media for varying ciphering options as well as steganographic embedding are also contemplated as a means for furthering ensuring computational complexity to any unauthorized user. Steganographic-mapping (watermarking) or transfer functions (scrambling or "chaffing") may be combined with encryption ciphers as a means for making each unique implementation or tangible device -- serialization or personalization of a method for engaging in trusted transactions, high risk, information-intensive or sensitive decision (military use, security use, restricted government use, privacy use, or any number similar commercial or noncommercial decision or transaction events).

Additional embodiments include actual control over the use or access to pharmaceuticals based on medical risk, condition or personalized advice to the user. Tangible methods for transfer of chemical, biological or physical agents intended for medical use or individualized control based on third party conditions (legal, medical, governmental, etc.) are governed by manipulation of the apparatus, device or system used to introduce foreign agents (informational, intangible or tangible) into patients (the intended, authorized or verified user).

Highly secure and artificial environments, such as aircraft flying simulations or visual financial trading information, may be representative of more risk to owners of actual tangible planes or tangible assets related to any financial information. Recognition of a digitized iris does not enable movement based confirmation of future secrets (the movements) that may be changed, destroyed or updated to ensure consistent or higher degrees of security maintenance. For some body movements, it may be possible to maintain better security than with written information. In other words, certain body movements may be prevented, or made difficult to perform even under rigorous demand by unauthorized agents. Blinking or other facial movements may be made impossible to verify the real time identity of the user. This adds a layer of security and increases the difficulty of defeating a cipher or a series of related ciphers (encryption-based or steganographically-based, where the digitized signal has humanly-perceptible fidelity or characteristics) depending on access or

sensitivity of information. It also maybe psychologically or human-rule driven. Certain humanly observable body movements, or detectable "telemetry-type" data (brain activity, heart beat, pulse, or any other medically observable information) may be either unique to an individual or simply general to certain behavior. This data may be important to use as a means of preventing poor decision-making, or requiring higher diligence before transacting or executing a given operation. At the least, the movements are a means for predetermining and assisting the generation of a binary key or seeding the generation of a cryptographic key, message or signature.

Any particular instance may be successively stored in subsets of any primary value information or value-added components (single key or key pair associated with a single message or signature to further serialize data that may have steganographic capacity for imperceptible embedding in the carrier signal, primary or value-added components data). The operation may be highly demanding, or may require human-based or driven or initiated decisions. The instructor, or the user, may have predetermined the conditions that indicate confidence or lack thereof at the time of the verification or authentication of the user. This may be for security reasons, or simply risk management, as information is increasingly processed at higher speeds and may require greater care in ensuring information data integrity. As well, humanly-observable (and convertible into binary data for deciphering) movements enable a form of bridging analog, human trust with digital or mathematically provable, actuarially, statistically, deterministically known or predictable measures of risk and trust. This novel feature is an additional benefit over the prior art and ensures future human-like characteristics in "digital" (underlying, "measurable" or "estimable" data integrity, authentication and confidence), electronic (analog transducers and transmitters), or binary transaction systems. Further security or serialization of transaction event information (human movement or observable condition used for secret key or equivalent generation) enable additional forms of trusted transactions.

Additional security may be assured with temporal-based limits on human body movement or biologically observable human condition (by use of a medical or human directed transducer). Interlocking keys and messages with blind signatures, or onion routing transmission techniques to obscure the identity of the user, are

further enhancements that may guarantee a high level of privacy to the user of the system or device. Information formats may be encrypted or have stored primary or value-added component information that has to arrive to the user without any digitally evident tampering for the user to make the best possible decision regarding the observed information.

Unlike the prior art, embodiments of the present invention consider the perceptibility of information to bridge human trust and confidence with cryptographic or "mathematical" measures or estimates of "security," "data integrity" or "trust." This is novel to the art of data security and secured transaction or transmission technologies.

4. Algorithmic Information Theory (AIT) for additional security

By implementing predetermined indications of mathematically provable randomness, the ability to discover secrets and human choice, based on unprovability or incompleteness, as discussed and is well-known in the art as originating with Godel (incompleteness theorem) and Turing (halting problem, uncomputability). Chaitin "discovered" randomness, stating essentially that randomness can be described mathematically, and thus differentiations between discrete and infinite randomness are logically observable. Because truth is relative in a quantum mechanical sense, degrees of credibility concern the level of trust that may be offered in any trusted transaction system. While the primary value that concerns us is information, the ability to describe programming size complexity (that is optimized functional data) enables self-limiting software to be programmed. To the extent that trusted transactions can never be physically perfect operations, uniqueness of information, as both data and code, is particularly important to providing higher security when computational cost and bandwidth is extraordinarily cheap.

Essentially, choice over answers to questions that cannot be characterized as "True" or "False," such as "This statement is false," have inherent randomness and are thus ripe for paradoxical response. More intricate paradoxes, Berry's Paradox, Turing's halting problem, as well as Chaitin's definition of "randomness," are sure to enable predictable infinite and finite (discrete) randomness with which to seed and cryptographic secret or generation of a symmetric, asymmetric key or digital

signature. Human perception as a means for enabling analog trust may be made inherently more secure by choosing responses to paradoxes that have no computable value. That Chaitin can describe "randomness" with logically structured instructions for the halting problem, in LISP or C programming languages, including the computer programming language of Mathematica, enabled the development of a randomness constant.

The equations of randomness may be implemented in software and offer a unique and novel means for further securing the generation of cryptographic or steganographic seeds, secrets, keys or messages. Of course, differences between any of these information elements as to the means for securing or authenticating data would enable flexible architectures combining various ciphers and methods for arriving at a rule for validation, authenticity, data integrity, confidence or enabling any subsequent manipulation of the associated data (primary value-added or value-added components).

5. Entertainment media exchange

According to one embodiment of the present invention, the device may be used for the exchange of entertainment media. This may include audio, video, multimedia, etc. In such an exchange, the perceived risk of value-added information piracy is relatively high for the seller or provider, while the perceived risk is relatively low for the purchaser. The obvious risk is that all potential "consumers" of the media access and copy the entertainment media for free. For music or video, or similar entertainment good, according the present invention provides the following structure may be used.

a) Fragile watermark structure

The fragile watermark, according to one embodiment of the present invention, can actually hold an entire value-added component, encoded in the least significant bit (LSB) of each 16-bit sample. This gives a data rate of 88200 bits per second in a stereo CD file, or a capacity of 1.89 M in a 3 minute song. This is an immense capacity relative to the expected size of the value-added component (100 - 200 K).

The fragile watermark is preferably bound to a specific copy (Unique ID) of a specific song (Unique ID), so that it cannot be transferred to other songs. This binding can be achieved through use of a hash in the following sequence:

(1) A block of value-added component is encoded into a block of samples.

(2) A hash of the value-added component block and a random number seeded by the owner's identity (Device or system Unique ID) is generated and encoded into the subsequent block of samples.

(3) A hash of the first two blocks of samples and a random number seeded by the owner's identity is generated and encoded into a third block of samples.

(4) Repeat steps 1-3 as necessary.

Each value-added component block may have the following structure:

```
{
    long  BlockIdentifier;     //A code for the type of block
    long  BlockLength;         //The length of the block
    ....                       //Block data of a length matching
BlockLength
    char  IdentityHash[hashSize];
    char  InsertionHash[hashSize];
}
```

An application can read the block identifier and determine if it recognizes the block type. If it does not recognize the block type, it can use the BlockLength to skip this block.

Certain Block Types are required to be present if the value-added component is to be accepted. These may include and identity block and a value-added component Hash block. The Block Data may or may not be encrypted, depending on whether the data is transfer-restricted (value-adding) or simply informative. For instance, user-added value-added component data would not need to be encrypted. The BlockIdentifier would indicate whether the block data was encrypted or not.

b) Robust open watermark

This is the mark that may indicate non-legacy content. In one embodiment, there may be two possible settings. "1" indicates non-legacy content that must be accompanied by a authenticable value-added component for entry into the domain (e.g., EMD or Electronic Media Distribution media content). "0", on the other hand, indicates non-legacy media that was distributed in a pre-packaged form (e.g., CDs, DVDs, game software, etc.). "0" content may or may not have a value-added component. "0" content may only be admitted from a read-only medium in its original file format (e.g., a "0" CD may only be admitted if it is present on a Red Book CD Specification medium).

c) Robust forensic watermark

This watermark may not be accessible to the consumer in any way. It may be secured by a symmetric key held only by the seller (or an asymmetric key pair that may be desired for some embodiments). A transaction ID may be embedded at the time of purchase with a hash matching the symmetric key (or key pair). The watermark may then be embedded using a very low density insertion mask (< 10 %), making it very difficult to find without the symmetric key. Retrieval of this watermark is not limited by real-time/low cost constraints. The recovery will only be attempted on pirated material. A recovery time of 2 hours on a 400 MHz PC is reasonable.

6. Additional parameters for value-adding components

Physical shipment of packaged goods or services (value-added information) is anticipated as being a potential option to consumers or purchasers as well as sellers and providers. That the value-adding information may be packaged or represented tangibly does not obviate the need for trusted transactions to ensure payment and the appropriate division of rights and responsibilities for various goods (a DVD for music or video), services (smart credit card or insurance card) or markets (trusted telephone system, government identification schemes). This type of transaction represents additional benefits over embodiments in the existing art -- on-demand trusted transactions and physical manufacture/delivery of goods is enabled, without risk to the overall system and its value-added information security. This amounts essentially to serializing or personalizing, depending on the

perspective in the transaction, each and every transaction, while building trusted transactions for the benefit of the marketplace for goods services and information.

7. Financial Or Insurance Device

The present invention enables systems and supported devices that are useful in situations where parties need to have pre-defined limits to risk exposure, such as an insurance policy or a claim. These systems are generally characterized by an emphasis on transmission and data security, which reduces the perceived risk of the insurer (a seller of risk coverage for pre-determined events). To the extent that insurance takes into account the history and existing condition of an asset, a measure of context or structure (tangible as well as intangible) to be covered, as well as an economically-based replacement value (though to confuse matters, there are also issues concerning such items as after market versus brand new, brand versus generic, etc.), there exist differences with more transparent financial devices. Financial devices (essentially a "credit agreement" or credit facility based on an imprecise estimate of condition but also experience or trust) rely on the ability, perceived or actuarially observable, to repay credit extended on behalf of the device holder. Whereas financial or credit history is transparent in many cases, private information about an individual's history or condition are perceived to be have higher implicit value to the user. Financial devices and insurance devices converge at those points where privacy or personal information are equivalent with financial or credit information. Both types of risk have differing requirements for updating or adjustment over the course of use of a particular line of credit or insurance policy.

Cars may be embedded with telemetry sensors to determine the real time condition of various components, such as the frame, engine, brakes, or any combination of components mutually deemed to justify such monitoring. Alternatively, a smart card-like device equipped with a transducer may be used to "capture" images of items that are packed (for travel insurance purposes), insurable items in a residence (for homeowner's insurance purposes), etc. Any image captured may be securely watermarked by the device and then exported to an insurance provider via a transmission line (an ATM, a wireless connection such as a mobile phone, a PC modem connection, etc.). An insurance provider may offer such

services at auto service/repair facilities, airports, etc. with a mutual reduction in claims costs and adjustments costs.

Medical information may similarly be digitally stored, securely watermarked, and time-stamped (for any perceptible data stored, such as images or voice) for reference to an individual's health. based on varying levels of access to stored information, which may be distributed among different physicians or handled by a central medical information infomediary. The secured image may be sent to an insurance provider as a secured image (both the device and storage facility may independently verify the security or tamperproofing of the perceptibly represented information). The doctor, patient, health care provider, government agencies can all have varying degrees of access that can be made transparent to the patient. This is an inherent benefit over the prior art in that the patient can see those records that are then watermarked and securely stored.

Additionally, the present invention provides the novel feature of enabling the same information, at the request or demand of the patient, to be sent to a personal or secure storage "space," so that patients may have more accessibility and control over their own medical records and medical conditions. In one embodiment, the information may be provided as digitized bits. In another embodiment, the data may be provided in a tangible form.

The information may be stored as tangible records or intangible, bit-represented records. Doctors may use tamperproofed signals (watermarked audio, image, video, virtual reality, any humanly-perceptible signal) and records that are perceptible to lower insurance costs and potential liability. The prior art ignores the mutual benefits afforded by bi-directional information exchange (that can be tamperproofed with secure watermarking) and transparency in creating opportunities for trusted transactions.

Additional data, such as the transaction information that may be evidenced on a credit card bill or statement, may also be automatically associated with the stored image(s) for later use. In one embodiment, the user may send the same secured data to a private data storage facility, or create personalized records, which may serve as a secondary set of records against which other data sent to the insurance or financial provider may be verified or validated. According to another

embodiment of the present invention, authorized mechanics, physicians, and pharmacists, may add to, but not access or manipulate, previously stored data. These individuals may also be bound by rules for establishing the history and condition of any person or physical good that is being underwritten or financed.

The present invention provides certification authorities the ability to determine the authenticity of data. In cases where public-key steganography or cryptosystems are preferred, the embodiments extend to those implementations as well. Moreover, they enable secure transmission capabilities over unsecured data transmission lines.

Referring to **Fig. 11**, a personal information device according to one embodiment of the present invention is provided. Personal information device (PID) 1102 may be used with financial institutions, insurance companies, etc.

In one embodiment, PID 1102 may be smart card; that is, a device that resembles a credit card, but includes a processor, a power supply, a memory, and an input and output device. In another embodiment, PID 1102 may be a card including a magnetic strip.

PID 1102 preferably has a Unique ID. In one embodiment, the Unique ID of PID 1102 may be a policy number, a social security number, etc.

PID 1102 may receive information from several sources. In one embodiment, telemetry data 1104 may be input to PID 1102. Perceptible data 1106, such as images, photos, etc. may be input to PID 1102. In still another embodiment, associated data, such as purchase receipts, descriptions, serial numbers, registrations, etc., which may be value-adding components, may be input to PID 1102.

PID 1102 may provide output data 1110 to a variety of entities. In one embodiment, output data 1110 may be provided to company 1112 and to storage 1114. Company 1112 may include any organization the may receive output data 1110, including an insurance company, a financial institution, etc. Storage 1114 may include any personal use for output data 1110, including a private data storage such as a fixed storage media, paper records, etc. Company 1112 and storage 1114 may receive output data 1110 in different formats. In one embodiment, output data 1110 is provided according to predetermined parameters for the entity.

Output data 1110 may be watermarked, or it may be time stamped, or it may include both. Other types of encryption are provided.

In general, output data 1110 is preferably provided to the entity via a secure communication link. Transmission of output data 1110 may be controlled by the entity (e.g., company 1112 or storage 1114) or by the user.

8. Authentication Device

According to another embodiment of the present invention, an authentication device may be provided. Referring to **Fig. 12**, authentication device 1202 may be a credit-card sized "smart card," including a processor, a power supply, a memory, and an input and output device. In another embodiment, authentication device 1202 may be a palm sized computing device.

A variety of input devices may be provided. In one embodiment, a bar code scanner may be used. In another embodiment, a keypad may be used. Other input devices may be used as necessary.

In one embodiment, authentication device 1202 may include a display, such as a LCD screen. Other display technologies are within the contemplation of the present invention.

In one embodiment, authentication device 1202 may be a government-issued device.

Anonymous authentication 1204 may be provided. Anonymous authentication 1204 may be used to authenticate a product, a medicine, a label, etc. Anonymous authentication 1204 communicates with authentication device 1202 to authenticate the item in question. In one embodiment, authentication device 1202 may display relevant information, such as known warnings, recommended dosages, etc. regarding the item in question.

In another embodiment, image capture device 1206 may be provided. Image capture device 1206 may include a digital camera, a scanner, etc. In one embodiment, image capture device 1206 may time stamp the image as it is captured.

Identity exchange 1208 may be provided. Identity exchange 1208 includes a Unique ID that may be authenticated or modified by the user. In one embodiment, in order to verify the identity of an individual, additional independent identify

verification may be required in addition to identity exchange 1208. This is because authentication device 1202 may be stolen, borrowed, etc.

Certification authority 1210 may be provided. Certification authority may be bound by federal, state, and local laws. In addition, private restrictions may apply to certification authority 1210.

In one embodiment, certification authority may be further bound by geographical (e.g., location) or age basis (e.g., date of birth, age, etc.) to verify.

Referring to **Fig. 13**, a method of use for an authentication device is provided. In step 1302, a user locates information to be authenticated. This may include a variety of information. The information is then entered into the authentication device.

In step 1304, perceptible data is marked with a public key secure watermark. In one embodiment, this may be done in real time.

In step 1306, the user provides a public key to initiate the authentication.

In step 1308, a response is sent from the certification authority, or additional prompts for higher access levels are provided.

In one embodiment, transmissions between any elements may be over a secure communication link, including SSL or similar transmission exchange.

In another embodiment of the present invention, an authentication device may comprise a Internet web browser. For example, the authentication device may be a "plug in" for a web browser. Such a authentication device may be used to verify, or authenticate, items on web pages. For instance, according to one embodiment of the present invention, the authentication device may be used to verify that an Internet bank that displays the FDIC logo is authorized to display this logo. In one embodiment, real time verification will allow a user to verify such, and govern transactions accordingly.

It will be evident to those of ordinary skill in the art that the above-described modes and embodiments of the present invention, while they disclose useful aspects of the present invention and its advantages, are illustrative and exemplary only, and do not describe or delimit the spirit and scope of the present invention, which are limited only by the claims that follow below.

I CLAIM:

1. A method for trusted transactions, comprising:

establishing an agreement to exchange digitally-sampled information between a first and a second party;

exchanging the digitally-sampled information between the first and the second party; and

approving the digitally-sampled information using an approval element selected from the group consisting of a predetermined key, a predetermined message, and a predetermined cipher, the step of approving the digitally-sampled information using an approval element consisting of a step selected from the group consisting of verifying the digitally-sampled information with the approval element, authenticating the digitally-sampled information with the approval element, and authorizing the digitally-sampled information with the approval element.

2. The method of claim 1, wherein the step of approving the digitally-sampled information precedes the step of exchanging digitally-sampled information.

3. The method of claim 1, wherein the step of approving the digitally-sampled information comprises:

transmitting a first party approval element from the first party to the second party; and

transmitting a second party approval element from the second party to the first party.

4. The method of claim 3, wherein the steps of transmitting the first party approval element and transmitting the second party approval element occur substantially simultaneously.

5. The method of claim 3, wherein the first party approval element and the second party approval element are symmetric.

6. The method of claim 3, wherein the first party approval element and the second party approval element are asymmetric.

7. The method of claim 1, wherein the approving step is accomplished using predetermined key pairs.

8. The method of claim 7, wherein the predetermined key pairs are created by a cipher selected from the group consisting of steganographic and cryptographic ciphers.

9. The method of claim 1, wherein the predetermined cipher is selected from the group consisting of a steganographic cipher and a cryptographic cipher.

10. The method of claim 1, wherein the predetermined message is selected from the group consisting of a unique identification, a unique time, data associated with a predetermined information function, and combinations thereof.

11. The method of claim 1, wherein the predetermined message has value independent from at least one primary value-adding component.

12. The method of claim 1, wherein the predetermined message contains at least one value-adding component.

13. The method of claim 1, wherein the step of approving the digitally-sampled information comprises:

verifying the digitally-sampled information with the approval element.

14. The method of claim 1, wherein the step of approving the digitally-sampled information comprises:

authenticating the digitally-sampled information with the approval element.

15. The method of claim 1, wherein the step of approving the digitally-sampled information comprises:

authorizing the digitally-sampled information with the approval element.

16. The method of claim 1, further comprising:

entering into a security arrangement based on the exchange.

17. The method of claim 16, wherein the security arrangement is a non-cash right.

18. The method of claim 16, wherein the security arrangement is an option for a non-cash right.

19. The method of claim 16, wherein the security arrangement is an equity purchase right.

20. A method for conducting a trusted transaction between two of a plurality of parties who have reached an agreement to transact, comprising:

establishing a secure transmission channel between the two parties;

approving an identity of at least one of the two parties;

determining an amount of value-added information to be exchanged between the parties, the value-added information comprising a plurality of value-adding components;

verifying the agreement to transact; and

transmitting the value-added information.

21. The method of claim 20, wherein the step of approving an identity of at least one of the two parties comprises:

at least one of the parties verifying at least one value-adding component.

22. The method of claim 20, wherein the step of approving an identity of at least one of the two parties comprises:

at least one of the parties authorizing at least one value-adding component.

23. The method of claim 20, wherein the step of approving an identity of at least one of the two parties comprises:

at least one of the parties authenticating at least one value-adding component.

24. The method of claim 20, wherein the step of establishing a secure transmission channel between two of a plurality of parties comprises:

exchanging data between the two parties;

selecting a pre-determined key to exchange over the secure transmission channel; and

securing the transmission channel by at least one of a password, a pass phrase entry, a query to a user, and real-time biometric data transfer.

25. The method of claim 20, wherein the step of approving an identity of at least one of the two parties comprises:

exchanging a value-adding component for each party to the other party.

26. The method of claim 20, wherein the step of approving an identity of at least one of the two parties comprises:

at least one of the parties independently verifying a value-adding component of the other party.

27. The method of claim 20, wherein a bandwidth of the primary value-added information comprises a description including at least one of a bandwidth requirement for transmission, a bandwidth requirement for storage, and a bandwidth requirement for playback.

28. The method of claim 20, wherein at least one term for the exchange of primary value-added information is negotiated between parties, the terms selected from the group consisting of an offer, an acceptance, and consideration.

29. The method of claim 28, wherein the at least one term changes in real time.

30. The method of claim 28, wherein access to the at least one term is restricted by at least one of a pass phrase, a password, a correct answer to a query, a real time authentication with a biometric, a real time authentication with personal entropy information, real time telemetry data, and access to additional transaction records.

31. The method of claim 28, wherein the at least one term is referenced by a subsequent transaction.

32. The method of claim 28, wherein the at least one term is access restricted by a provider of at least one value-adding component.

33. The method of claim 28, wherein the at least one term is traced by a provider of at least one value-adding component.

34. The method of claim 28, wherein the at least one term is authenticated by a provider of at least one value-adding component.

35. The method of claim 28, wherein the at least one term is accessed for at least one of verification, authentication, and authorization.

36. The method of claim 28, wherein the at least one term comprises at least one of readable text, visible color, voice command, and visual instructions.

37. The method of claim 28, wherein the at least one term comprises humanly perceptible information.

38. The method of claim 20, wherein the value-added information is convertible into a tangible good.

39. The method of claim 20, further comprising verifying the value-added information.

40. The method of claim 20, further comprising authenticating the value-added information.

41. The method of claim 20, wherein the value-adding components comprise at least one of an equity purchase right, an option, a warrant, and a security instrument.

42. The method of claim 20, wherein the value-adding components comprise a non-cash service.

43. A method for conducting at least one trusted transaction between at least two parties, comprising:

authenticating the at least two parties;

agreeing to a security of a transmission channel;

exchanging secondary value-added information;

determining at least one term for a primary value-added information exchange; and

facilitating payment for the transaction based on the terms.

44. The method of claim 43, wherein the step of facilitating payment for the transaction is accomplished in real-time.

45. The method of claim 44, wherein the at least one term includes micropayment systems.

46. The method of claim 43, wherein the transaction is governed by at least one of legal restrictions that apply to at least one of the parties, a timing of the transaction, a geographic location of the transaction, and value-added information.

47. The method of claim 43, wherein the value-added information is represented physically.

48. The method of claim 43, wherein the secondary value-added information comprises at least one of an equity option and at least one term from a previous trusted transaction.

49. The method of claim 43, wherein the secondary value-added information derives benefit from a previous trusted transaction.

50. The method of claim 49, wherein the at least two trusted transactions are substantially contiguous.

51. The method of claim 49, wherein the at least two trusted transactions have at least one of a time or an event limitation.

52. The method of claim 43, further comprising the step of:

agreeing to at least one term for a different transaction.

53. The method of claim 43, wherein the first trusted transaction enables manipulation of information in a subsequent transaction.

54. A method for conducting a trusted transaction between at least two parties, comprising:

establishing a steganographic cipher;

exchanging secondary value-added information between the parties;

agreeing to at least one term for the exchange of primary value-added information; and

facilitating payment for the transaction.

55. The method of claim 54, wherein the step of facilitating payment for the transaction is accomplished in real-time.

56. The method of claim 54, wherein the step of facilitating payment for the transaction is based on the at least one term for the primary value-added information exchange.

57. The method of claim 54, wherein the transaction is governed by at least an age and a geographical limitation.

58. The method of claim 54, wherein the transaction is governed by at least one of legal restrictions that apply to at least one of the parties, a timing of the transaction, a geographic location of the transaction, and value-added information.

59. The method of claim 54, wherein at least one of the primary and secondary value-added information is represented physically.

60. A method for conducting a trusted transaction between at least two parties, comprising:

identifying at least one of a unique identification for each of the at least two parties, a unique identification of the transaction, a unique identification of value-

added information to be transacted, and a unique identification of a value-adding component;

applying a steganographic cipher; and

verifying an agreement to transact between the parties.

61. The method of claim 60, wherein the trusted transaction is governed by at least one of a transaction age and a geographical location of the transaction.

62. The method of claim 60, wherein the trusted transaction is governed by legal restrictions that apply to at least one of the parties, a timing of the transaction, and value-added information.

63. The method of claim 60, wherein the value-added information is represented physically.

64. The method of claim 60, further comprising the step of:

transmitting the value-added information.

65. The method of claim 60, wherein the agreement causes at least one secondary term to be enabled for at least one of the parties.

66. The method of claim 60, wherein the agreement creates at least one term for a second trusted transaction.

67. The method of claim 60, further comprising the step of:

agreeing to at least one term for a second trusted transaction.

68. A method for bi-directionally exchanging value-added information between at least two parties, comprising:

associating a plurality of unique identifiers with the value-added information, the value-added information including at least one of a digital watermark, a file header, a file attachment, and a file wrapper;

associating each of the at least two parties with unique identifiers, the unique identifiers including at least one of a digital watermark, a file header, a file attachment, and a file wrapper; and

exchanging value-added information between the at least two parties.

69. The method of claim 68, wherein the transaction and the unique identifiers are stored for subsequent reference.

70. The method of claim 68, wherein unique identifiers are access restricted by at least one pre-determined rule.

71. The method of claim 68, wherein the unique identifiers are asymmetrically access restricted.

72. The method of claim 70, wherein the access restriction is dependent on verification of a querying party.

73. The method of claim 70, wherein the access restriction allows value-added information to be transmitted in an altered format.

74. The method of claim 68, further comprising the step of:

associating the bi-directional exchange of value-added information with a subsequent exchange of additional value-added information.

75. The method of claim 74, wherein the additional value-added information is governed by at least one separate term.

76. The method of claim 74, wherein the additional value-added information comprises a right to purchase equity in at least one of the parties to the transaction.

77. The method of claim 68, further comprising the step of agreeing to at least one term for a subsequent transaction.

78. A method for exchanging value-added information between at least two parties, comprising:

providing a data transmission means;

verifying the parties to the transaction;

negotiating at least one term selected from the group consisting of a price, a service, a selection, and combinations thereof; and

binding the at least one term to the information using at least one of a digital watermark, a file header, metadata, and a file wrapper;

wherein the at least one bound transaction term comprises value-added information.

79. The method of claim 78, wherein the at least one bound term cannot be removed without altering the value-added information.

80. The method of claim 78, wherein an authentication of the value-added information requires successful verification of the at least one bound term.

81. A method for trusted transactions, comprising the steps of:

receiving data to be processed;

determining a structure of the data;

determining if the data is authentic; and

determining an associated usage of the data based on the data structure and the authenticity of the data.

82. The method of claim 81, wherein the data is comprises at least one of aesthetic data and functional data.

83. The method of claim 81, wherein the structure of the data is determined based on at least one of a digital signature, a digital watermark, and a digital notary.

84. The method of claim 81, wherein the authenticity of the data is determined based on at least one of a digital signature, a digital watermark and a digital notary.

85. The method of claim 83, further comprising the step of verifying at least one of the digital signature, the digital watermark, and the digital notary by at least one of a trusted third party and a certification authority

86. The method of claim 83, wherein a bit from at least one of the digital signature, the digital watermark and the digital notary can be verified by at least one of a trusted third party and a certification authority.

87. A method for secure transaction, comprising:

receiving a request to process a transaction;

uniquely identifying a source of the request;

uniquely identifying at least one term of the request; and

storing identification information for transaction negotiation.

88. The method of claim 87, wherein the at least one term of the request includes at least one of a condition and a timing of the request.

89. The method of claim 87, wherein the request may be received over at least one of a secure and an unsecure transmission line.

90. The method of claim 87, wherein the source of the request is identified by at least one of a determinable origin of the source and a predetermined routing of the request by the seller.

91. The method of claim 87, wherein the at least one term of the request comprises a value-adding component.

92. The method of claim 87, wherein the transaction is noncontiguous with the request.

93. The method of claim 87, wherein the transaction and the request are processed in real time.

94. A method for the facilitation of the exchange of information data between at least a first party and a second party, comprising:

receiving a rule governing information data from a first party;

receiving a request for the information data from a second party;

matching the rule with the request; and

uniquely identifying the information data and the first and second parties;

wherein the information data is selected from the group consisting of unstructured data and structured data.

95. The method of claim 94, wherein the rule governs a use of the information data.

96. The method of claim 95, wherein the use comprises manipulating the information data.

97. The method of claim 95, wherein the use comprises transferring the information data.

98. The method of claim 95, wherein the use comprises subsequently changing to the information data.

99. The method of claim 95, wherein the use comprises playing the information data.

100. The method of claim 95, wherein the use comprises recording the information data.

101. The method of claim 95, wherein the use comprises converting the information data from at least one of analog to digital format and digital to analog format.

102. The method of claim 94, wherein the structured data comprises at least one of source code and executable code.

103. The method of claim 94, wherein the request may be filtered according to at least one of a characteristic, a function, an aesthetic, a condition, a history, a context, a consideration, a cost, a time, a bandwidth requirement, a storage

requirement, an available format, an owner identification, a creator identification, a seller identification, an infomediary identification, a distributor identification, a distribution parameter, an age in unit of time, and a upcoming information data.

104. The method of claim 94, wherein the unique identification is cryptographically secure.

105. The method of claim 104, wherein the unique identification may be cryptographically secured by using at least one of a cryptographic cipher, a stegnographic cipher for digital signatures, a special one-way hash, a digital watermark, and a time stamp, and combinations thereof.

106. The method of claim 94, further comprising the step of verifying the unique identification by an independent third party

107. The method of claim 106, wherein the independent third party comprises at least one of a certification authority, a creator of the information, an owner of the information, and a mutually agreed to third party.

108. The method of claim 94, wherein the exchange is in real time.

100. The method of claim 94, wherein the exchange is substantially noncontiguous.

110. A method for rights management, comprising:

receiving information;

determining whether the information is structured information or unstructured information;

identifying the information with a steganographic cipher;

authenticating the information with at least one of a digital signature and digital watermark check; and

associating the identification and authentication results with at least one of a predetermined record, a predetermined rule, and a predetermined function.

111. The method of claim 110, further comprising the step of:

limiting an access to the information based on a predetermined exposure of a decision maker.

112. The method of claim 110, further comprising the step of:

limiting a financial exposure based on a predetermined exposure of a decision maker.

113. A method for rights management, comprising:

exchanging information between at least two parties;

verifying the information, the verification performed by at least one of the parties; and

activating at least one of a predetermined act and a rule based on the result of the verification of information.

114. The method of claim 113, wherein information is exchanged in a format selected from the group consisting of an analog waveform and binary data.

115. The method of claim 113, further comprising the step of authenticating the verification by a trusted third party.

116. The method of claim 113, wherein an anonymity of each party is maintained during the step of verifying the information.

117. The method of claim 113, further comprising the step of making the verification publicly available for additional verification.

118. The method of claim 113, wherein the predetermined rule is activated noncontiguously with verification.

119. The method of claim 113, further comprising the step of making the accessible for further authentication and identification.

120. A method for risk management, comprising:

receiving information;

determining whether the information is structured or unstructured;

identifying information with a predetermined ciphered key;

authenticating information with at least one of a digital signature, a digital watermark check, and a predetermined ciphered key;

associating identification and authentication results with a predetermined rule; and

limiting access based on a predetermined exposure of a decision maker.

121. A method for securely exchanging information data between at least two parties, comprising:

creating a private key;

deriving a corresponding public key corresponding to the information data sought and at least one of (a) verifiable data associated with different versions of the

information data, (b) verifiable data associated with a transmitting device, and (c) verifiable data associated with an identity of the party seeking the information data;

establishing a set of one time signatures relating to the information data;

establishing a hierarchy of access to the set of one time signatures;

creating a public key signature that is verifiable with the public key, including the hierarchy of access to the set of one time signatures;

providing the information to a certification authority for verification; and

verifying the one time signature and the hierarchy of access to enable transfer of predetermined data.

122. A method for authenticating an exchange of a plurality of sets of information data between at least two parties, comprising:

creating a plurality of hierarchical classes based on a perceptual quality of the information data;

assigning each set of information data to a corresponding hierarchical class;

defining access to each hierarchical classes and to each set of information data based on at least one recognizable feature of the information data to be exchanged;

predetermining access to the sets of information data by perceptually-based quality determinations;

establishing at least one connection between the exchanging parties;

perceptually recognizing at least one of the sets of information data dependent on user provided value-added information data; and

enabling a trusted transaction based on verification, and associated access, governing at least one of a set of information data sets.

123. The method of claim 122, further comprising the step of grouping each hierarchical class by at least one of a quality, a price, and a service.

124. The method of claim 123, wherein the grouping is determined by at least one of a buyer and a seller.

125. The method of claim 123, wherein the grouping enables greater exchange of information.

126. A method for authenticating the exchange of perceptual information data between at least two parties over a networked system, comprising:

creating a plurality of hierarchical classes based on a perceptual quality of the information data;

assigning each set of information data to a corresponding hierarchical class;

defining access to each hierarchical classes and to each set of information data based on at least one recognizable feature of the information data to be exchanged;

perceptually recognizing at least one of the sets of information data dependent on user provided value-added information data;

enabling a trusted transaction of the information data based on verification of means of payment, and associated access, governing at least one copy of the information data sought;

associating the transaction event with the information data prior to transmission of the information data; and

transmitting and confirming delivery of the information data

127. The method of claim 126, further comprising the step of grouping the class of data by at least one of quality, price, and service.

128. The method of claim 127, wherein the grouping is determined by at least one of a buyer and a seller.

129. The method of claim 127, wherein the grouping enables greater exchange of information.

130. The method of claim 126, further comprising the step of:

confirming both a digital and an analog copy of the transmission.

131. The method of claim 127, further comprising the step of:

associating the transaction event with the buyer or seller to develop trust with other party

132. The method of claim 126, further comprising the step of:

charging at least one party based on a transaction bandwidth requirement.

133. A device for conducting a trusted transaction between at least two parties who have agreed to transact, comprising:

means for uniquely identifying unique identification information selected from the group consisting of a unique identification of one of the parties, a unique

identification of the transaction, a unique identification of value-added information to be transacted, and a unique identification of a value-adding component;

a steganographic cipher; and

means for verifying an agreement to transact between the parties.

134. The device of claim 133, wherein the unique identification information seeds the steganographic cipher.

135. The device of claim 133, wherein the unique identification information is verifiable.

136. The device of claim 133, further comprising:

means for transmitting value-added information.

137. The device of claim 136, wherein the means for transmitting value-added information transmits the value-added information by a method selected from the group consisting of electrical and physical.

138. The device of claim 136, wherein the wherein the means for transmitting value-added information transmits the value-added information in a medium selected from the group consisting of a pre-determined file format and a predetermined carrier medium.

139. A device for conducting a trusted transaction between at least two parties who have agreed to transact, comprising:

means for uniquely identifying unique identification information selected from the group consisting of a unique identification of one of the parties, a unique identification of the transaction, a unique identification of value-added information to be transacted, and a unique identification of a value-adding component; and

means for enabling a subsequent mutually agreed to at least one term.

140. The method of claim 139, wherein the at least one subsequent term concerns at least one of equity, service, and recognition.

141. A device for conducting trusted transactions between at least two parties, comprising:

a steganographic cipher;

a controller for receiving input data or outputting output data; and

at least one input/output connection,

wherein the device has a unique identification code.

142. The device of claim 141, wherein the unique identification code is predetermined.

143. The device of claim 141, wherein the unique identification code is upgradeable.

144. The device of claim 141, wherein the steganographic cipher comprises:

a number generator selected from the group consisting of a pseudo-random number generator and a random number generator;

a predetermined key generation algorithm selected from the group consisting of a hash function and a special one-way function;

a predetermined message information selected from the group consisting of a digital signature, a time stamp, a digital watermark, and function-dependent data;

a predetermination of the information carrier signals characteristics selected from the group consisting of a perceptual characteristic and a signal feature.

145. The device of claim 141, wherein the steganographic cipher manipulates the input data.

146. The device of claim 141, wherein the steganographic cipher manipulates the output data

147. The device of claim 141, wherein the input of input data is controlled by predetermined information selected from the group consisting of a pass phrase, a password, biometric data, and a personal entropy query.

148. The device of claim 144, wherein an identification of a device holder requires at least one additional iteration of verification by at least one of a pass phrase, a password, biometric data, and a personal entropy query.

149. The device of claim 141, wherein the device converts at least one value-added information metrics selected from the group consisting of a price, a selection, and a service into humanly perceptible information.

150. The device of claim 149, wherein the humanly perceptible information relates to at least one of a present value cost to the party, at least one term for use, a level of confidence over the transaction, a level of confidence over transmission security, and a data integrity metric of the value-added information.

151. The device of claim 141, wherein the device is manufactured as a device selected from the group consisting of a smart card, a microchip, and a software application.

152. The device of claim 151, wherein the manufactured device is tamper-resistant.

153. The device of claim 151, wherein the manufactured device ceases to function if at least one function of the manufactured device is altered by an unauthorized party.

154. The device of claim 151, wherein the software application is subject to a steganographic cipher for serialization or creating unique instances of individual copies of the application.

155. The device of claim 141, further comprising an analog to digital converter.

156. The device of claim 141, wherein the device is securely linked to at least one of a means for payment and a transmission channel for private key exchange and approval.

157. The device of claim 156, wherein the key approval is selected from the group consisting of identification, authentication, and authorization.

158. The device of claim 141, wherein the device transacts according to at least one predetermination of at least an identity of the vendor, a plurality of conditions of the information transfer, a payment, and an identity of a separate but similar device.

159. The device of claim 141, wherein the device further comprises:

an internal memory.

160. A trusted transaction device for transmitting authentic value-added information data between at least two parties, comprising:

a display;

a unique identifier;

means for ciphering information input and output;

means for interacting with other similarly functional devices; and

means for storing or retrieving value-added information and a value-adding component.

161. The device of claim 160, wherein the display transceives cryptographically verifiable information.

162. The device of claim 161, wherein the cryptographically verifiable information is observed by a user.

163. The device of claim 160, wherein the unique identifier is upgradeable.

164. The device of claim 160, wherein the unique identifier is serialized.

165. The device of claim 160, wherein the unique identifier comprises at least one of a means for facilitating transaction authorization, a means for facilitating bandwidth requirements, and a means for associating the unique identifier with information.

166. The device of claim 160, wherein the means for ciphering information comprises at least one of a means for facilitating transaction authorization, a means for facilitating bandwidth requirements, and a means for associating the unique identifier with information.

167. The device of claim 160, further comprising:

a means for establishing communications/connecting with other similarly outfitted devices;

a means for storing or retrieving trusted transaction value-adding component data; and

a means for attaching storage or transducers to the device.

168. The device of claim 167, further comprising:

means for anonymous tracing of the transaction.

169. The device of claim 167, wherein information is processed in real time.

170. A device for securely exchanging information data, comprising:

means for creating a private key by the party seeking predetermined data;

means for deriving a corresponding public key based on the predetermined data and at least one of verifiable data associated with different versions of the information, verifiable data associated with a transmitting device, and verifiable data associated with the identity of the party seeking information;

means for creating a set of one-time signatures relating to the predetermined data;

means for validating a predetermined hierarchy of access of the set of one-time signatures;

means for creating a public key signature, verifiable with the public key, including the access hierarchy of one time signatures;

means for securely transacting predetermined data by providing information relating to a proposed transaction; and

means for verifying the one time signature and the hierarchy of access to enable transfer of predetermined data.

171. The device of claim 170, further comprising

a means for interacting with other equipped devices.

172. The device of claim 171, further comprising:

means for establishing a secure transmission.

173. A system for the secure exchange of predetermined, verifiable information data between at least two parties, comprising:

at least one condition for the use of the information;

means for differentiating between predetermined information and other seemingly identical information based on an authentication protocol;

means for associating authenticity of verifiable information data with at least one condition for use;

a storage unit for storing the predetermined, verifiable information; and

means for communicating with the predetermined, verifiable information storage.

174. The system of claim 173, wherein the means for differentiating between predetermined information and the seemingly identical information based on an authentication protocol comprises at least one of a hash, a signature, and a secure watermark.

175. The system of claim 173, further comprising:

means for authenticating verifiable information flow between transacting parties.

176. The system of claim 173, wherein the system securely exchanges predetermined, verifiable information data prior to consummating verifiable financial transaction between the parties.

177. A system for the exchange of information, comprising:

at least one sender;

at least a receiver;

a verifiable message; and

a verification of the message by at least one of the senders and the receivers; wherein a verification of the message enables a decision over receiving additional related information.

178. A system for computer based decision protocol comprising:

a means for identifying between structured and unstructured information;

a means for authenticating structured information; and

a means for enabling a decision rule based on the identity and authenticity of the information.

179. The system of claim 178, further comprising:

a means for comparing decision results with at least one predetermined rule.

180. A system for computer-based decision protocol, comprising:

means for identifying between structured and unstructured information;

means for identifying structured information; and

means for enabling a predetermined decision rule based on the identity of the information.

181. The system of claim 180, wherein the structured information is defined by at least one of a digital signal processor and a general purpose computing device.

182. The system of claim 180, wherein the structured information comprises binary data.

183. The system of claim 180, wherein the structured information is humanly perceptible.

184. The system of claim 180, wherein the structured information is defined in a bit addressable manner.

185. The system of claim 180, wherein the structured information has at least one mathematically definable characteristic.

186. The system of claim 180, wherein the structured information is selected from the group consisting of pseudo-random and random.

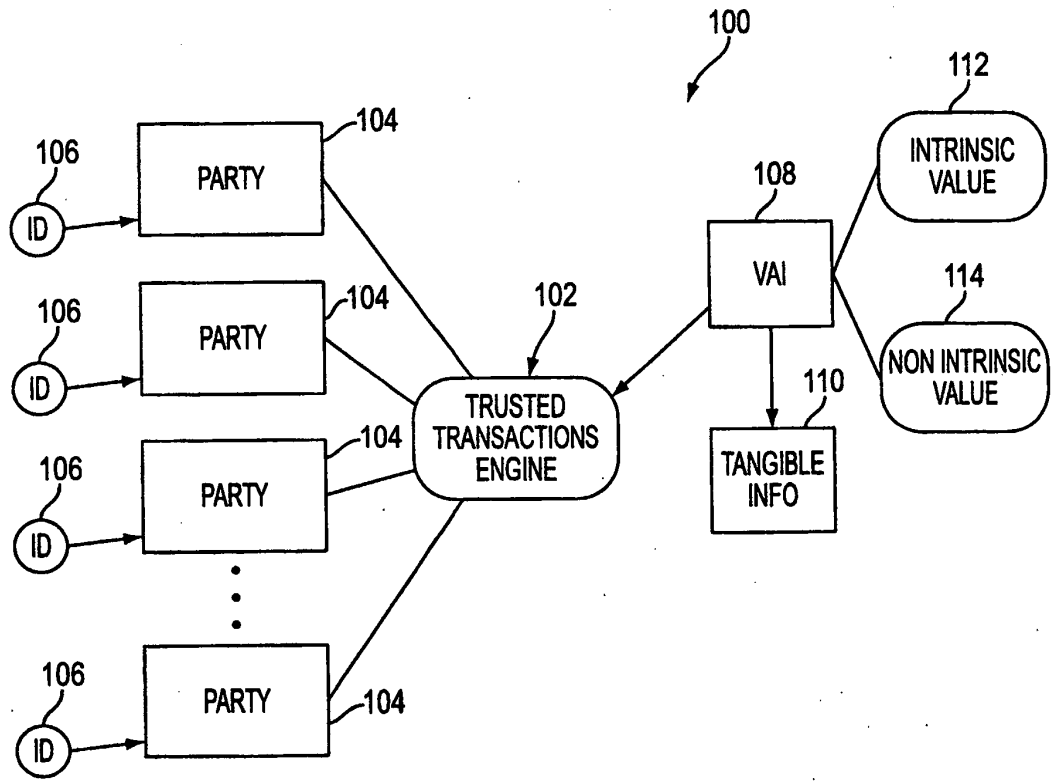

100
112
INTRINSIC VALUE
106
ID
PARTY
104
108
VAI
114
NON INTRINSIC VALUE
102
TRUSTED TRANSACTIONS ENGINE
110
TANGIBLE INFO

FIG. 1

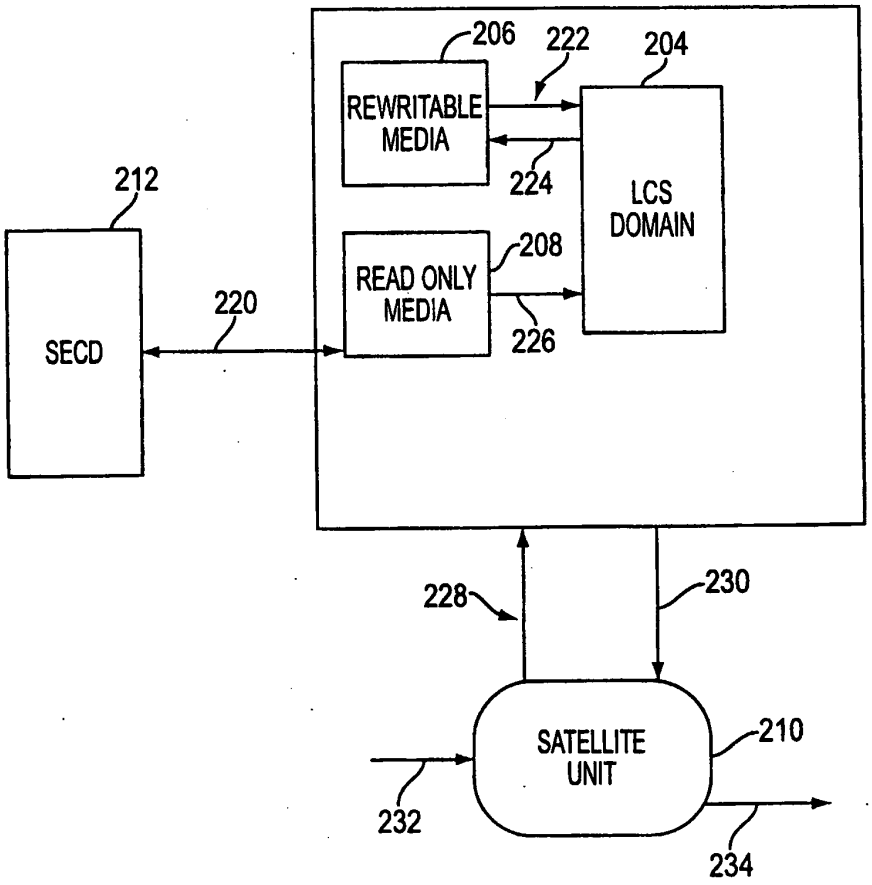

206
222
204
REWRITABLE MEDIA
224
LCS DOMAIN
212
208
READ ONLY MEDIA
220
SECD
226
228
230
SATELLITE UNIT
210
232
234

FIG. 2

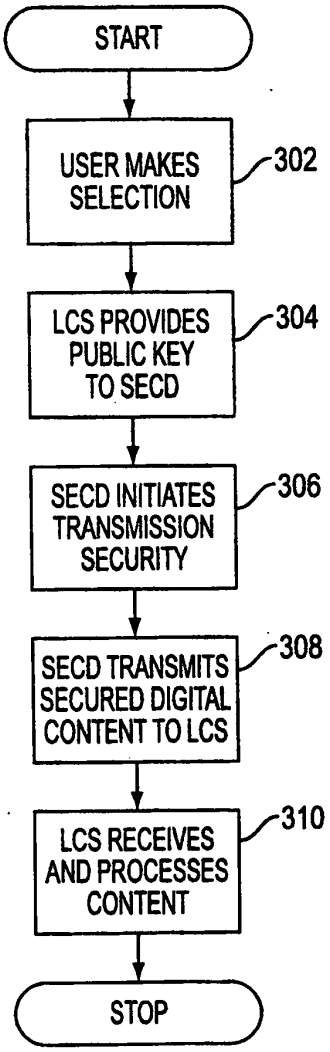

START
USER MAKES SELECTION
302
LCS PROVIDES PUBLIC KEY TO SECD
304
SECD INITIATES TRANSMISSION SECURITY
306
SECD TRANSMITS SECURED DIGITAL CONTENT TO LCS
308
LCS RECEIVES AND PROCESSES CONTENT
310
STOP

FIG. 3

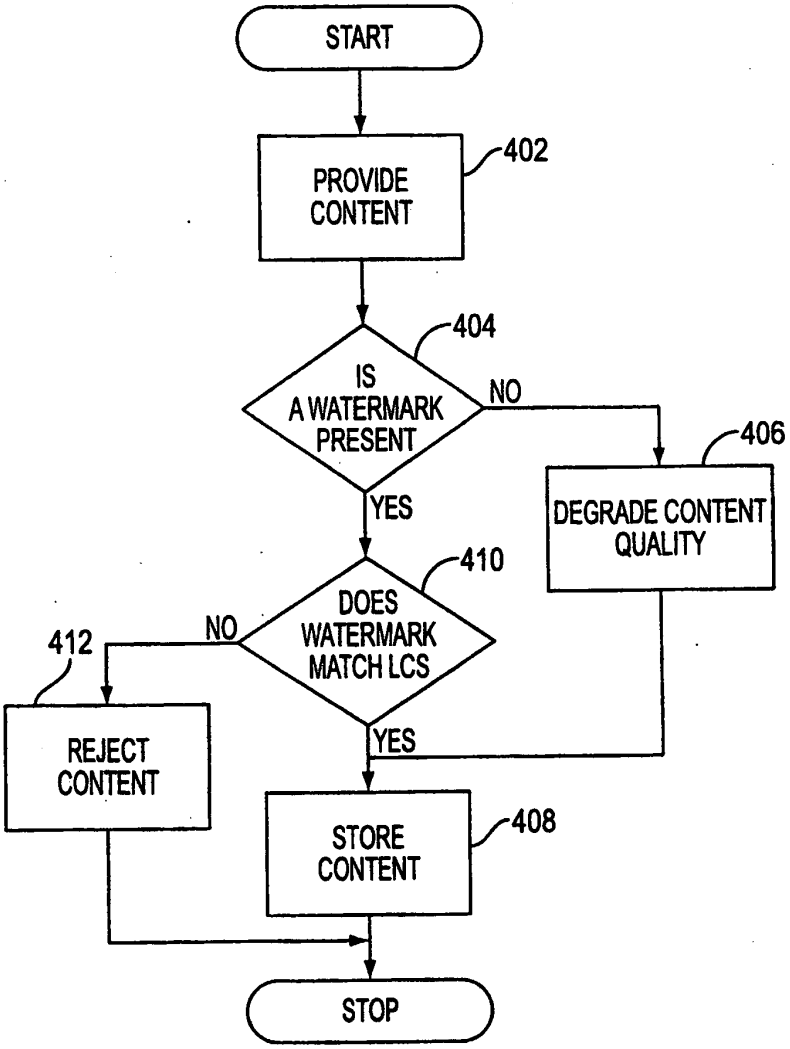

START
PROVIDE CONTENT
402
IS A WATERMARK PRESENT
404
NO
406
DEGRADE CONTENT QUALITY
YES
DOES WATERMARK MATCH LCS
410
NO
412
REJECT CONTENT
YES
STORE CONTENT
408
STOP

FIG. 4

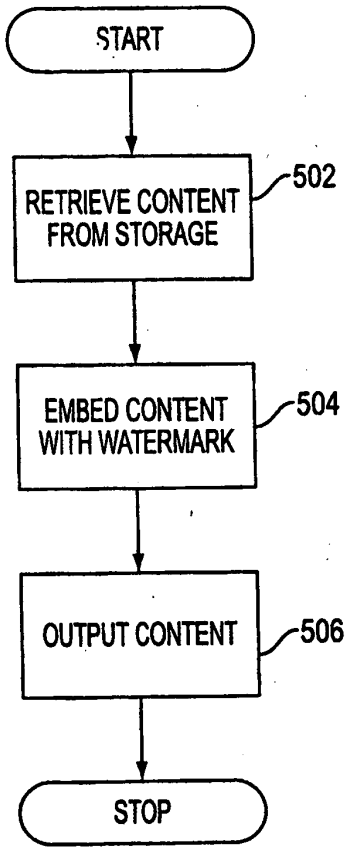

START
RETRIEVE CONTENT FROM STORAGE
502
EMBED CONTENT WITH WATERMARK
504
OUTPUT CONTENT
506
STOP

FIG. 5

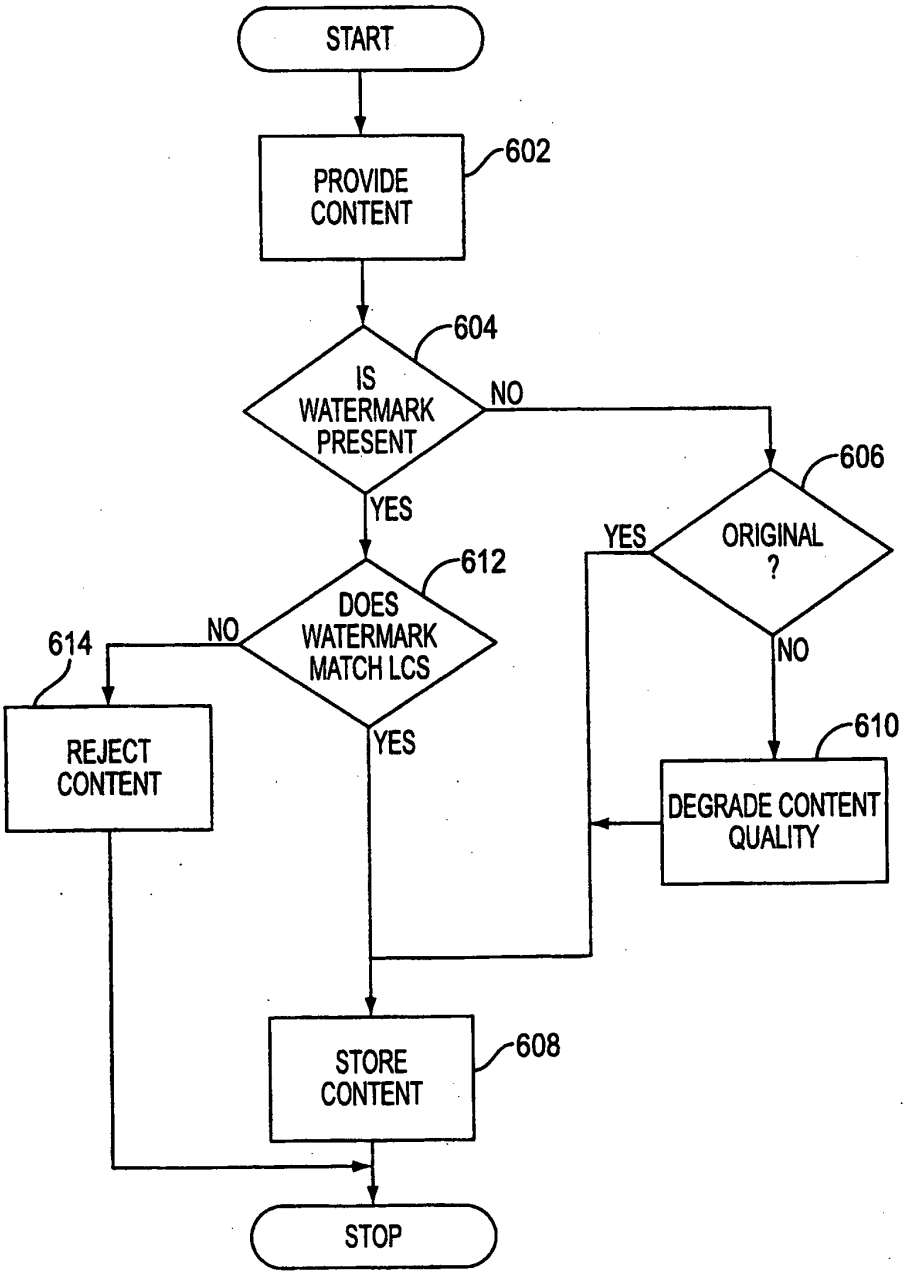

START
PROVIDE CONTENT
602
IS WATERMARK PRESENT
604
NO
YES
ORIGINAL ?
606
YES
NO
DOES WATERMARK MATCH LCS
612
NO
614
YES
REJECT CONTENT
DEGRADE CONTENT QUALITY
610
STORE CONTENT
608
STOP

FIG. 6

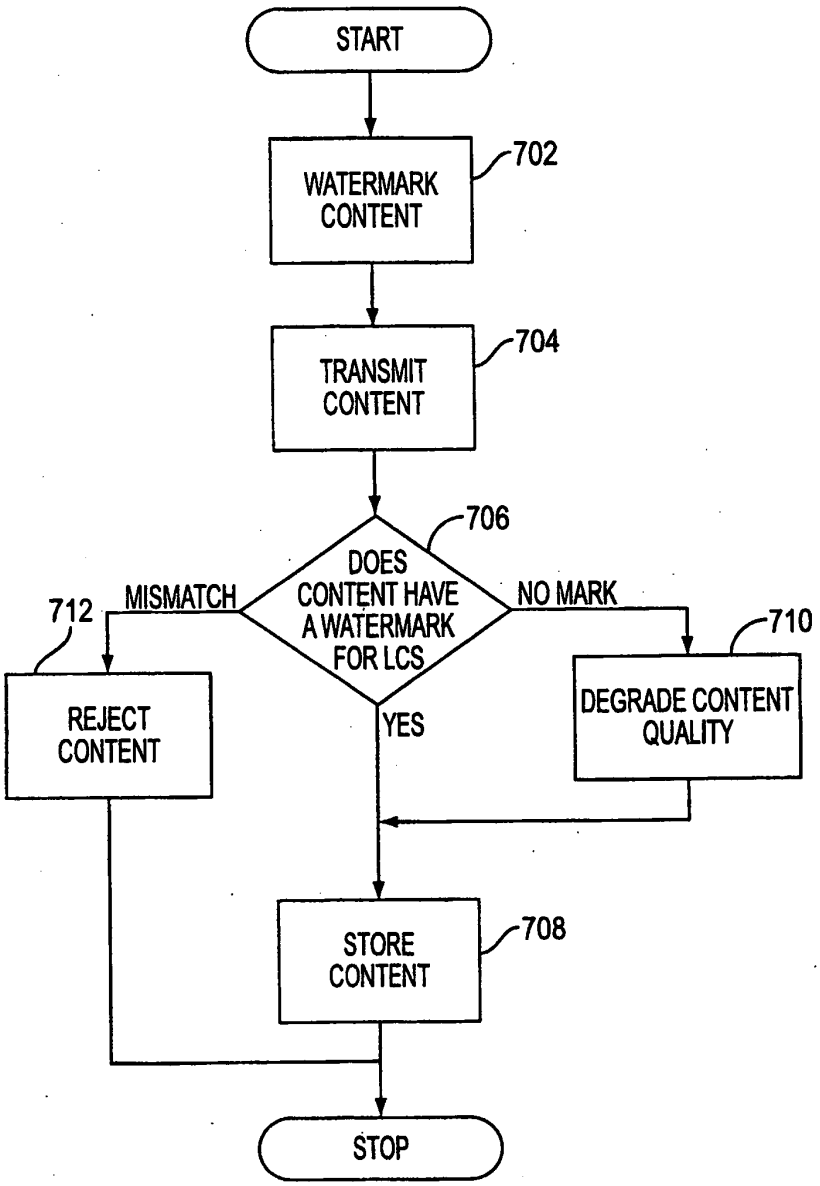

START
WATERMARK CONTENT
702
TRANSMIT CONTENT
704
706
DOES CONTENT HAVE A WATERMARK FOR LCS
MISMATCH
NO MARK
YES
712
REJECT CONTENT
710
DEGRADE CONTENT QUALITY
STORE CONTENT
708
STOP

FIG. 7

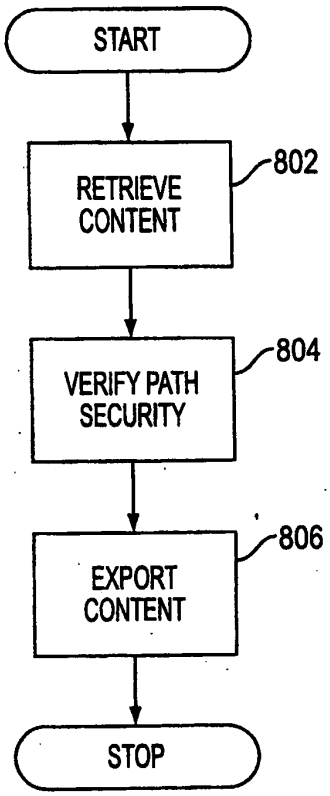

START
RETRIEVE CONTENT
802
VERIFY PATH SECURITY
804
EXPORT CONTENT
806
STOP

FIG. 8

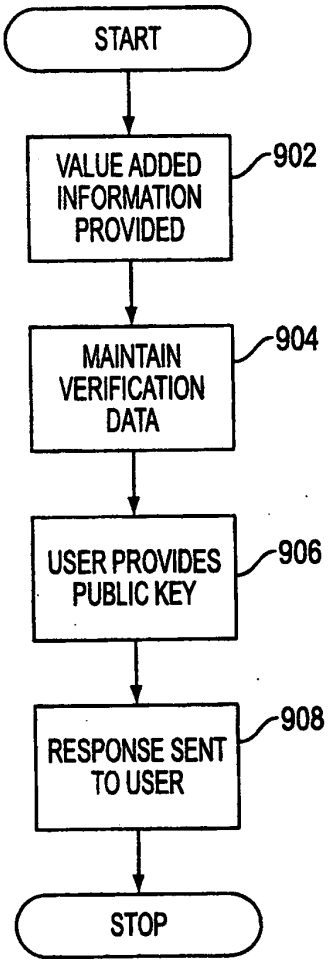

START
VALUE ADDED INFORMATION PROVIDED
902
MAINTAIN VERIFICATION DATA
904
USER PROVIDES PUBLIC KEY
906
RESPONSE SENT TO USER
908
STOP

FIG. 9

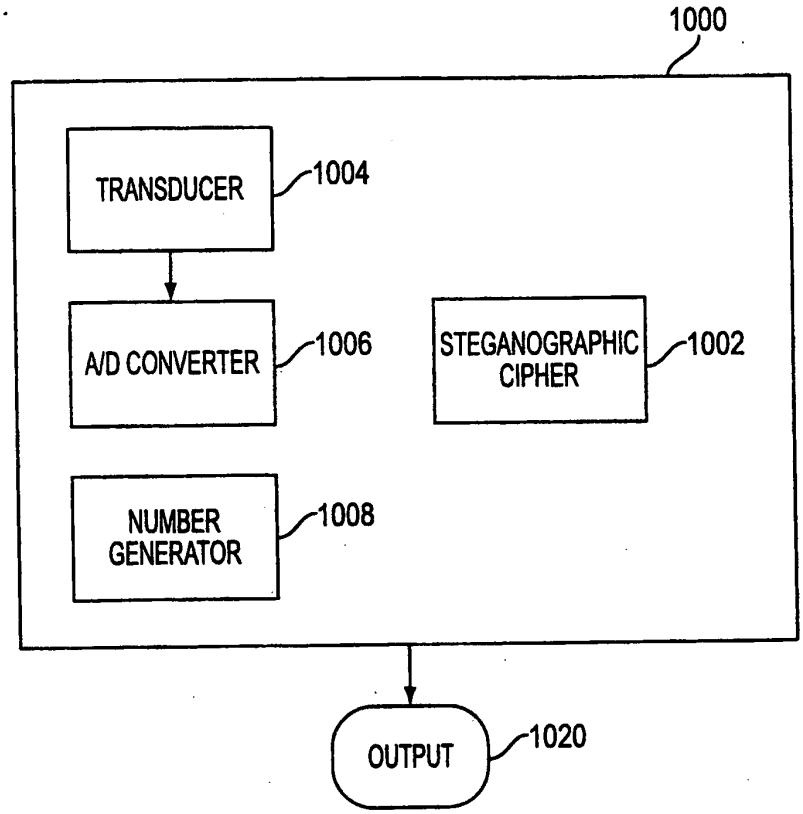

1000
TRANSDUCER
1004
A/D CONVERTER
1006
STEGANOGRAPHIC CIPHER
1002
NUMBER GENERATOR
1008
OUTPUT
1020

FIG. 10

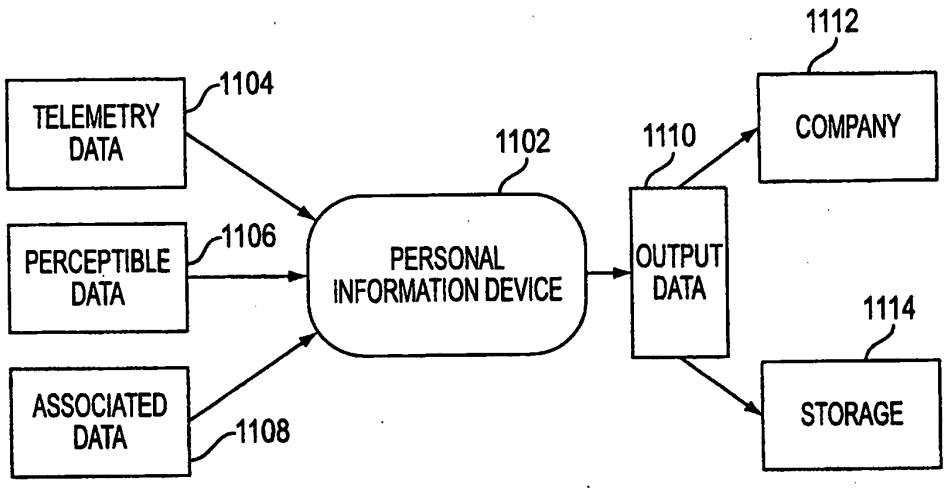

TELEMETRY DATA
1104
PERCEPTIBLE DATA
1106
ASSOCIATED DATA
1108
PERSONAL INFORMATION DEVICE
1102
OUTPUT DATA
1110
COMPANY
1112
STORAGE
1114

FIG. 11

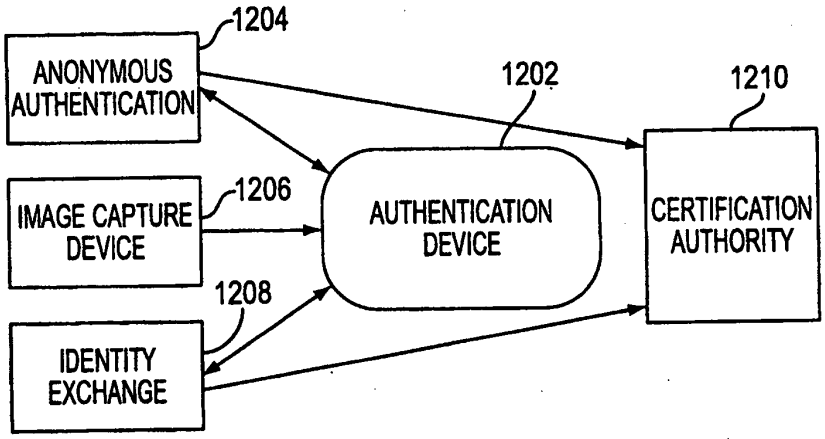

1204
ANONYMOUS AUTHENTICATION
1202
1210
IMAGE CAPTURE DEVICE
1206
AUTHENTICATION DEVICE
CERTIFICATION AUTHORITY
1208
IDENTITY EXCHANGE

FIG. 12

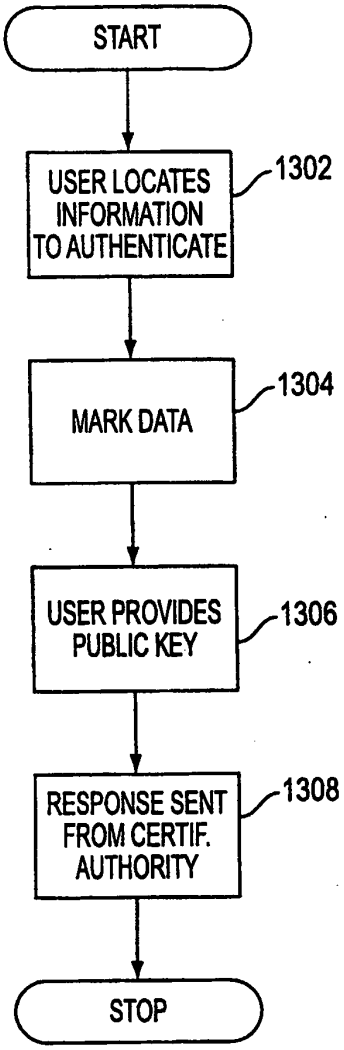

START
USER LOCATES INFORMATION TO AUTHENTICATE
1302
MARK DATA
1304
USER PROVIDES PUBLIC KEY
1306
RESPONSE SENT FROM CERTIF. AUTHORITY
1308
STOP

FIG. 13

INTERNATIONAL SEARCH REPORT

Int onal Application No
PCT/US 00/33126

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 903 721 A (SIXTUS TIMOTHY) 11 May 1999 (1999-05-11) abstract column 3, line 26 -column 5, line 31	1-19
X	US 5 790 677 A (SPELMAN JEFFREY F ET AL) 4 August 1998 (1998-08-04) abstract column 2, line 6 -column 4, line 39	1-19
X	WO 96 29795 A (MICALI SILVIO) 26 September 1996 (1996-09-26) abstract page 5, line 27 -page 8, line 6	1-19

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 March 2001	04.04.01

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Corcoran, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

In onal Application No
PCT/US 00/33126

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 24833 A (MICALI SILVIO) 10 July 1997 (1997-07-10) abstract page 2, line 12 -page 5, line 8	1-19
A	US 5 539 735 A (MOSKOWITZ SCOTT A) 23 July 1996 (1996-07-23) abstract column 1, line 60 -column 4, line 29	1-19
A	SIRBU M ET AL: "NETBILL: AN INTERNET COMMERCE SYSTEM OPTIMIZED FOR NETWORK DELIVERED SERVICES" DIGEST OF PAPERS OF THE COMPUTER SOCIETY COMPUTER CONFERENCE (SPRING) COMPCON,US,LOS ALAMITOS, IEEE COMP. SOC. PRESS, vol. CONF. 40, 5 March 1995 (1995-03-05), pages 20-25, XP000577034 ISBN: 0-7803-2657-1 The whole document	1-19
A	SCHUNTER M ET AL: "A status report on the SEMPER framework for secure electronic commerce" COMPUTER NETWORKS AND ISDN SYSTEMS,NL,NORTH HOLLAND PUBLISHING. AMSTERDAM, vol. 30, no. 16-18, 30 September 1998 (1998-09-30), pages 1501-1510, XP004138681 ISSN: 0169-7552 2. Model for electronic commerce 3. The SEMPER framework	1-19
A	KONRAD K ET AL: "Trust and electronic commerce-more than a technical problem" PROCEEDINGS OF THE 18TH IEEE SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS, PROCEEDINGS 18TH IEEE SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS, LAUSANNE, SWITZERLAND, 19-22 OCT. 1999, pages 360-365, XP002162270 1999, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-7695-0290-3 3. Trust, Security and Electronic Commerce 4. Technology and Institutions	1-19

-/--

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/US 00/33126

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	KINI A ET AL: "Trust in electronic commerce: definition and theoretical considerations" PROCEEDINGS OF THE THIRTY-FIRST HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES (CAT. NO.98TB100216), PROCEEDINGS OF THE THIRTY-FIRST HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, KOHALA COAST, HI, USA, 6-9 JAN. 1998, pages 51-61, XP002162271 1998, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-8186-8255-8 1.3 The Significance of Trust in Electronic Commerce, ---	1-19
A	STEINAUER D D ET AL: "Trust and traceability in electronic commerce" STANDARD VIEW, SEPT. 1997, ACM, USA, vol. 5, no. 3, pages 118-124, XP002162272 ISSN: 1067-9936 The whole document ---	1-19
A	US 5 687 236 A (MOSKOWITZ SCOTT A ET AL) 11 November 1997 (1997-11-11) abstract ---	8,9
A	US 5 745 569 A (MOSKOWITZ SCOTT A ET AL) 28 April 1998 (1998-04-28) abstract -----	8,9

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/US 00/33126

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5903721 A	11-05-1999	AU 6549498 A	29-09-1998
		DE 1008022 T	25-01-2001
		EP 1008022 A	14-06-2000
		ES 2150892 T	16-12-2000
		NO 994428 A	09-11-1999
		WO 9840809 A	17-09-1998
US 5790677 A	04-08-1998	NONE	
WO 9629795 A	26-09-1996	WO 9806198 A	12-02-1998
		CA 2215908 A	26-09-1996
		EP 0815671 A	07-01-1998
		US 5553145 A	03-09-1996
		US 5629982 A	13-05-1997
		US 5666420 A	09-09-1997
		US 6137884 A	24-10-2000
		US 6141750 A	31-10-2000
		EP 0917781 A	26-05-1999
		JP 2000515649 T	21-11-2000
WO 9724833 A	10-07-1997	US 5615269 A	25-03-1997
		AU 1951497 A	28-07-1997
US 5539735 A	23-07-1996	US 5428606 A	27-06-1995
		WO 9701892 A	16-01-1997
US 5687236 A	11-11-1997	US 5613004 A	18-03-1997
		EP 0872073 A	21-10-1998
		WO 9642151 A	27-12-1996
US 5745569 A	28-04-1998	AU 1829497 A	11-08-1997
		WO 9726732 A	24-07-1997

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 00/33126

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 20-186
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

DISH-Blue Spike-842
Exhibit 1004, Page 1038

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.2

Claims Nos.: 20-186

In view of the large number and also the wording of the claims presently on file, which render it difficult, if not impossible, to determine the matter for which protection is sought, the present application fails to comply with the clarity and conciseness requirements of Article 6 PCT (see also Rule 6.1(a) PCT) to such an extent that a meaningful search is impossible.

Moreover, the proliferation of independent claims and the broad manner in which these have been worded make it impossible to determine which parts of the claims may be said to define subject-matter for which protection might legitimately be sought (Article 6 PCT). For these reasons, a meaningful search over the whole breadth of the claim(s) is impossible.

Consequently, the search has been restricted to the subject matter recited in claims 1-19.

The applicant's attention is drawn to the fact that claims, or parts of claims, relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure.

OIPE IAP84
OCT 19 2007
PATENT & TRADEMARK OFFICE

UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	11/895,388	Confirmation No. 2103
Applicant	:	Scott A. MOSKOWITZ	
Filed	:	August 24, 2007	
TC/A.U.	:	2132	
Examiner	:	NA	
Docket No.	:	80391.0003CONT2	

MAIL STOP AMENDMENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRELIMINARY AMENDMENT

Prior to examination on the merits and prior to calculation of the filing fee, please enter the following amendments to the application.

IN THE CLAIMS:

Claims 6-31 were previously canceled without prejudice or disclaimer. Claims 6-31 were previously subject to a restriction requirement. Applicant reserves the right to pursue the subject matter of the original claims in this application and in other applications. This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (original) A method for copy protection of digital information, the digital information including a digital sample and format information, comprising the steps of:

identifying a portion of the format information to be encoded;

generating encoded format information from the identified portion of the format information; and

generating encoded digital information, including the digital sample and the encoded format information.

2. (original) The method of claim 1, further comprising the step of requiring a predetermined key to decode the encoded format information.

3. (original) The method of claim 2, wherein the digital sample and format information are configured to be used with a digital player, and wherein information output from the digital player will have a degraded quality unless the encoded format information is decoded with the predetermined key.

4. (original) The method of claim 3, wherein the information output from the digital player represents a still image, audio or video.

5. (original) The method of claim 3, wherein the information output represents text data to be authenticated.

Claims 6 – 31 (cancelled without prejudice to Applicant's right to seek allowance of said claims in a related application)

32. (original) A method for copy protection of software comprising: embedding the software with a watermark wherein the embedded software operates in a manner substantially the same as the software prior to the embedding step.

33. (original) The process of claim 32, wherein the step of embedding the software with a watermark increases the complexity of code analysis and/or tampering with the software.

34. (original) The process of claim 32, wherein the watermarked software queries a user for personalization information during installation of the software

35. (original) The process of claim 32, wherein the watermark is accessible with a key.

36. (original) The process of claim 35, wherein the key enables authorized use of the watermarked software.

37. (original) The process according to claim 35, wherein the key and license information are interchangeable.

38. (original) The process according to claim 32, wherein the step of embedding the software with a watermark is performed during execution of the software.

39. (original) The process according to claim 32, wherein the step of embedding the software with a watermark modifies the structure of the software being embedded.

40. (original) An article of manufacture comprising a machine readable medium, having thereon stored instructions adapted to be executed by a processor, which instructions when executed result in a process comprising: receiving potentially watermarked software; and identifying the software by extracting the watermark.

41. (original) The article of manufacture of claim 40, wherein the watermark is associated with information fixed prior to distribution of the watermarked software.

42. (original) The article of manufacture of claim 40, wherein the watermark affects functionality of the watermarked software.

43. (original) The article of manufacture of claim 40, wherein the extracted watermark enables generation of a key.

44. (original) The article of manufacture of claim 43, wherein the generated key and licensing information are associated.

45. (original) The article of manufacture of claim 40, further comprising limiting functionality of the software if the watermark cannot be extracted.

46. (original) A method for watermarking software comprising: determining the structure a plurality of code contained in the software; and configuring at least a portion of the plurality of code according to a watermarking process.

DISH-Blue Spike-842
Exhibit 1004, Page 1042

47. (original) The process of claim 46, wherein the watermarking process further comprises inserting information into the software after installation.

48. (original) The process of claim 46, wherein the watermarking process configures the at least a portion of the plurality of code according to a key.

49. (original) The process of claim 46, wherein the watermarking process increases the complexity of code analysis and/or tampering with the software.

50. (original) The process of claim 46, wherein the watermarking process is selected from the group comprising: data hiding, steganography or steganographic ciphering.

51. (original) The process of claim 46, wherein the watermarking process is applied during execution of the software.

52. (original) A system for copy protection of software comprising the steps of: associating license information with a copy of a software application; encoding the associated license information into the copy of the software application using a watermarking process; providing the copy of the software application having license information encoded therein to a user; and, comparing information received by a user with the encoded license information.

53. (original) The system of claim 52, wherein the encoding is controlled by a key.

54. (original) The system of claim 52, wherein the step of comparing the user supplied information with the encoded license information enables authorization of the software.

55. (original) The system of claim 53, wherein the key is fixed prior to distribution of the software.

56. (original) The system of claim 52, wherein the license information comprises code which affects functionality of the watermarked software.

57. (currently amended) The system of claim 52, wherein the watermarked software is resistant to code analysis and/or tampering.

DISH-Blue Spike-842
Exhibit 1004, Page 1043

REMARKS

Applicant requests entry of the amendments and submits that this application is in condition for allowance, and a notice to this effect is earnestly sought.

Respectfully submitted,

Date: October 17, 2007

By: _____

Scott A. Moskowitz
Tel (305) 956-9041
Fax (305) 956-9042

OIPE IAP64
OCT 19 2007
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	11/895,388	Confirmation No. 2103
Applicant	:	Scott A. MOSKOWITZ	
Filed	:	August 24, 2007	
TC/A.U.	:	2132	
Examiner	:	NA	
Docket No.	:	80391.0003CONT2	

MAIL STOP AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Dear Sir:

Applicant(s) submit copies of the references listed on the attached SB08 Form(s) for consideration and request that the U.S. Patent and Trademark Office make them of record in this application.

Applicant(s) state the following:

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Information Disclosure Statement; or

☐ No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and to the knowledge of Applicant(s) no item of information contained in this

Information Disclosure Statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

☒ In accordance with 37 C.F.R. § 1.97(b), this Information Disclosure Statement is believed to be submitted prior to issuance of a first Office Action and/or within three months of the filing date of the application. It is respectfully submitted that no fee is required for consideration of this information.

☐ This Information Disclosure Statement is being submitted after the mailing of a non-final Office Action, but is believed to be prior to a final Office Action or a Notice of Allowance. Pursuant to 37 C.F.R. § 1.97(c), payment in the amount of $180.00 as set forth in 37 C.F.R. § 1.17(p) is enclosed.

While the information and references disclosed in this Information Disclosure Statement are submitted pursuant to 37 C.F.R. § 1.56, this submission is not intended to constitute an admission that any patent, publication or other information referred to is "prior art" to this invention. Applicant(s) reserve the right to contest the "prior art" status of any information submitted or asserted against the application.

Additionally, pursuant to C.F.R. § 1.78, Applicant(s) wish to inform the Examiner of the existence of the following co-pending U.S. patent applications, patent applications and issued U.S. patents that share a common inventor or applicant with the present application. Under 37 C.F.R. § 1.98(a)(1), Applicant(s) also wish to inform the Examiner of the existence of the following co-pending foreign patents and patent applications that share a common inventor with the present application in the "section separate from the citations of other documents" entitled "Foreign Patent Documents", below:

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

U.S. PATENT DOCUMENTS

EXAMINER'S
INITIALS:

_____ U.S. Patent Application No. 08/999,766, filed July 23, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent Application No. 11/894,443, filed August 21, 2007, entitled "Steganographic Method and Device";

_____ U.S. Patent Application No. 11/894,476, filed August 21, 2007, entitled "Steganographic Method and Device";

_____ U.S. Patent Application No. 11/050,779, filed February 7, 2005, entitled "Steganographic Method and Device" – Publication No. 20050177727 – August 11, 2005;

_____ U.S. Patent Application No. 08/674,726, filed July 2, 1996, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management";

_____ U.S. Patent Application No. 09/545,589, filed April 7, 2000, entitled "Method and System for Digital Watermarking" (issued as U.S. Patent No. 7,007,166);

_____ U.S. Patent Application No. 11/244,213, filed October 5, 2005, entitled "Method and System for Digital Watermarking" – Publication No. 20060101269 – May 11, 2006;

_____ U.S. Patent Application No. 11/649,026, filed January 3, 2007, entitled "Method and System for Digital Watermarking" – Publication No. 20070113094 – May 17, 2007;

_____ U.S. Patent Application No. 09/046,627, filed March 24, 1998, entitled "Method for Combining Transfer Function with Predetermined Key Creation" (issued as U.S. Patent No. 6,598,162);

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ U.S. Patent Application 10/602,777, filed June 25, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation" – Publication No. 20040086119 – May 6, 2004;

_____ U.S. Patent Application 11/895,388, filed August 24, 2007, entitled "Data Protection Method and Device";

_____ U.S. Patent Application No. 09/053,628, filed April 2, 1998, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" (issued as U.S. Patent No. 6,205,249);

_____ U.S. Patent Application No. 09/644,098, filed August 23, 2000, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" (issued as U.S. Patent No. 7,035,409);

_____ U.S. Patent Application No. 09/767,733, filed January 24, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" – Publication No. 20010010078 - July 26, 2001;

_____ U.S. Patent Application No. 11/358,874, filed February 21, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" -- Publication No. 20060140403 – June 29, 2006;

_____ U.S. Patent Application No. 10/417,231, filed April 17, 2003, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth" – Publication No. 20030200439 – October 23, 2003;

_____ U.S. Patent Application No. 11/900,065, filed September 10, 2007, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth";

_____ U.S. Patent Application No. 11/900,066, filed September 10, 2007, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth";

_____ U.S. Patent Application No. 09/789,711, filed February 22, 2001, entitled "Optimization Methods for the Insertion, Protection, and Detection of

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

Digital Watermarks in Digital Data" – Publication No. 20010010078 - October 11, 2001 (issued as U.S. Patent No. 7,107,451);

_____ U.S. Patent Application No. 11/497,822, filed August 2, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070011458 – January 11, 2007;

_____ U.S. Patent Application No. 11/599,964, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent Application No. 11/599,838, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070226506 – September 27, 2007;

_____ U.S. Patent Application No. 11/897,790, filed August 31, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent Application No. 11/897,791, filed August 31, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent Application No. 11/899,661, filed September 7, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent Application No. 11/899,662, filed September 7, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent Application No. 10/369,344, filed February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data" – Publication No. 20030219143 – November 27, 2003 (issued as U.S. Patent No. 7,095,874);

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ U.S. Patent Application No. 11/482,654, filed July 7, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data" -- Publication No. 20060285722 – December 21, 2006;

_____ U.S. Patent Application No. 09/594,719, filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems" (issued as U.S. Patent 7,123,718);

_____ U.S. Patent Application No. 11/519,467, filed September 12, 2006, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems" -- Publication No. 20070064940 – March 22, 2007;

_____ U.S. Patent Application No 09/731,040, filed December 7, 2000, entitled "Systems, Methods And Devices For Trusted Transactions" -- Publication No. 20020010684 – January 24, 2002 (issued as U.S. Patent 7,159,116);

_____ U.S. Patent Application No 11/512,701, filed August 29, 2006, entitled "Systems, Methods And Devices For Trusted Transactions" -- Publication No. 20070028113 – February 1, 2007;

_____ U.S. Patent Application No. 10/049,101, filed February 8, 2002, entitled "A Secure Personal Content Server" (which claims priority to International Application No. PCT/US00/21189, filed August 4, 2000, which claims priority to U.S. Patent Application No. 60/147,134, filed August 4, 1999, and to U.S. Patent Application No. 60/213,489, filed June 23, 2000);

_____ U.S. Patent Application No. 09/657,181, filed September 7, 2000, entitled "Method And Device For Monitoring And Analyzing Signals";

_____ U.S. Patent Application No. 10/805,484, filed March 22, 2004, entitled "Method And Device For Monitoring And Analyzing Signals"(which claims priority to U.S. Patent Application No. 09/671,739, filed September 29, 2000, which is a CIP of U.S. Patent Application No. 09/657,181) -- Publication No. 20040243540 – December 2, 2004;

_____ U.S. Patent Application No. 09/956,262, filed September 20, 2001, entitled "Improved Security Based on Subliminal and Supraliminal

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

Channels For Data Objects" -- Publication No. 20020056041 – May 9, 2002 (issued as U.S. Patent No. 7,127,615);

_____ U.S. Patent Application No. 11/518,806, filed September 11, 2006, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects";

_____ U.S. Patent Application No. 11/026,234, filed December 30, 2004, entitled "Z-Transform Implementation of Digital Watermarks" -- Publication No. 20050135615 – June 23, 2005 (issued as U.S. Patent No. 7,152,162);

_____ U.S. Patent Application No. 11/592,079, filed November 2, 2006, entitled "Linear Predictive Coding Implementation of Digital Watermarks" -- Publication No. 20070079131 – April 5, 2007;

_____ U.S. Patent Application No. 09/731,039, filed December 7, 2000, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects" -- Publication No. 20020071556 – June 13, 2002 (issued as U.S. Patent No. 7,177,429);

_____ U.S. Patent Application No. 11/647,861, filed December 29, 2006, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects" -- Publication No. 20070110240 – April 5, 2007;

_____ U.S. Patent No. 5,428,606, issued June 27, 1995, entitled "Digital Commodities Exchange";

_____ U.S. Patent No. 5,539,735, issued July 23, 1996, entitled "Digital Information Commodities Exchange";

_____ U.S. Patent No. 5,613,004, issued March 18, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent No. 5,687,236, issued November 11, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent No. 5,745,569, issued April 28, 1998, entitled "Method for Stega-Protection of Computer Code";

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ U.S. Patent No. 5,822,432, issued October 13, 1998, entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System";

_____ U.S. Patent No. 5,889,868, issued July 2, 1996, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 5,905,800, issued May 18, 1999, entitled "Method & System for Digital Watermarking";

_____ U.S. Patent No. 6,078,664, issued June 20, 2000, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 6,205,249, issued March 20, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

_____ U.S. Patent No. 6,522,767, issued February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 6,598,162, issued July 22, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation";

_____ U.S. Patent No. 6,853,726, issued February 8, 2005, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 7,007,166, issued February 28, 2006, entitled "Method & System for Digital Watermarking";

_____ U.S. Patent No. 7,035,049, issued April 25, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

_____ U.S. Patent No. 7,095,874, issued August 22, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 7,107,451, issued September 12, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ U.S. Patent No. 7,123,718, issued October 17, 2006, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems";

_____ U.S. Patent No. 7,127,615, issued October 24, 2006, "Improved Security Based on Subliminal and Supraliminal Channels for Data Objects";

_____ U.S. Patent No. 7,152,162, issued December 19, 2006, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 7,159,116, issued January 2, 2007, entitled "Systems, Methods and Devices for Trusted Transactions";

_____ U.S. Patent No. 7,177,429, issued February 13, 2007, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects"

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

FOREIGN PATENT DOCUMENTS

EXAMINER'S
INITIALS:

_____ PCT Application No. PCT/US95/08159, filed June 26, 1995, entitled, "Digital Information Commodities Exchange with Virtual Menuing";

_____ PCT Application No. PCT/US96/10257, filed June 7, 1996, entitled, "Steganographic Method and Device" -- corresponding to -- EPO Application No. 96919405.9, entitled "Steganographic Method and Device";

_____ PCT Application No. PCT/US97/00651, filed January 16, 1997, entitled, "Method for Stega-Cipher Protection of Computer Code" – corresponding to AU199718294A (not available);

_____ PCT Application No. PCT/US97/00652, filed January 17, 1997, entitled, "Method for an Encrypted Digital Watermark" – corresponding to AU199718295A (not available);

_____ PCT Application No. PCT/US97/11455, filed July 2, 1997, entitled, "Optimization Methods for the Insertion, Protection and Detection of Digital Watermarks in Digitized Data" – corresponding to AU199735881A (not available);

_____ PCT Application No. PCT/US99/07262, filed April 2, 1999, entitled, "Multiple Transform Utilization and Applications for Secure Digital Watermarking" – corresponding to – Japan App. No. 2000-542907, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" (included herein);

_____ PCT Application No. PCT/US00/06522, filed March 14, 2000, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems";

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ PCT Application No. PCT/US00/18411, filed July 5, 2000, entitled, "Copy Protection of Digital Data Combining Steganographic and Cryptographic Techniques" – corresponding to AU200060709A5 (not available);

_____ PCT Application No. PCT/US00/21189, filed August 4, 2000, entitled, "A Secure Personal Content Server";

_____ PCT Application No. PCT/US00/33126, filed December 7, 2000, entitled, "Systems, Methods and Devices for Trusted Transactions" – corresponding to AU200120659A5 (not available);

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. This Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed documents and information.

Respectfully submitted,

Date: October 17, 2007

By:

Scott A. Moskowitz
Tel# (305) 956-9041
Fax# (305) 956-9042

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

PTO/SB/08B (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

OCT 19 2007 PATENT & TRADEMARK OFFICE

Sheet 1 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		PCT International Search Report, completed Sept. 13, 1995; authorized officer Huy D. Vu (PCT/US95/08159) (2 pages)	
		PCT International Search Report, completed June 11, 1996; authorized officer Salvatore Cangialosi (PCT/US96/10257) (4 pages)	
		Supplementary European Search Report, completed Mar. 5, 2004; authorized officer J. Hazel (EP 96 91 9405) (1 page)	
		PCT International Search Report, completed April 4, 1997; authorized officer Bernarr Earl Gregory (PCT/US97/00651) (1 page)	
		PCT International Search Report, completed May 6, 1997; authorized officer Salvatore Cangialosi (PCT/US97/00652) (3 pages)	
		PCT International Search Report, completed Oct. 23, 1997; authorized officer David Cain (PCT/US97/11455) (1 page)	
		PCT International Search Report, completed July 12, 1999; authorized officer R. Hubeau (PCT/US99/07262) (3 pages)	
		PCT International Search Report, completed June 30, 2000; authorized officer Paul E. Callahan (PCT/US00/06522) (7 pages)	
		Supplementary European Search Report, completed June 27, 2002; authorized officer M. Schoeyer (EP 00 91 9398) (1 page)	
		PCT International Search Report, date of mailing Mar. 15, 2001; authorized officer Marja Brouwers (PCT/US00/18411) (5 pages)	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		PCT International Search Report, completed July 20, 2001; authorized officer A. Sigolo (PCT/US00/18411) (5 pages)	
		PCT International Search Report, completed March 20, 2001; authorized officer P. Corcoran (PCT/US00/33126) (6 pages)	
		PCT International Search Report, completed January 26, 2001; authorized officer Gilberto Barron (PCT/US00/21189) (3 pages)	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Schneier, Bruce, Applied Cryptography, 2nd Ed., John Wiley & Sons, pp. 9-10, 1996	
		Menezes, Alfred J., Handbook of Applied Crypography, CRC Press, p. 46, 1997	
		Merriam-Webster's Collegiate Dictionary, 10th Ed., Merriam Webster, Inc., p.207	
		Brealy, et al., Principles of Corporate Finance, "Appendix A-Using Option Valuation Models", 1984, pp. 448-449	
		Copeland, et al., Real Options:A Practioner's Guide, 2001 pp. 106-107, 201-202, 204-208.	
		Sarkar, M. "An Assessment of Pricing Mechanisms for the Internet-A Regulatory Imperative", presented MIT Workshop on Internet Economics, Mar. 1995 http://www.press.vmich.edu/iep/works/SarkAsses.html on	
		Crawford, D.W. "Pricing Network Usage:A Market for Bandwith of Market Communication?" presented MIT Workshop on Internet Economics, Mar. 1995 http://www.press.vmich.edu/iep/works/CrawMarket.html on March	
		LOW, S.H., "Equilibrium Allocation and Pricing of Variable Resources Among User-Suppliers", 1988. http://www.citesear.nj.nec.com/366503.html	
		Caronni, Germano, "Assuring Ownership Rights for Digital Images", published proceeds of reliable IT systems, v15 '95, H.H. Bruggemann and W. Gerhardt-Hackel (Ed.) Viewing Publishing Company, Germany, 1995	
		Zhao, Jian. "A WWW Service to Embed and Prove Digital Copyright Watermarks", Proc. of the european conf. on Mulitmedia Applications, Services & Techinques Louvain-La-Neuve, Belgium, May 1996	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Gruhl,Daniel et al.,Echo Hiding. In Proceeding of the Workshop on Information Hiding. No. 1174 in Lecture Notes in Computer Science,Cambridge,England (May/June 1996)	
		Oomen,A.W.J. et al., A Variable Bit Rate Buried Data Channel for Compact Disc, J.Audio Eng.Sc.,Vol.43,No.1/2,pp. 23-28 (1995).	
		Ten Kate,W. et al., A New Surround-Stereo-Surround Coding Techniques, J. Audio Eng.Soc.,Vol. 40,No. 5,pp. 376-383 (1992)	
		Gerzon, Michael et al., A High Rate Buried Data Channel for Audio CD, presentation notes, Audio Engineering Soc. 94th Convention (1993).	
		Sklar,Bernard, Digital Communications, pp. 601-603 (1988)	
		Jayant, N.S. et al., Digital Coding of Waveforms, Prentice Hall Inc., Englewood Cliffs,NJ, pp. 486-509 (1984)	
		Bender, Walter R. et al., Techniques for Data Hiding, SPIE Int. Soc. Opt. Eng., Vol. 2420, pp. 164-173, 1995.	
		Zhao, Jian et al., Embedding Robust Labels into Images for Copyright Protection, (xp 000571976), pp. 242-251, 1995.	
		Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, p. 175, 1997.	
		Schneier, Bruce, Applied Cryptography, 1st Ed., pp. 67-68, 1994.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		ten Kate, W. et al., "Digital Audio Carrying Extra Information", IEEE, CH 2847-2/90/0000-1097, (1990)	
		van Schyndel, et al. A digital Watermark, IEEE Int'l Computer Processing Conference, Austin,TX, Nov 13-16, 1994, pp. 86-90	
		Smith, et al. Modulation and Information Hiding in Images, Springer Verlag, 1st Int'l Workshop, Cambridge, UK, May 30-June 1,1996, pp. 207-227	
		Kutter, Martin et al., Digital Signature of Color Images Using Amplitude Modulation, SPIE-E197, vol. 3022, pp. 518-527	
		Puate, Joan et al., Using Fractal Compression Scheme to Embed a Digital Signature into an Image, SPIE-96 Proceedings, vol. 2915, Mar. 1997, pp. 108-118	
		Swanson, Mitchell D.,et al., Transparent Robust Image Watermarking, Proc. of the 1996 IEEE Int'l Conf. on Image Processing, Vol. 111, 1996 , pp. 211-214	
		Swanson, Mitchell D., et al. Robust Data Hiding for Images, 7th IEEE Digital Signal Processing Workshop, Leon, Norway. Sept. 1-4,1996, pp. 37-40	
		Zhao, Jian et al., Embedding Robust Labels into Images for Copyright Protection, Proceeding of the Know Right '95 Conference, pp. 242-251.	
		Koch, E., et al., Towards Robust and Hidden Image Copyright Labeling, 1995 IEEE Workshop on Nonlinear Signal and Image Processing, Jun. 1995 Neos Marmaras, pp. 4	
		Van Schyandel, et al., Towards a Robust Digital Watermark, Second Asain Image Processing Conference, Dec. 6-8,1995,Singapore, Vol. 2,pp. 504-508	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 6 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Tirkel,A.Z., A Two-Dimensional Digital Watermark, DICTA '95, Univ. of Queensland, Brisbane, Dec. 5-8,1995, pp. 7	
		Tirkel,A.Z., Image Watermarking-A Spread Spectrum Application, ISSSTA '96, Sept.96, Mainz, German, pp. 6.	
		O'Ruanaidh, et al. Watermarking Digital Images for Copyright Protection, IEEE Proceedings, Vol. 143, No. 4, Aug. 96, pp. 250-256.	
		Cox, et al., Secure Spread Spectrum Watermarking for Multimedia, NEC Research Institude, Techinal Report 95-10, pp. 33	
		Kahn, D., The Code Breakers, The MacMillan Company, 1969, pp. xIII, 81-83,513,515,522-526,863.	
		Boney, et al., Digital Watermarks for Audio Signals, EVSIPCO, 96, pp. 473-480.	
		Dept. of Electrical Engineering, Del Ft University of Technology, Del ft The Netherlands,Cr.C. Langelaar et al.,Copy Protection for Mulitmedia Data based on Labeling Techniques ,July 1996, 9 pp	
		F. Hartung, et al., Digital Watermarking of Raw and Compressed Video, SPIE Vol. 2952, pp. 205-213.	
		Craver, et al., Can Invisible Watermarks Resolve Rightful Ownerships? IBM Research Report, RC 20509 (July 25,1996) 21 pp.	
		Press, et al., Numerical Recipes In C, Cambridge Univ. Press, 1988, pp. 398-417.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 7 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Pohlmann, Ken C., Principles of Digital Audio, 3rd Ed., 1995, pp. 32-37, 40-48,138,147-149,332,333,364, 499-501,508-509,564-571.	
		Pohlmann, Ken C., Principles of Digital Audio, 2nd Ed., 1991, pp. 1-9,19-25,30-33,41-48,54-57,86-107,375-387.	
		Schneier, Bruce, Applied Cryptography, John Wiley & Sons, inc. , New York,1994, pp. 68,69,387-392,1-57,273-275,321-324.	
		Boney, et al., Digital Watermarks for Audio Signals, Proceedings of the International Conf. on Multimedia Computing and Systems, June 17-23,1996,Hiroshima, Japan, 0-8186-7436-9196, pp. 473-480.	
		Johnson, et al., Transform Permuted Watermarking for Copyright Protection of Digital Video, IEEE Globecom 1998, Nov 8-12,1998, New York, New York, Vol. 2,1998, pp. 684-689,(ISBN 0-7803-4985-7)	
		Rivest, et al., "Pay Word and Micromint: Two Simple Micropayment Schemes, "MIT Laboratory for Computer Science, Cambridge, MA, May 7,1996, pp. 1-18	
		Bender, et al., Techniques for Data Hiding, IBM Systems Journal, Vol. 35, Nos 3 & 4,1996,pp. 313-336.	
		Moskowitz, Bandwith as Currency, IEEE Multimedia, Jan-Mar 2003, pp. 14-21.	
		Moskowitz, Multimedia Security Technologies for Digital Rights Management, 2006, Academic Press, "Introduction-Digital Rights Management" pp. 3-22	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 8 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Tomsich, et al., "Towards a secure and de-centralized digital watermarking infrastructure for the protection of Intellectual Property", in Electronic Commerce and Web Technologies, Proceedings (ECWEB	
		Moskowitz, "What is Acceptable Quality in the Application of Digital Watermarking: Trade-offs of Security, Robustness and Quality", IEEE Computer Society Proceedings of ITCC 2002 April 10, 2002 pp. 80-84	
		Lemma, et al. "Secure Watermark Embedding through Partial Encryption", International Workshop on Digital Watermarking ("IWDW" 2006). Springer Lecture Notes in Computer Science 2006. (to appear) 13	
		Kocher, et al., "Self Protecting Digital Content", Technical Report from the CRI Content Security Research Initiative, Crytography Research, Inc. 2002-2003. 14 pages.	
		Sirbu, M. et al., "Net Bill: An Internet Commerce System Optimized for Network Delivered Services", Digest of Papers of the Computer Society Computer Conference (Spring). 5 March 1995. pp. 20-25. vol. CONF40.	
		Schunter, M. et al., "A Status Report on the SEMPER framework for Secure Electronic Commerce", Computer Networks and ISDN Systems, 30 Sept 1998 pp. 1501-1510 Vol. 30 No. 16-18 NL North Holland	
		Konrad, K. et al., "Trust and Elecronic Commerce-more than a techinal problem," Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems 19-22 October 1999 pp. 360-365 Lausanne	
		Kini, a. et al., "Trust in Electronic Commerce: Definition and Theoretical Considerations", Proceedings of the 31st Hawaii Int'l Conf on System Sciences (Cat. No. 98TB100216). 6-9 January 1998. pp. 51-61. Los	
		Steinauer D. D., et al., "Trust and Traceability in Electronic Commerce", Standard View, Sept 1997, pp 118-124, vol. 5 No. 3, ACM, USA	
		Hartung, et al. "Multimedia Watermarking Techniques", Proceedings of the IEEE, Special Issue, Identification & Protection of Multimedia Information, pp 1079-1107 July 1999 Vol. 87 No. 7 IEEE	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 9 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Rivest,et al., PayWord and MicroMint: Two simple micropayment schemes, MIT Laboratory for Computer Science, Cambridge, MA 02139, April 27,2001, pp. 1-18.	
		Horowitz, et al., The Art of Electronics, 2nd Ed., 1989, pp.7.	
		Delaigle, J.-F., et al. "Digital Watermarking," Proceedings of the SPIE, vol. 2659, Feb 1, 1996, pp. 99-110 (Abstract).	
		Schneider, M., et al. "Robust Content Based Digital Signature for Image Authentication," Proceedings of the International Conference on Image Processing (IC. Lausanne), Sept. 16-19, 1996, pp. 227-230, IEEE ISBN:	
		Cox, I. J., et al. "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, Vol. 6 No. 12, Dec. 1, 1997, pp. 1673-1686.	
		Wong, Ping Wah. "A Public Key Watermark for Image Verification and Authentication," IEEE International Conference on Image Processing, Vol. 1, Oct. 4-7, 1998, pp. 455-459.	
		Fabien A.P. Petitcolas, Ross J. Anderson and Markkus G. Kuhn, "Attacks on Copyright Marking Systems," LNCS, Vol. 1525, April 14-17, 1998, pp. 218-238, ISBN: 3-540-65386-4	
		Ross Anderson, "Stretching the Limits of Steganography," LNCS, Vol. 1174, May/June 1996, 10 pages, ISBN: 3-540-61996-8.	
		Joseph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", pre-publication, Summer 1997, 4 pages	
		Joseph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", Submitted to Signal Processing, August 21, 1997, 19 pages	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

OIPE IAP
OCT 19 2007
PATENT & TRADEMARK OFFICE

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Numb	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,939,515	07/03/1990	Adelson	
		US-5,161,210	11/03/1992	Druyvesteyn,et.al.	
		US-5,450,490	09/12/1995	Jensen et.al.	
		US-5,530,751	06/25/1996	Morris	
		US-5,579,124	11/26/1996	Aijala et.al	
		US-5,721,788	02/24/1998	Powell et.al.	
		US-5,828,325	10/27/1998	Wolose Wicz et.al.	
		US-5,912,972	06/15/1999	Barton	
		US-5,930,377	07/27/1999	Powell et.al.	
		US-5,583,488	12/10/1996	Sala et.al.	
		US-5,748,783	05/05/1998	Rhoads	
		US-6,330,672	12/11/2001	Shur	
		US-5,243,423	09/07/1993	DeJean et.al.	
		US-5,319,735	06/07/1994	Preuss et.al	
		US-5,113,437	05/12/1992	Best et.al.	
		US-4,876,617	10/24/1989	Best et.al.	
		US-5,379,345	01/03/1995	Greenberg	
		US-5,646,997	07/08/1997	Barton	
		US-4,672,605	06/09/1987	Hustig et.al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		European Patent No. EP0565947A1	10/20/1993	Kuusama, Juha		
		WO 95/14289	05/26/1995	Rhoads, Geoffrey		
		European Patent No. 0581317A2	02/02/1994	Powell, Robert et.al.		
		European Patent No. 0372601A1	06/13/1990	Druyvesteyn, Wm. et.al.		
		W098/37513	08/27/1998	Biggar, Michael et.al.		
		European Patent No. 0651554A	05/03/1995	Eastman Kodak Co.		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,748,668	05/31/1998	Shamir, et.al.	
		US-4,789,928	12/06/1988	Fujisaki	
		US-4,908,873	03/13/1990	Philibert, et.al.	
		US-4,980,782	12/25/1990	Ginkel	
		US-5,073,925	12/17/1991	Nagata, et.al.	
		US-5,243,515	09/07/1993	Lee	
		US-5,287,407	02/15/1994	Holmes	
		US-5,428,606	06/27/1995	Moskowitz	
		US-5,365,586	11/15/1994	Indeck, et.al.	
		US-5,394,324	02/28/1995	Clearwater	
		US-5,408,505	04/18/1995	Indeck, et.al	
		US-5,412,718	05/02/1995	Narasimhalv, et.al	
		US-5,487,168	01/23/1996	Geiner, et.al.	
		US-5,493,677	02/20/1996	Balogh, et.al	
		US-5,530,759	06/25/1996	Braudaway, et.al	
		US-5,606,609	02/25/1997	Houser, et.al.	
		US-5,613,004	03/18/1997	Cooperman, et.al.	
		US-5,617,119	04/01/1997	Briggs, et.al	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		WO 99/62044	12/02/1999	Handel, Theodore et.al		
		WIPO 96/29795	09/26/1996	Micali		
		WIPO 97/24833	07/10/1997	Micali		
		EP 0649261	04/19/1995	Enari		
		NL 100523	09/1998			

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,528,588	07/09/1985	Lofberg	
		US-5,832,119	11/03/1998	Rhoads	
		US-5,859,920	01/12/1999	Daly et.al	
		US-4,979,210	12/18/1990	Nagata et.al	
		US-5,774,452	06/30/1998	Wolosewicz	
		US-4,405,829	09/20/1983	Rivest et.al	
		US-6,330,335	12/11/2001	Rhoads	
		US-3,986,624	10/19/1976	Cates Jr. et.al	
		US-5,363,448	11/08/1994	Koopman et.al	
		US-5,568,570	10/22/1996	Rabbani	
		US-5,636,292	06/03/1997	Rhoads	
		US-4,972,471	11/20/1990	Gross et.al.	
		US-5,893,067	04/06/1999	Bender et.al.	
		US-5,689,587	11/18/1997	Bender et.al.	
		US-3,984,624	10/05/1976	Waggener	
		US-4,038,596	07/26/1977	Lee	
		US-4,200,770	04/29/1980	Hellman, et.al.	
		US-4,218,582	08/19/1980	Hellman, et.al.	
		US-4,424,414	01/03/1984	Hellman, et.al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		WO 9744736	11/27/1997	Wehrenberg		
		WO 9952271	10/14/1999	Moskowitz		
		WO 9963443	12/09/1999	Ho,Anthony Tung Shuen		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number / Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,640,569	06/17/1997	Miller, et.al.	
		US-5,659,726	08/19/1997	Sandford,II, et.al	
		US-5,664,018	09/02/1997	Leighton	
		US-5,687,236	11/11/1997	Moskowitz, et.al.	
		US-5,734,752	03/31/1998	Knox	
		US-5,745,569	04/28/1998	Moskowitz, et.al	
		US-5,506,795	04/09/1996	Yamakawa	
		US-5,680,462	10/21/1997	Miller, et.al	
		US-5,696,828	12/09/1997	Koopman, Jr.	
		US-5,740,244	04/14/1998	Indeck, et.al.	
		US-5,751,811	05/12/1998	Koopman, Jr.	
		US-5,757,923	05/26/1998	Koopman, Jr.	
		US-5,889,868	03/30/1999	Moskowitz, et.al.	
		US-6,208,745	03/27/2001	Florenio, et.al.	
		US-6,285,775	09/04/2001	Wu, et.al.	
		US-6,385,329	05/07/2002	Sharma, et.al	
		US-6,530,021	03/04/2003	Epstein, et.al.	
		US-6,425,081	07/23/2002	Iwamura	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document / Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,522,769	02/18/2003	Rhoads, et.al.	
		US-2005/0160271	07/21/2005	Brundage, et.al	
		US-6,665,489	12/16/2003	Collart	
		US-2004/0128514	07/01/2004	Rhoads	
		US-2004/0037449	02/26/2004	Davis, et.al.	
		US-6,823,455	11/23/2004	Macy, et.al.	
		US-2003/0133702	07/17/2003	Collart	
		US-6,668,246	12/23/2003	Yeung, et.al.	
		US-6,405,203	06/11/2002	Collart	
		US-6,141,754	10/31/2000	Choy	
		US-6,493,457	12/10/2002	Quackenbush	
		US-5,629,980	05/13/1997	Stefik, et.al.	
		US-5,943,422	08/24/1999	Van Wie, et.al.	
		US-5,636,276	06/03/1997	Brugger	
		US-5,341,429	08/23/1994	Stringer, et.al.	
		US-6,754,822	06/22/2004	Zhao	
		US-6,131,162	10/10/2000	Yoshiura et.al.	
		US-7,058,570	06/06/2006	Yu, et.al.	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 6 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,930,369	07/27/1999	Cox, et.al.	
		US-6,415,041	07/02/2002	Oami, et.al.	
		US-6,141,753	10/31/2000	Zhao, et.al.	
		US-2002/0097873	07/25/2002	Petrovic	
		US-6,785,815	08/31/2004	Serret-Avila, et.al.	
		US-6,523,113	02/18/2003	Wehrenberg	
		US-6,233,347	05/15/2001	Chen, et.al.	
		US-6,233,684	05/15/2001	Stefik, et.al.	
		US-2006/0013395	01/19/2006	Brundage, et.al.	
		US-7,043,050	05/09/2006	Yuval	
		US-5,809,160	09/15/1998	Powell, et.al.	
		US-6,272,634	08/07/2001	Tewfik, et.al.	
		US-6,282,650	08/28/2001	Davis	
		US-6,557,103	04/29/2003	Boncelet, Jr., et.al.	
		US-2003/0126445	07/03/2003	Wehrenberg	
		US-6,978,370	12/20/2005	Kocher	
		US-2006/0005029	01/05/2006	Petrovic, et.al.	
		US-6,278,791	08/21/2001	Honsinger, et.al.	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 7 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,598,162	07/22/2003	Moskowitz	
		US-6,275,988	08/14/2001	Nagashima, et al.	
		US-6,051,029	04/18/2000	Paterson, et al.	
		US-5,917,915	06/29/1999	Hirose	
		US-6,775,772	08/10/2004	Binding, et al.	
		US-6,668,246	12/23/2003	Yeung, et al.	
		US-6,351,765	02/26/2002	Pietropaolo, et al.	
		US-6,049,838	04/11/2000	Miller, et al.	
		US-5,398,285	03/14/1995	Borgelt, et al.	
		US-5,737,733	04/07/1998	Eller	
		US-2002/0103883	08/01/2002	Haverstock, et al.	
		US-5,673,316	09/30/1997	Auerbach, et al.	
		US-6,647,424	11/11/2003	Pearson, et al.	
		US-6,977,894	12/20/2005	Achilles, et al.	
		US-6,453,252	09/17/2002	Laroche	
		US-5,077,665	12/31/1991	Silverman, et al.	
		US-5,136,581	08/04/1992	Muehrcke	
		US-5,341,477	08/23/1994	Pitkin, et al.	
		US-5,581,703	12/03/1996	Baugher, et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 8 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,548,579	08/20/1996	Lebrun, et al.	
		US-5,905,975	05/18/1999	Ausubel	
		US-6,457,058	09/24/2002	Ullum et al.	
		US-6,381,618	04/30/2002	Jones et al.	
		US-2002/0026343	02/28/2002	Duenke	
		US-6,230,268	05/08/2001	Miwa et al.	
		US-6,199,058	03/06/2001	Wong et al.	
		US-5,920,900	07/06/1999	Poole et al.	
		US-5,884,033	03/16/1999	Duvall et al.	
		US-5,478,990	12/26/1995	Montanari et al.	
		US-6,430,302	08/06/2002	Rhoads	
		US-6,725,372	04/20/2004	Lewis et al.	
		US-6,606,393	08/12/2003	Xie et al.	
		US-6,584,125	06/24/2003	Katto	
		US-6,442,283	08/27/2002	Tewfik et al.	
		US-6,377,625	04/23/2002	Kim	
		US-6,282,300	08/28/2001	Bloom et al.	
		US-6,205,249	03/20/2001	Moskowitz	
		US-6,029,126	02/22/2000	Malvar	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 9 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,754,697	05/19/1998	Fu et al.	
		US-5,479,210	12/26/1995	Cawley et al.	
		US-3,947,825	03/30/1976	Cassada	
		US-5,903,721	05/11/1999	Sixtus	
		US-5,790,677	08/04/1998	Fox et al.	
		US-5,243,515	09/07/1993	Clearwater	
		US-4,339,134	07/13/1982	Macheel	
		US-4,827,508	05/02/1989	Shear	
		US-4,896,275	01/23/1990	Jackson	
		US-4,977,594	12/11/1990	Shear	
		US-5,050,213	09/17/1991	Shear	
		US-5,369,707	11/29/1994	Follendore, III	
		US-5,406,627	04/11/1995	Thompson et al.	
		US-5,410,598	04/25/1995	Shear	
		US-5,469,536	11/21/1995	Blank	
		US-5,497,419	03/05/1996	Hill	
		US-5,513,261	04/30/1996	Maher	
		US-5,530,739	06/25/1996	Okada	
		US-5,598,470	01/28/1997	Cooper et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 10 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Num	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,625,690	04/29/1997	Michel et al.	
		US-5,633,932	05/27/1997	Davis et al.	
		US-5,719,937	02/17/1998	Warren et al.	
		US-5,737,416	04/07/1998	Cooper et al.	
		US-5,765,152	06/09/1998	Erickson	
		US-5,799,083	08/25/1998	Brothers et al.	
		US-5,973,731	10/26/1999	Schwab	
		US-5,894,521	04/13/1999	Conley	
		US-5,905,800	05/18/1999	Moskowitz et al.	
		US-5,963,909	10/05/1999	Warren et al.	
		US-5,974,141	10/26/1999	Saito	
		US-5,999,217	12/07/1999	Berners-Lee	
		US-6,041,316	03/21/2000	Allen	
		US-6,081,251	06/27/2000	Sakai et al.	
		US-6,278,780	08/21/2001	Shimada	
		US-6,301,663	10/09/2001	Kato et al.	
		US-6,240,121	05/29/2001	Senoh	
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 11 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	
Attorney Docket Num	NA 80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Pate... Applicant of Cited Document	Relevant Passages or Relevant Figures Appear
		US- 6,088,455	07/11/2000	Logan et al.	
		US- 5,634,040	05/27/1997	Her et al.	
		US- 6,381,747	04/30/2002	Wonfor et al.	
		US- 4,969,204	11/06/1990	Melnychuck et al.	
		US- 6,966,002	11/15/2005	Torrubia-Saez	
		US- 6,263,313	07/17/2001	Milstead, et al.	
		US- 7,093,295	08/15/2006	Saito	
		US- 6,587,837	07/01/2003	Spagna et al.	
		US- 6,931,534	08/16/2005	Jandel et al.	
		US- 2004/0049695	03/11/2004	Choi et al.	
		US- 2004/0083369	04/29/2004	Erlingsson et al.	
		US- 5,677,952	10/14/1997	Blakely et al.	
		US- 5,768,396	06/16/1998	Sone	
		US- 7,266,697	09/04/2007	Kirovski et al.	
		US- 5,136,646	08/04/1992	Haber et al.	
		US- 5,136,647	08/04/1992	Haber et al.	
		US- 7,206,649	04/17/2007	Kirovski et al.	
		US- 6,532,284	03/11/2003	Walker et al.	
		US- 7,020,285	03/28/2006	Kirovski et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Tr
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of inf

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 12 of 12

Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Num	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- 7,046,808	05/12/2006	Metois et al.	
		US- 6,430,301	08/06/2002	Petrovic	
		US- 2004/0059918	03/25/2004	Xu	
		US- 6,345,100	02/05/2002	Levine	
		US- 2004/0093521	05/13/2004	Hamadeh et al.	
		US- 2007/0083467	04/12/2007	Lindahl et al.	
		US- 7,231,524	06/12/2007	Burns	
		US- 2005/0246554	11/03/2005	Batson	
		US- 6,668,325	02/23/2003	Collberg et al.	
		US- 7,050,396	05/23/2006	Cohen et al.	
		US- 6,842,862	01/11/2005	Chow et al.	
		US- 7,051,208	05/23/2006	Venkatesan et al.	
		US- 7,240,210	07/03/2007	Michak et al.	
		US- 7,150,003	12/12/2006	Naumovich et al.	
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

OIPE IAP84 OCT 19 2007 PATENT & TRADEMARK OFFICE

IFW

PTO/SB/21 (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

ENCLOSURES (Check all that apply)

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☑ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☑ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☑ Other Enclosure(s) (please Identify below):

Remarks

70 non-patent literature; 14 foreign patent documents; 13foreign patent and US unpublished patent applications by common inventor/applicant (CFR 1.78)

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name			
Signature	Scott Moskowitz		
Printed name	Scott MOSKOWITZ		
Date	October 17, 2007	Reg. No.	

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	Scott Moskowitz		
Typed or printed name	Scott MOSKOWITZ	Date	October 17, 2007

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/895,388	08/24/2007	Scott A. Moskowitz	80391.0003CONT2

CONFIRMATION NO. 2103

Scott A. Moskowitz
#2505
16711 Collins Avenue
Sunny Isless Beach, FL33160

Title: Data protection method and device

Publication No. US-2008-0016365-A1
Publication Date: 01/17/2008

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Pre-Grant Publication Division, 703-605-4283

UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	11/895,388	Confirmation No. 2103
Applicant	:	Scott A. MOSKOWITZ	
Filed	:	August 24, 2007	
TC/A.U.	:	2432	
Examiner	:	NA	
Docket No.	:	80391.0003CONT2	

MAIL STOP AMENDMENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRELIMINARY AMENDMENT

Prior to examination on the merits and prior to calculation of the filing fee, please enter the following amendments to the application.

09/10/2009 CNGUYEN2 00000033 11895388
01 FC:1201 220.00 OP

IN THE CLAIMS:

Claims 6-31 were previously canceled without prejudice or disclaimer. Claims 6-31 were previously subject to a restriction requirement. Applicant reserves the right to pursue the subject matter of the original claims in this application and in other applications. This listing of claims will replace all prior versions, and listings, of claims in the application:

The Claims

1. (original) A method for copy protection of digital information, the digital information including a digital sample and format information, comprising the steps of:

identifying a portion of the format information to be encoded;

generating encoded format information from the identified portion of the format information; and

generating encoded digital information, including the digital sample and the encoded format information.

2. (original) The method of claim 1, further comprising the step of requiring a predetermined key to decode the encoded format information.

3. (original) The method of claim 2, wherein the digital sample and format information are configured to be used with a digital player, and wherein information output from the digital player will have a degraded quality unless the encoded format information is decoded with the predetermined key.

4. (original) The method of claim 3, wherein the information output from the digital player represents a still image, audio or video.

5. (original) The method of claim 3, wherein the information output represents text data to be authenticated.

Claims 6 – 31 (cancelled without prejudice to Applicant's right to seek allowance of said claims in a related application)

32. (original) A method for copy protection of software comprising: embedding the software with a watermark wherein the embedded software operates in a manner substantially the same as the software prior to the embedding step.

33. (original) The process of claim 32, wherein the step of embedding the software with a watermark increases the complexity of code analysis and/or tampering with the software.

34. (original) The process of claim 32, wherein the watermarked software queries a user for personalization information during installation of the software

35. (original) The process of claim 32, wherein the watermark is accessible with a key.

36. (original) The process of claim 35, wherein the key enables authorized use of the watermarked software.

37. (original) The process according to claim 35, wherein the key and license information are interchangeable.

38. (original) The process according to claim 32, wherein the step of embedding the software with a watermark is performed during execution of the software.

39. (original) The process according to claim 32, wherein the step of embedding the software with a watermark modifies the structure of the software being embedded.

40. (original) An article of manufacture comprising a machine readable medium, having thereon stored instructions adapted to be executed by a processor, which instructions when executed result in a process comprising: receiving potentially watermarked software; and identifying the software by extracting the watermark.

41. (original) The article of manufacture of claim 40, wherein the watermark is associated with information fixed prior to distribution of the watermarked software.

42. (original) The article of manufacture of claim 40, wherein the watermark affects functionality of the watermarked software.

43. (original) The article of manufacture of claim 40, wherein the extracted watermark enables generation of a key.

44. (original) The article of manufacture of claim 43, wherein the generated key and licensing information are associated.

45. (original) The article of manufacture of claim 40, further comprising limiting functionality of the software if the watermark cannot be extracted.

46. (original) A method for watermarking software comprising: determining the structure a plurality of code contained in the software; and configuring at least a portion of the plurality of code according to a watermarking process.

47. (original) The process of claim 46, wherein the watermarking process further comprises inserting information into the software after installation.

48. (original) The process of claim 46, wherein the watermarking process configures the at least a portion of the plurality of code according to a key.

49. (original) The process of claim 46, wherein the watermarking process increases the complexity of code analysis and/or tampering with the software.

50. (original) The process of claim 46, wherein the watermarking process is selected from the group comprising: data hiding, steganography or steganographic ciphering.

51. (original) The process of claim 46, wherein the watermarking process is applied during execution of the software.

52. (currently amended) A system for copy protection of software comprising [[the steps of]]:

an encoder for associating license information with a copy of a software application[[;]] and encoding the associated license information into the copy of the software application [[using a watermarking process]]; and

an installer for installing [[providing]] the copy of the software application having license information encoded therein [[to a user;]] and[[,]] comparing information received by a user with the encoded license information.

53. (original) The system of claim 52, wherein the encoding is controlled by a key.

54. (original) The system of claim 52, wherein the step of comparing the user supplied information with the encoded license information enables authorization of the software.

55. (original) The system of claim 53, wherein the key is fixed prior to distribution of the software.

56. (currently amended) The system of claim 52, wherein the license information comprises code which affects functionality of the [[watermarked]] software.

57. (currently amended) The system of claim 52, wherein the [[watermarked]] software is resistant to code analysis and/or tampering.

58. (new) A method for licensed software use, the method comprising the steps of:

requesting license information associated with the software;

comparing the requested license information with license information stored in the software; and

enabling use of the software based on the comparison step.

59. (new) An article of manufacture comprising a machine readable medium, having thereon stored instructions representing software adapted to be executed by a processor, the instructions comprising:

instructions for requesting license information associated with the software;

instructions for enabling the software after the received license information has been compared with license information stored in the software; and

instructions for enabling authorized use of the software.

REMARKS

Applicant requests entry of the amendments and submits that this application is in condition for allowance, and a notice to this effect is earnestly sought.

Respectfully submitted,

Date: September 8, 2009

By: _____
Scott A. Moskowitz
Tel (305) 956-9041
Fax (305) 956-9042

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	11/895,388	Confirmation No. 2103
Applicant	:	Scott A. MOSKOWITZ	
Filed	:	August 24, 2007	
TC/A.U.	:	2432	
Examiner	:	NA	
Docket No.	:	80391.0003CONT2	

MAIL STOP: AMENDMENT - IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Dear Sir:

Applicant(s) submit copies of the references listed on the attached SB08 Form(s) for consideration and request that the U.S. Patent and Trademark Office make them of record in this application.

Applicant(s) state the following:

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Information Disclosure Statement; or

☐ No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and to the knowledge of Applicant(s) no item of information contained in this

09/10/2009 CNGUYEN2 00000033 11895388
02 FC:1806 180.00 OP

Information Disclosure Statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

☒ In accordance with 37 C.F.R. § 1.97(b), this Information Disclosure Statement is believed to be submitted prior to issuance of a first Office Action and/or within three months of the filing date of the application. It is respectfully submitted that no fee is required for consideration of this information.

☐ This Information Disclosure Statement is being submitted after the mailing of a non-final Office Action, but is believed to be prior to a final Office Action or a Notice of Allowance. Pursuant to 37 C.F.R. § 1.97(c), payment in the amount of $180.00 as set forth in 37 C.F.R. § 1.17(p) is enclosed.

While the information and references disclosed in this Information Disclosure Statement are submitted pursuant to 37 C.F.R. § 1.56, this submission is not intended to constitute an admission that any patent, publication or other information referred to is "prior art" to this invention. Applicant(s) reserve the right to contest the "prior art" status of any information submitted or asserted against the application.

Additionally, pursuant to C.F.R. § 1.78, Applicant(s) wish to inform the Examiner of the existence of the following co-pending U.S. patents and patent applications that share a common inventor with the present application. Under 37 C.F.R. § 1.98(a)(1), Applicant(s) also wish to inform the Examiner of the existence of the following co-pending foreign patents and patent applications that share a common inventor with the present application in the "section separate from the citations of other documents" entitled "Foreign Patent Documents", below:

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

U.S. PATENT DOCUMENTS

EXAMINER'S
INITIALS:

_____ U.S. Patent Application No. 08/999,766, filed July 23, 1997, entitled "Steganographic Method and Device" (issued as U.S. Patent No. 7,568,100);

_____ U.S. Patent Application No. 11/894,443, filed August 21, 2007, entitled "Steganographic Method and Device" – Publication No. 20080075277 – March 27, 2008;

_____ U.S. Patent Application No. 11/894,476, filed August 21, 2007, entitled "Steganographic Method and Device" – Publication No. 20070294536 – December 20, 2007;

_____ U.S. Patent Application No. 11/050,779, filed February 7, 2005, entitled "Steganographic Method and Device" – Publication No. 20050177727 – August 11, 2005;

_____ U.S. Patent Application No. 12/383,916, filed March 30, 2009, entitled "Steganographic Method and Device";

_____ U.S. Patent Application No. 08/674,726, filed July 2, 1996, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management" (issued as U.S. Patent No. 7,362,775);

_____ U.S. Patent Application No. 12/009,914, filed January 23, 2008, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management" -- Publication No. 20080151934 – June 26, 2008;

_____ U.S. Patent Application No. 09/545,589, filed April 7, 2000, entitled "Method and System for Digital Watermarking" (issued as U.S. Patent No. 7,007,166);

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ U.S. Patent Application No. 11/244,213, filed October 5, 2005, entitled "Method and System for Digital Watermarking" – Publication No. 20060101269 – May 11, 2006 (issued as U.S. Patent No. 7,343,492);

_____ U.S. Patent Application No. 11/649,026, filed January 3, 2007, entitled "Method and System for Digital Watermarking" – Publication No. 20070113094 – May 17, 2007;

_____ U.S. Patent Application No. 12/005,230, filed December 26, 2007, entitled "Method and System for Digital Watermarking" – Publication No. 20080133927 – June 5, 2008;

_____ U.S. Patent Application No. 09/046,627, filed March 24, 1998, entitled "Method for Combining Transfer Function with Predetermined Key Creation" (issued as U.S. Patent No. 6,598,162);

_____ U.S. Patent Application 10/602,777, filed June 25, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation" – Publication No. 20040086119 – May 6, 2004;

_____ U.S. Patent Application 11/895,388, filed August 24, 2007, entitled "Data Protection Method and Device" – Publication No. 20080016365 – January 17, 2008;

_____ U.S. Patent Application No. 09/053,628, filed April 2, 1998, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" (issued as U.S. Patent No. 6,205,249);

_____ U.S. Patent Application No. 09/644,098, filed August 23, 2000, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" (issued as U.S. Patent No. 7,035,409);

_____ U.S. Patent Application No. 09/767,733, filed January 24, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" – Publication No. 20010010078 - July 26, 2001;

_____ U.S. Patent Application No. 11/358,874, filed February 21, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" – Publication No. 20060140403 – June 29, 2006;

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ U.S. Patent Application No. 10/417,231, filed April 17, 2003, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth" – Publication No. 20030200439 – October 23, 2003 (issued as U.S. Patent No. 7,287,275);

_____ U.S. Patent Application No. 11/900,065, filed September 10, 2007, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth" – Publication No. 20080005571 – January 3, 2008;

_____ U.S. Patent Application No. 11/900,066, filed September 10, 2007, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth" -- Publication No. 20080005572 – January 3, 2008 (issued as U.S. Patent No. 7,530,102);

_____ U.S. Patent Application No. 12/383,289, filed March 23, 2009, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth" -- Publication No. 20090210711 – August 20, 2009;

_____ U.S. Patent Application No. 09/789,711, filed February 22, 2001, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20010010078 - October 11, 2001 (issued as U.S. Patent No. 7,107,451);

_____ U.S. Patent Application No. 11/497,822, filed August 2, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070011458 – January 11, 2007 (issued as U.S. Patent No. 7,457,962);

_____ U.S. Patent Application No. 12/217,834, filed July 9, 2008, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20090037740 – February 5, 2009;

_____ U.S. Patent Application No. 11/599,964, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

Digital Watermarks in Digital Data" – Publication No. 20080046742 – February 21, 2008;

_____ U.S. Patent Application No. 11/599,838, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070226506 – September 27, 2007 (Notice of Allowance Rec'd);

_____ U.S. Patent Application No. 11/897,790, filed August 31, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070300072 – December 27, 2007 (Allowance & Issue Fees Paid);

_____ U.S. Patent Application No. 12/462,799, filed August 10, 2009, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent Application No. 11/897,791, filed August 31, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20080022113 – January 24, 2008;

_____ U.S. Patent Application No. 11/899,661, filed September 7, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070300073 – December 27, 2007 (Notice of Allowance Rec'd);

_____ U.S. Patent Application No. 11/899,662, filed September 7, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20080022114 – January 24, 2008;

_____ U.S. Patent Application No. 10/369,344, filed February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data" – Publication No. 20030219143 – November 27, 2003 (issued as U.S. Patent No. 7,095,874);

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ U.S. Patent Application No. 11/482,654, filed July 7, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data" – Publication No. 20060285722 – December 21, 2006 (issued as U.S. Patent No. 7,409,073);

_____ U.S. Patent Application No. 12/215,812, filed June 30, 2008, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent Application No. 09/594,719, filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems" (issued as U.S. Patent No. 7,123,718);

_____ U.S. Patent Application No. 11/519,467, filed September 12, 2006, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems" – Publication No. 20070064940 – March 22, 2007;

_____ U.S. Patent Application No 09/731,040, filed December 7, 2000, entitled "Systems, Methods And Devices For Trusted Transactions" – Publication No. 20020010684 – January 24, 2002 (issued as U.S. Patent No. 7,159,116);

_____ U.S. Patent Application No 11/512,701, filed August 29, 2006, entitled "Systems, Methods And Devices For Trusted Transactions" – Publication No. 20070028113 – February 1, 2007;

_____ U.S. Patent Application No. 10/049,101, filed February 8, 2002, entitled "A Secure Personal Content Server" (which claims priority to International Application No. PCT/US00/21189, filed August 4, 2000, which claims priority to U.S. Patent Application No. 60/147,134, filed August 4, 1999, and to U.S. Patent Application No. 60/213,489, filed June 23, 2000) – (issued as U.S. Patent No. 7,475,246);

_____ U.S. Patent Application No. 12/287,443, filed October 9, 2008, entitled "A Secure Personal Content Server" (which claims priority to International Application No. PCT/US00/21189, filed August 4, 2000, which claims priority to U.S. Patent Application No. 60/147,134, filed August 4, 1999,

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

and to U.S. Patent Application No. 60/213,489, filed June 23, 2000) – Publication No. 20090089427 – April 2, 2009;

_____ U.S. Patent Application No. 09/657,181, filed September 7, 2000, entitled "Method And Device For Monitoring And Analyzing Signals" (issued as U.S. Patent No. 7,346,472);

_____ U.S. Patent Application No. 12/005,229, filed December 26, 2007, entitled "Method And Device For Monitoring And Analyzing Signals" -- Publication No. 20080109417 – May 8, 2008;

_____ U.S. Patent Application No. 10/805,484, filed March 22, 2004, entitled "Method And Device For Monitoring And Analyzing Signals"(which claims priority to U.S. Patent Application No. 09/671,739, filed September 29, 2000, which is a CIP of U.S. Patent Application No. 09/657,181) – Publication No. 20040243540 – December 2, 2004 – (abandoned);

_____ U.S. Patent Application No. 09/956,262, filed September 20, 2001, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects" -- Publication No. 20020056041 – May 9, 2002 (issued as U.S. Patent No. 7,127,615);

_____ U.S. Patent Application No. 11/518,806, filed September 11, 2006, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects" – Publication No. 20080028222 – January 31, 2008;

_____ U.S. Patent Application No. 11/026,234, filed December 30, 2004, entitled "Z-Transform Implementation of Digital Watermarks" – Publication No. 20050135615 – June 23, 2005 (issued as U.S. Patent No. 7,152,162);

_____ U.S. Patent Application No. 11/592,079, filed November 2, 2006, entitled "Linear Predictive Coding Implementation of Digital Watermarks" -- Publication No. 20070079131 – April 5, 2007;

_____ U.S. Patent Application No. 09/731,039, filed December 7, 2000, entitled "System and Methods for Permitting Open Access to Data Objects and

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

for Securing Data within the Data Objects" – Publication No. 20020071556 – June 13, 2002 (issued as U.S. Patent No. 7,177,429);

_____ U.S. Patent Application No. 11/647,861, filed December 29, 2006, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects" – Publication No. 20070110240 – April 5, 2007 (issued as U.S. Patent No. 7,532,725);

_____ U.S. Patent Application No. 12/383,879, filed March 30, 2009, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects" – Publication No. 20090190754 – July 30, 2009;

_____ U.S. Patent No. 5,428,606, issued June 27, 1995, entitled "Digital Commodities Exchange";

_____ U.S. Patent No. 5,539,735, issued July 23, 1996, entitled "Digital Information Commodities Exchange";

_____ U.S. Patent No. 5,613,004, issued March 18, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent No. 5,687,236, issued November 11, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent No. 5,745,569, issued April 28, 1998, entitled "Method for Stega-Protection of Computer Code";

_____ U.S. Patent No. 5,822,432, issued October 13, 1998, entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System";

_____ U.S. Patent No. 5,889,868, issued July 2, 1996, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 5,905,800, issued May 18, 1999, entitled "Method & System for Digital Watermarking";

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ U.S. Patent No. 6,078,664, issued June 20, 2000, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 6,205,249, issued March 20, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

_____ U.S. Patent No. 6,522,767, issued February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 6,598,162, issued July 22, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation";

_____ U.S. Patent No. 6,853,726, issued February 8, 2005, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 7,007,166, issued February 28, 2006, entitled "Method & System for Digital Watermarking";

_____ U.S. Patent No. 7,035,049, issued April 25, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

_____ U.S. Patent No. 7,095,874, issued August 22, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 7,107,451, issued September 12, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent No. 7,123,718, issued October 17, 2006, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems";

_____ U.S. Patent No. 7,127,615, issued October 24, 2006, "Improved Security Based on Subliminal and Supraliminal Channels for Data Objects";

_____ U.S. Patent No. 7,152,162, issued December 19, 2006, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 7,159,116, issued January 2, 2007, entitled "Systems, Methods and Devices for Trusted Transactions";

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ U.S. Patent No. 7,177,429, issued February 13, 2007, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects";

_____ U.S. Patent No. 7,287,275, issued October 23, 2007, entitled "Methods, Systems and Devices for Packet Watermarking And Efficient Provisioning Of Bandwidth";

_____ U.S. Patent No. 7,343,492, issued March 11, 2008, entitled "Method and System for Digital Watermarking";

_____ U.S. Patent No. 7,346,472, issued March 18, 2008, entitled "Method and Device for Monitoring and Analyzing Signals";

_____ U.S. Patent No. 7,362,775, issued April 22, 2008, entitled "Methods for Assigning Values to And Exchanging Bandwidth Securitization Instruments" (title amended September 6, 2000);

_____ U.S. Patent No. 7,409,073, issued August 5, 2008, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 7,457,962, issued November 25, 2008, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data"

_____ U.S. Patent No. 7,475,246, issued January 6, 2009, entitled "A Secure Personal Content Server";

_____ U.S. Patent No. 7,530,102, issued May 5, 2009, entitled "Methods, Systems and Devices for Packet Watermarking And Efficient Provisioning Of Bandwidth";

_____ U.S. Patent No. 7,532,725, issued May 12, 2009, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects";

_____ U.S. Patent No. 7,568,100, issued July 28, 2009, entitled "Steganographic Method and Device"

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

FOREIGN PATENT DOCUMENTS

EXAMINER'S
INITIALS:

_____ PCT Application No. PCT/US95/08159, filed June 26, 1995, entitled, "Digital Information Commodities Exchange with Virtual Menuing";

_____ PCT Application No. PCT/US96/10257, filed June 7, 1996, entitled, "Steganographic Method and Device" – corresponding to – EPO Application No. 96919405.9, entitled "Steganographic Method and Device";

_____ PCT Application No. PCT/US97/00651, filed January 16, 1997, entitled, "Method for Stega-Cipher Protection of Computer Code" – corresponding to AU199718294A (not available);

_____ PCT Application No. PCT/US97/00652, filed January 17, 1997, entitled, "Method for an Encrypted Digital Watermark" – corresponding to AU199718295A (not available);

_____ PCT Application No. PCT/US97/11455, filed July 2, 1997, entitled, "Optimization Methods for the Insertion, Protection and Detection of Digital Watermarks in Digitized Data" – corresponding to AU199735881A (not available);

_____ PCT Application No. PCT/US99/07262, filed April 2, 1999, entitled, "Multiple Transform Utilization and Applications for Secure Digital Watermarking" – corresponding to – Japan App. No. 2000-542907, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

_____ PCT Application No. PCT/US00/06522, filed March 14, 2000, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems";

_____ PCT Application No. PCT/US00/18411, filed July 5, 2000, entitled, "Copy Protection of Digital Data Combining Steganographic and Cryptographic Techniques" – corresponding to AU200060709A5 (not available);

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ PCT Application No. PCT/US00/21189, filed August 4, 2000, entitled, "A Secure Personal Content Server";

_____ PCT Application No. PCT/US00/33126, filed December 7, 2000, entitled, "Systems, Methods and Devices for Trusted Transactions" – corresponding to AU200120659A5 (not available);

_____ EPO Divisional Patent Application No. 07112420.0, entitled "Steganographic Method and Device" (corresponding to PCT Application No. PCT/US96/10257, filed June 7, 1996, entitled, "Steganographic Method and Device" – cited above – previously provided)

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. This Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed documents and information.

Respectfully submitted,

Date: September 8, 2009

By:

Scott A. Moskowitz
Tel# (305) 956-9041
Fax# (305) 956-9042

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

OIPE
SEP 08 2009
PATENT & TRADEMARK OFFICE

PTO/SB/08A (01-08)
Approved for use through 01/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 4

Complete if Known	
Application Number	11/895,388
Filing Date	Aug 24, 2007
First Named Inventor	Scott A. Moskowitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	80391.0003Cont 2

U. S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- 6,389,538	05/14/2002	Gruse et al.	
		US- 5,513,126	04/30/1996	Harkins et al.	
		US- 5,657,461	08/12/1997	Harkins et al.	
		US- 4,390,898	06/28/1983	Bond et al.	
		US- 5,471,533	11/28/1995	Wang et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		EP 1547337 B1	03/22/2006	Erlingsson et al.		
		EP 1354276 B1	12/12/2007	Bum et al.		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08a (01-08)
Approved for use through 05/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 4

Complete if Known	
Application Number	11/895 388
Filing Date	August 24, 2007
First Named Inventor	Scott A Moskowitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- 6,044,471	03/28/2000	Colvin	
		US- 7,103,184	09/05/2006	Jian	
		US- 7,233,669	06/19/2007	Candelore	
		US- 6,446,211	09/03/2002	Colvin	
		US- 6,484,264	11/19/2002	Colvin	
		US- 6,502,195	12/31/2002	Colvin	
		US- 6,785,825	08/31/2004	Colvin	
		US- 6,792,548	09/14/2004	Colvin	
		US- 6,792,549	09/14/2004	Colvin	
		US- 6,795,925	09/21/2004	Colvin	
		US- 6,799,277	09/28/2004	Colvin	
		US- 6,813,717	11/02/2004	Colvin	
		US- 6,813,718	11/02/2004	Colvin	
		US- 6,857,078	02/15/2005	Colvin	
		US- 6,986,063	01/10/2006	Colvin	
		US- 2004/0117628	06/17/2004	Colvin	
		US- 2004/0117664	06/17/2004	Colvin	
		US- 2004/0225894	11/11/2004	Colvin	
		US- [redacted]	[redacted]	[redacted]	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 4

Complete if Known	
Application Number	11/895,388
Filing Date	Aug 24 2007
First Named Inventor	Scott A Moskowitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-7,177,430	02/13/2007	Kim	
		US-5,210,820	05/11/1993	Kenyon	
		US-2001/0043594	11/22/2001	Ogawa et al.	
		US-6,658,010	12/03/2003	Enns et al.	
		US-6,463,468	10/08/2002	Buch et al.	
		US-5,862,260	01/19/1999	Rhoads	
		US-6,373,960	04/16/2002	Conover et al.	
		US-2007/0253594	11/01/2007	Lu et al.	
		US-2006/0041753	02/23/2006	Haitsma	
		US-6,784,354	08/31/2004	Lu et al.	
		US-2007/0127717	06/07/2007	Herre et al.	
		US-2006/0013451	01/19/2006	Haitsma	
		US-5,918,223	06/29/1999	Blum	
		US-5,765,152	06/09/1998	Erickson	
		US-5,142,576	08/25/1992	Nadan	
		US-5,923,763	07/13/1999	Walker et al.	
		US-2004/0028222	02/12/2004	Sewell et al.	
		US-7,460,994	12/02/2008	Herre et al.	
		US-7,107,451	09/12/2006	Moskowitz	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 4

Complete if Known	
Application Number	11/894,388
Filing Date	Aug 24, 2007
First Named Inventor	Scott A Moskowitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	8039I.0007 CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,748,783	05/05/1998	Rhoads	
		US-5,850,481	12/15/1998	Rhoads	
		US-5,860,099	01/12/1999	Milios et al.	
		US-6,363,483	03/26/2002	Keshav	
		US-7,162,642	01/09/2007	Schumann et al.	
		US-6,834,308	12/21/2004	Ikezoye et al.	
		US-6,983,337	11/22/2005	Wold	
		US-7,363,278	04/22/2008	Schmelzer et al.	
		US-2002/0073043	06/13/2002	Herman et al.	
		US-2004/0125983	07/01/2004	Reed et al.	
		US-2002/0161741	10/31/2002	Wang et al.	
		US-7,289,643	10/30/2007	Brunk et al.	
		US-7,286,451	10/23/2007	Wirtz et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (01-08)
Approved for use through 01/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	11/895,388
Filing Date	Aug 24, 2007
First Named Inventor	Scott A. Mosenlitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	80391.0003.CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		~~PCT International Search Report, completed July 26, 2001; authorized officer A. Sigolo (PCT/US00/18411) (5 pages)~~	
		~~PCT International Search Report, completed March 29, 2001; authorized officer P. Corcoran (PCT/US00/22100) (3 pages)~~	
		~~PCT International Search Report, completed January 26, 2001; authorized officer A. Sigolo (PCT/US00/21100) (3 pages)~~	
		European Search Report, completed October 15, 2007; authorized officer James Hazel (EP 07 11 2420) (9 pages)	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	11/895,388
Filing Date	Aug 24, 2007
First Named Inventor	Scott A. Moskowitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		STAIND (The Singles 1996-2006), Warner Music - Atlantic, Pre-Release CD image, 2006, 1 page.	
		Arctic Monkeys (Whatever People Say I Am, That's What I'm Not), Domino Recording Co. Ltd., Pre-Release CD image, 2005, 1 page.	
		Radiohead ("Hail To The Thief"), EMI Music Group - Capitol, Pre-Release CD image, 2003, 1 page.	
		OASIS (Dig Out Your Soul), Big Brother Recordings Ltd., Promotion CD image, 2009, 1 page.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	11/895,388
Filing Date	Aug 24, 2007
First Named Inventor	Scott A Moskowitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	8039.0003cont2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Rivest, R. "Chaffing and Winnowing: Confidentiality without Encryption", MIT Lab for Computer Science, http://people.csail.mit.edu/rivest/Chaffing.txt, April 24, 1998, 9 pp.	
		PortalPlayer, PP502 digital media management system-on-chip, May 1, 2003, 4 pp.	
		VeriDisc, "The search for a Rational Solution to Digital Rights Management (DRM)", http://64.244.235.240/news/whitepaper/docs/veridisc_white_paper.pdf, 2001, 15 pp.	
		Cayre, et al., "Kerckhoff's-Based Embedding Security Classes for WOA Data Hiding". IEEE Transactions on Information Forensics and Security, Vol. 3 No. 1, March 2008, 15 pp.	
		Wayback Machine, dated January 17, 1999, http://web.archive.org/web/19990117020420/http://www.netzero.com/, accessed on February 19, 2008.	
		Namgoong, H., "An Integrated Approach to Legacy Data for Multimedia Applications", Proceedings of the 23rd EUROMICRO Conference, Vol., Issue 1-4, September, 1997, pp 387-391	
		Wayback Machine, dated August 26, 2007, http://web.archive.org/web/20070826151732/http://www.screenplaysmag.com/tabid/96/articleType/ArticleView/articleId/495/Default.aspx/	
		"YouTube Copyright Policy: Video Identification tool - YouTube Help", accessed June 4, 2009, http://www.google.com/support/youtube/bin/answer.py?h1=en&answer=83766, 3 pp.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 547 337 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
22.03.2006 Bulletin 2006/12

(21) Application number: **03771837.6**

(22) Date of filing: **25.07.2003**

(51) Int Cl.:
H04L 29/06 *(2006.01)* ***H04N 1/32*** *(2006.01)*

(86) International application number:
PCT/US2003/023302

(87) International publication number:
WO 2004/012416 (05.02.2004 Gazette 2004/06)

(54) **Watermarking at the packet level**

Wasserzeicheneinbettung auf der Paketebene

Tatouage numérique au niveau des paquets

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR

(30) Priority: **26.07.2002 US 398564 P**

(43) Date of publication of application:
29.06.2005 Bulletin 2005/26

(73) Proprietor: **Green Border Technologies**
Mountain View, CA 94043 (US)

(72) Inventors:
- **ERLINGSSON, Ulfar**
  San Francisco, CA 94115 (US)
- **BOYEN, Xavier**

  (US)
- **ANDERSON, Darrell**

  (US)
- **GRAY, Wayne**

  (US)

(74) Representative: **Beresford, Keith Denis Lewis et al**
BERESFORD & Co.
16 High Holborn
London WC1V 6BX (GB)

(56) References cited:
DE-A- 19 926 783
US-A1- 2002 059 522
US-B1- 6 282 650

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art.

EP 1 547 337 B1

Description

FIELD OF THE INVENTION

[0001] This invention relates generally to methods and systems for providing secure transactions across a network and, more particularly, to methods and systems for watermarking at the packet level.

BACKGROUND OF THE INVENTION

[0002] The ubiquity of networked computing environments, and the ever increasing reliance thereupon, has created a demand for network security products that guard against attacks from outside the network, such as computer worms or viruses, distributed denial of service attacks, and targeted criminal computer trespassing. Often ignored when discussing network security, but just as dangerous and disruptive, are attacks from inside the network. The proliferation of powerful portable networked computers, such as laptops, handheld devices, and personal digital assistants (PDAs), makes it particularly easy for an insider to connect a personal machine to a restricted network and unknowingly spread malicious programs, thereby compromising the integrity of the network.

[0003] Traditional approaches to ensuring the security and integrity of computer networks of any size include, for example, user authentication mechanisms, Internet firewalls and gateways, intrusion detection and reporting, systems, installation, update, and configuration deployment systems, and distributed computer management systems. User authentication mechanisms provide security by allowing only authorized users to log on to the network devices for which they have been approved. Among other things, these mechanisms may be useful for preventing persons foreign to the organization ("foreign persons") from inadvertently or maliciously compromising the network integrity from within, by means of, e.g., introducing malicious "Trojan horse" software, or tampering with the authorized installed software base. Internet firewalls and gateways filter out potentially unsafe content originating from untrusted sources at the point of entry into a network environment. Intrusion detection and reporting systems, including "anti-virus" software, aim at limiting the extent of the damage after a breach of integrity has occurred, by means of early detection and hopeful containment of the breach.

[0004] Installation, update, and configuration deployment systems, when used in conjunction with the above mechanisms, ensure that the security software is up-to-date in order to respond against the most recent attacks as they are discovered.. Distributed computer management systems ensure that all devices on a network have an approved configuration and only run approved applications.

[0005] All of the security mechanisms described above operate on the premise that if a networked environment is defended from outside threats, the entire environment will remain safe. These security mechanisms, however, are useless against internal threats such as the following. Say, for example, an authorized user inadvertently introduces a computer virus on an authorized machine by opening an infected piece of email from a business partner. In this case, the virus takes control of the machine and proceeds to replicate over the entire network. Another such internal threat is, for example, an authorized user that takes home an authorized laptop computer and connects it back to the internal network the following day. In the meantime, the laptop became infected with a virus, which has spread to the network from the inside. Yet another example of an internal threat is an authorized user that brings his or her own personal laptop or handheld computer and configures it to interoperate with the corporate network. Most networks do not authenticate the machines that are connected to them, or do so in such a way that the security credentials can easily be replicated across machines, thereby allowing the network to become infected. A further example of an internal threat is a hacker that exploits the poor security of existing wireless network offerings to gain access to a nearby corporate wireless network. Even though the trespasser is probably unable to log on to the network, lacking a valid password, the integrity of the network may still be potentially compromised by his or her activities.

[0006] These examples illustrate the necessity of some form of protection against internal threats, whether the threats result from inadvertence or malice.

The document US6282650 discloses a digital watermarking as a technique to protect against unauthorized copying and distribution of digital content. This is accomplished by placing the watermark into a noise band of the data set.

SUMMARY OF THE INVENTION

[0007] According to at least one aspect of the invention, method device and system are disclosed for providing secure transmissions across a network comprising a transmitting device and a receiving device. At the transmitting device, a stream of watermark bits is generated. Next, a plurality of watermarks is generated, each of the plurality of watermarks comprising an index number and a portion of the stream of watermark bits. The watermarks are inserted into the headers of a plurality of outgoing packets. At the receiving device, the plurality of outgoing packets are received and it is determined if a received packet is valid based on the watermark in the header of the received packet.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate exemplary implementations and embodiments of the invention and, together with the detailed description, serve to explain the principles of the invention. In the drawings,

[0009] **FIG. 1** is a high level block diagram of an exemplary client-side system for practicing systems and methods consistent with the present invention;

[0010] **FIG. 2** is a high level block diagram of an exemplary server-side system for practicing systems and methods consistent with the present invention;

[0011] **FIG. 3** shows one exemplary method for watermarking outgoing packets consistent with the present invention;

[0012] **FIG. 4** shows one exemplary method for verifying incoming watermarked packets consistent with the present invention;

[0013] **FIG. 5** illustrates one embodiment of a client-server system consistent with the present invention; and

[0014] **FIG. 6** shows, in more detail, an example of a client-server system interconnected through the network.

DETAILED DESCRIPTION

[0015] Reference will now be made in detail to exemplary implementations and embodiments of the invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

INTRODUCTION

[0016] The present invention provides methods and systems for addressing the threats posed to a computer network environment that may be created by the connection of potentially unsafe devices to, and from within, the network environment. It is well known that conventional networks may comprise "servers" and "clients." Generally speaking, "servers" are the devices in a network that provide data and "clients" are other machines in the network that request data. In most cases, servers are protected against direct user tampering, but may be subject to internal attacks coming from the various clients that connect to the network. Systems and methods consistent with the present invention protect servers against such internal network attacks.

[0017] The present invention is described herein in terms of "client" aspects and "server" aspects. However, those skilled in the art will understand that, in some cases, the same machine in a network may act as both a client and a server. The same machine may, for example, work as a client in one transaction, but then operate as a server in a different transaction. This may occur, for example, when machines are interconnected as peers in a work group. In such cases, both the client and the server aspects of the invention described therein may be practiced on the same machine.

[0018] The principles of the present invention may be described generally as follows. First, a client is determined to be "clean," that is, not containing a virus, Trojan horse, malicious software, or is otherwise secure. Once determined to be clean, the clean machine is associated with a secret token that acts as a cryptographic seal of authenticity. The secret token may take the form of, for example, a cryptographic key, a secret token, or a digital certificate. The determination that a client is clean may occur upon initial setup of a client by an authorized administrator or during operation by, for example, an automatic or manual process that inspects and validates the machine state or configuration.

[0019] The newly configured machine may also be equipped with a configuration monitoring system, which can monitor and mediate system activity. The configuration monitoring system may be integrated at the highest privilege level within the operating system and may ascertain that no unauthorized change has been effected or unauthorized application installed. The configuration monitoring system may act in accordance with a security policy in force in the network. If an anomaly or unauthorized action is detected, the integrity of the machine configuration or of the security mechanism itself may become untrustworthy, so the configuration monitoring system may destroy the secret token for this particular machine.

[0020] A communications monitoring system may be used, on the client machine, to intercept outgoing information packets. As long as the secret token is present, the communications monitor may use it to cryptographically watermark outgoing packets. In certain embodiments of the present invention, the watermarking is transparent to the underlying protocol, i.e., it does not affect the content of the packets, and does not interfere with the proper working of the communication protocols in case the receiving end is not equipped to recognize the watermarks.

[0021] On the server side, a similar communications monitor may be set to intercept and filter incoming packets as close as possible to the point of entry. Thereafter, the communications monitor only relays to other functions, such as higher-level services or applications, those packets that bear a valid and current watermark. The non-watermarked packets may be simply discarded.

[0022] In at least one embodiment, a system consistent with the present invention may comprise a client side and a

server side. In certain embodiments, the client side and the server side may be present in the same machine if, for example, the machine is to operate as both a trusted client and a server on the protected network.

CLIENT-SIDE SYSTEM

[0023] **FIG. 1** is a high level block diagram of an exemplary client-side system for practicing systems and methods consistent with the present invention. As shown in FIG. 1, in exeraplary embodiments, a client comprises a configuration monitoring module 110, a communications monitoring module 120, and a watermarking module 130. Session table 170 stores active sessions and can be queried by other modules to determine if a particular session is active.

[0024] Configuration monitoring module 110 may monitor the configuration of any number of applications 140, 141, 142, ... 14n and of operating system kernel 150 running on the client. Such monitoring may be, for example, constant, periodic, or may be triggered by events, such as a request to use secret token 115 by watermarking module 130, or other events that may result in a configuration change. Examples of events that may cause potentially threatening configuration changes include, without being limited to:

- Anti-virus definition database becoming too old;
- Key system components being tampered with;
- Modification of key system or application binaries;
- Security or configuration parameters being modified;
- Modification of system configuration files or databases;
- Device driver being installed or loaded into the kernel;
- Non-sanctioned application being installed in the main environment (as opposed to within an isolated virtualized safety environment); and
- Security software being uninstalled (such as GreenBorder Internet Security, which provides a transparently isolated virtual environment for untrusted applications).

[0025] Configuration monitoring module 110 also safeguards the secret token 115, by monitoring the configuration of applications 140, 141, 142, ... 14n, and of operating system kernel 150, detecting changes to the configurations, and destroying secret token 115 or otherwise blocking its use, if a potentially threatening change to a configuration is detected. As mentioned above, the secret token may take the form of, for example, a cryptographic key, a secret token, or a digital certificate.

[0026] Configuration monitoring module 110 may be implemented using a combination of techniques commonly known to those skilled in the art, and services provided by common host operating systems. For example, the Windows Cryptographic API provides support for storing secret data on the local machine in a keyless, yet obfuscated manner. In at least one exemplary embodiment, configuration monitoring module 120 may be launched during the start-up sequence, at which time it verifies the integrity of the current configuration (such as, by comparing it to a cryptographically-signed reference specification).

[0027] Communications monitoring module 120 intercepts outgoing packets (such as IP packets, for systems communicating via the Internet Protocol) and checks to see if a secure communications session is still available. If a secure communications session has been established with the server, communications monitoring module 120 sends the packets to watermarking module 130 for tagging with a cryptographic watermark. In certain embodiments of the present invention, this module (and its counterpart on the server side, communications monitoring module 220) may reside at the base of the communication stack within the operating system kernel and may depend on the specifics of the operating system or the networking protocol in use. For example, communications monitoring modules 120 and 220 may be low-level IP stack monitors in charge of intercepting the outgoing or incoming IP traffic. In at least one exemplary embodiment, communications monitoring modules 120 and 220 are inserted to reside within the IP stack of the host operating system in such a way as to be activated whenever an IP segment or packet is to be transmitted or received. Communications monitoring modules 120 and 220 may then initiate watermarking-related operations by making appropriate calls to the watermarking module 130 and/or watermark verification module 230. In certain embodiments, both modules may reside within the kernel in an actual implementation. One exemplary implementation of an interface between a low-level IP stack monitor and watermarking module 130 may be found in Appendix A.

[0028] In certain embodiments, communications monitoring modules 120 and 220 may be inserted into modem versions of the FreeBSD kernel, which is a variant of Unix. Communications monitoring modules 120 and 220 may then be compiled as a run-time loadable kernel module, which attaches to the kernel-supplied hooks into the IP stack, originally designed to accommodate external packet filters or firewalls. In certain operating systems, such as Microsoft Windows, the kernel source code may be unavailable. In such implementations, communications monitoring modules 120 and 220 ay be loaded alongside an operating kernel, and inserted into the running kernel by redirecting internal IP-stack kernel system calls, in a manner familiar to those skilled in the art.

[0029] Configuration monitoring module 110 also provides secret token 115 to watermarking module 130 as needed. Watermarking module 130, for example, receives packets from communications module 120 and communicates with configuration monitoring module 110 to determine if secret token 115 is still available for use in watermarking packets. Watermarking module 130 may initiate, maintain, and, if necessary, restore, a shared secret authentication state with each server the client is communicating with. In certain embodiments, this module is independent of the operating system, although it may optionally communicate with a network-wide security infrastructure (such as a Kerberos interface or public-key infrastructure (PKI) 135) to obtain server-specific key material, such as during the initial authentication data sent upon first communicating with a new server.

SERVER-SIDE SYSTEM

[0030] **FIG. 2** is a high level block diagram of an exemplary server-side system for practicing systems and methods consistent with the present invention. In exemplary embodiments, the server-side system is composed of a communications monitoring module 220 and a watermark verification module 230. Optionally, the server-side system may also comprise a policy module 270.

[0031] Communications monitoring module 220 intercepts incoming network traffic, and filters it before providing it to the rest of the system and/or applications running on the server. In at least one embodiment, communications monitoring module 220 filters incoming traffic based on watermark validity. In certain embodiments, both module 220 and its namesake on the client side (module 120) may reside at a low level within the operating system of the server and client, respectively. The operation of these modules may also vary depending on the networking protocol in use.

[0032] Watermark verification module 230 may be called by communications monitoring module 220. Watermark verification module 230 verifies the validity of the watermarks associated with incoming packets, and determines whether the bearing packets should be allowed to proceed, or be dropped. In certain embodiments, this determination is optionally based on a security policy. This module may optionally interact with a network-wide security infrastructure, for example, to obtain client-specific key material used during the validation of the initial authentication data received from a client.

[0033] An optional security policy module 270 may be used to specify exceptions to the watermark-based filtering scheme in order, for example, to allow some or all incoming packets to be allowed to proceed, even without a valid watermark. For example, an exemplary policy may state that all Dynamic Host Configuration Protocol (DHCP) requests and Domain Name System (DNS) queries should be allowed to proceed, even without a valid watermark. The DHCP is an Internet protocol for automating the configuration of computers that use TCP/IP and can be used to automatically assign IP addresses, deliver TCP/IP stack configuration parameters, and provide other configuration information. DNS is used to translate between domain names and IP addresses and control Internet email delivery and location of web sites.

WATERMARKING

[0034] Methods and systems consistent with the present invention construct watermarks that are compatible with network transport protocols, such as Internet Protocol, by creating a covert channel in the packet header that is non-disruptive to the standards of various transport protocols. Communications may begin with a special packet recognized only by compliant servers. Thereafter, subsequent packets in a session are transparently watermarked using available bytes in the header, albeit in such a way that links them in a sequence originating in the initial packet.

[0035] **FIG. 3** shows one exemplary method for watermarking outgoing packets consistent with the present invention. To begin, a client prepares to transmit a packet to a server. The request to send a packet is intercepted (step 310). The packet may be intercepted, for example, by communications monitoring module 120 of Fig. 1. The communications monitoring module checks to see if the client already has established a secure communication session with the target server by, for example, checking the active sessions stored in table 170 (step 320). If the client has not yet established a secure communication session with the server, such as when starting communication with a server for the first time, the client initiates a secure communication session (step 325).

[0036] To initiate a secure communication session, the originating client sends a packet containing authentication/synchronization data to the server (step 330). The authentication/synchronization data may be based on the secret token of the client (assuming that it has not been discarded by the configuration verification subsystem). The authentication/synchronization data may be constructed based on single-pass symmetric or asymmetric encrypted key exchange techniques as known in the art. In some embodiments, construction of the authentication/synchronization data using a symmetric cipher or message authentication code (MAC), for example, may be preferred, such as in the case where all servers are restricted devices that may be entrusted with the knowledge of the secret tokens provided to the clients (e.g., centrally administered corporate servers out of reach of ordinary users). In certain embodiments, use of an asymmetric cipher or key exchange scheme may be preferred or even mandated depending on the application. Use of an asymmetric cipher may allow the authentication mechanism to work even though the servers are not entrusted with copies of the client tokens.

[0037] The authentication/synchronization data may be constructed based on some or all of the following elements: the client secret token; the server public key, if applicable; the client network address (and .port, if applicable); the server network address (and port, if applicable); the current time; and a cryptographic salt. In general, the authentication/synchronization data proves to the server, in a cryptographically strong way, that the client still possesses its secret token (typically without revealing it), which is a means for indicating that data from the client is coming from a safe and approved configuration. This authentication/synchronization data may also be used to establish a cryptographically strong shared secret session state between the client and the server, which the subsequent packet watermarks can leverage.

[0038] Upon sending the initial synchronization packet, the client constructs the corresponding shared cipher state, and stores it for future use. This information may be stored, for example, in table 260 of FIG. 2, which may be a lookup table, wherein the information is stored under the server designation (e.g., indexed by address and port). Upon receiving the initial synchronization packet, the server authenticates the information by, for example, verifying that the time stamp is current and the claimed source and destination addresses are correct (see, for example, step 425 of FIG. 4). The server may then use the received data to construct the shared stream cipher state, as will be discussed in more detail below. Table 260, therefore, indicates whether a particular session is an active session.

[0039] Once a shared cipher state has been achieved between the client and the server, communications from the client to the server may proceed. Before watermarking of packets may take place, methods consistent with the present invention determine whether the secret token is still available. As discussed herein, watermarking module 130 may query configuration monitoring module for the status of secret token 115. If configuration monitoring module 110 has detected a potentially threatening change to a configuration, signaling perhaps that the client is no longer "clean," configuration monitoring module 115 may have destroyed or rendered unavailable secret token 115. In this case, the packets may not be watermarked, but may be transmitted to the target server (step 340).

[0040] If, however, secret token 115 is still available (step 335), a watermark may be computed based on the secret token (step 345) and the watermark may be attached to one or more packets (step 350). Thereafter, the watermarked packets may be sent to the server (step 355).

[0041] Specifically, the initial special packet is used to set up a shared secret session key from the client to the server. The shared secret session key may then be used to generate a sequence of bits to be used as watermarks for the regular data packets in the session. The sequence used to watermark regular data packets may, for example, be a stream generated using a stream cipher such as RC4, a block cipher such as 3DES in CBC mode, or other equivalent pseudo-random stream generating techniques. The stream may be pseudo-random. Techniques for generating the stream may be implemented in software or hardware.

[0042] In at least one exemplary embodiment, on the client side, each outgoing packet to the designated server is transparently watermarked with cipher stream data by replacing a certain number of bits of header information with an equivalent number of bits from the generated stream. The amount of data added to each packet may vary according to underlying packet format. In the Internet Protocol, for example, two bytes or sixteen bits of watermark can be transparently inserted in each data packet using methods described herein. In one exemplary embodiment, the watermarks are generated sequentially from the initial state of the stream cipher (and thus differ from one packet to the next). Additionally, each watermark in a given sequence may be associated with an index number, starting at 0 (thus, in this example, 0 is the index of the synchronization packet, 1 is the index of the watermark attached with the first data packet, and so on). Hence, the client generates watermarks in increasing natural order of index number.

[0043] In certain embodiments, the value of the data used to watermark the packets does not depend on the data payload of the packet to which it is attached. In alternative embodiments, however, the watermark may be constructed to cryptographically depend on the packet content, thereby ensuring the integrity of such content.

[0044] Unlike alternative backward-incompatible technologies, such as SSL, the watermarking approach allows compliant servers to gain assurance of package integrity without breaking backward compatibility with non-compliant servers, thereby allowing clients to employ this technique without knowing whether the recipient is equipped with the technology to recognize the watermarks. In at least one such exemplary embodiment, the watermarks may be constructed using at least a portion of a MAC, instead of the actual cipher stream data, where the MAC is derived from the packet content data to protect, and is keyed by the cipher stream data it replaces, as those skilled in the art will appreciate.

[0045] In certain embodiments, payload-independent watermarks allow the underlying operating system to fully exploit the direct memory access (DMA) capabilities of the networking hardware, whereby the packet payload may be directly copied from main memory to the networking hardware buffer, without being seen by the CPU. Computing a MAC would otherwise force the CPU to access the payload.

[0046] The present invention also provides methods and systems to reduce or eliminate the lost, duplicated, or reordered packets that often occur in most computer networks. **FIG. 4** shows one exemplary method for verifying incoming watermarked packets consistent with the present invention. On the receiving end, incoming packets may be intercepted (step 410) such as by communications monitoring module 220 of FIG. 2. Communications monitoring module 220 may determine if the server has an active session with the client that sent the intercepted packet (step 415). If the server has

no active session with the transmitting client, the, server determines whether the incoming packet is authentication/ synchronization data sent by the client to establish a session (step 420). If the intercepted packet is authentication/ synchronization data, the server may authenticate the client information and establish a secure session (step 425). The server may authenticate the information by, for example, verifying that the time stamp is current and the claimed source and destination addresses are correct. The server may then use the received data to construct the shared stream cipher state, which it may then associate with the client's address and port. The server may also store the authentication/ synchronization data for use in computing

[0047] Authentication of each pair of communicating client and server uses a unique shared secret stream cipher state for the watermark generation and verification. To accommodate this, each client maintains a table of all current authenticated sessions indexed by server addresses (optionally including the ports) in table 170. Table 170 is periodically purged of any stale entry it may contain. "Stale" entries may be determined, for example, based on the time of last communication or other heuristics. If an active session is mistakenly purged, the client may be caused to re-synchronize with the server upon sending the next packet. The server similarly maintains a table of active sessions indexed by client network addresses (and, optionally, ports) in table 260.

[0048] If the intercepted packet is not authentication/synchronization data, or the client cannot be authenticated based on the authentication/synchronization data provided by the intercepted packet (step 425), the packet may simply be discarded as untrusted (step 430).

[0049] If, however, the server already has an active session with the client (step 415), the watermark may be extracted from the intercepted packet (step 440). The watermark may either be extracted by, for example, communications monitoring module 220 (and sent to watermark verification module 230) or directly by watermark verification module 230 if the entire packet is sent to watermark verification module 230 for processing.

[0050] After the watermark has been extracted, the watermark may be compared to "forward" and "backward" windows of expected watermarks maintained or generated by the server (step 445). As mentioned above, at the client, each watermark in a given sequence may be associated with an index number, such that watermarks are generated in an increasing natural order of the index numbers. In the present invention, the server may at all times maintain a record of or pointer to the index number of the highest-numbered valid watermark it has received (from a particular client). This index number may also be called the "pivot." The server may also maintain or generate two small lists, or windows, associating watermarks with their index numbers. A forward window comprises the watermarks whose index numbers immediately follow the pivot. A backward window comprises watermarks whose index numbers immediately precede the pivot. The server may generate the expected watermarks in the forward and backward windows based on the authentication/synchronization information received from the client.

[0051] Whenever the server receives a packet from a client, the watermark may be compared with the contents of both windows, so as to determine the index number of the match, if any (step 445). If a match is found in the forward window (step 450), the pivot may be increased accordingly, and the forward and backward windows may be adjusted based on the new pivot (step 460). For example, the forward window entries with index numbers between the old and the new value of the pivot may be displaced to the backward window, after which the forward window may be replenished with an appropriate number of new watermarks ahead of the current pivot, and the backward window may be trimmed of its oldest entries. If a match is found in the backward window (step 455), the matching entry may be removed from that window (the pivot and the forward window remain unchanged).

[0052] The watermark is accepted as valid (and therefore allowed to proceed) only if there was a match in either window (step 470). If no match was detected in step 450, the packet is discarded (step 430).

[0053] In at least one embodiment, to account for the possibility of severe transient network problems, an additional mechanism is provided, whereby, upon receiving an invalid watermark from a client, the server replies with a special re-authentication request (e.g., formatted as a UDP packet to an otherwise unused port, or using in any other method). Upon receiving such request, the client may choose to restart the entire unidirectional authentication process, in order to achieve a fresh shared state with the server.

Packet watermarking over IP

[0054] This section describes the systems aspects of transparently watermarking Internet Protocol packets, in a backward compatible fashion. Two orthogonal approaches are presented, which may be used independently or in tandem, to afford the greater watermarking capacity.

[0055] Data transmission over an IP network occurs in logical units, called segments, whose length is variable and is at the discretion of the sender. Depending on their length, segments may be broken down in multiple units called packets, or transmitted atomically as a single packet. Packets belonging to the same segment are reassembled at the receiving end, to reconstitute the original segment; in case of a transmission problem with one of the packets, the entire segment is discarded. In support of this mechanism, the IP protocol provides for a 16-bit segment ID field in the IP header, that is a random value attributed and attached upon creation of the segment, and that is preserved in all packets, which the

segment is broken up into, during transit. IP packet headers also contain "offset" and "length" fields, which are used to indicate the relative position of the packet within the segment, as well as a "next" flag, which is used to indicate whether the bearer is the last packet of the segment, or not. In addition to the above, IP packet headers also contain two 32-bit source and destination address fields, as well as a rarely used 8-bit TOS field (originally meant to specify terms of service options).

[0056] One exemplary method of watermarking consistent with the present invention is direct watermarking using the segment ID field. This exemplary watermarking method exploits the segment ID mechanism by substituting a watermark for the segment ID field (the specific value of which is generated according to the methods described elsewhere in this document). If the segment must be divided into several packets, all packets inherit the same watermark from the modified segment ID field, in order to comply with the requirements of the IP protocol.

[0057] On the client side, outgoing IP packets are intercepted after the segment header is constructed. The outgoing IP packets may be intercepted by, for example, communications monitoring module 120 of FIG. 1. At this stage, both the source and destination addresses are known and therefore may be used in constructing the watermark.

[0058] On the server side, the ID field of incoming segments is extracted following the stage in which complete segments are reassembled from incoming packets, but preceding the stage in which the reassembled packet is transmitted to higher-level functions for further processing (which may include operating system and application-level services). Incoming segments may be intercepted by, for example, communications monitoring module 220 of FIG. 2. The watermark may then be validated by, for example, watermark verification module 230, and the segment accordingly approved or discarded according to the teachings of the present invention.

[0059] A second exemplary method for watermarking consistent with the present invention involves fragmented watermarking using the TOS field. This watermarking approach exploits the rarely used (currently 8-bit) TOS field in IP headers, conjointly with the fragmentation mechanism, in order to provide at least 32 bits (4 bytes) of watermark per IP segment.

[0060] The method works by breaking up the target segment into a number of unambiguously ordered packets, encoding 8 bits of watermark in each of these packets. Any segment with non-empty payload may be broken into some number of unambiguously ordered packets, recognized by unique combinations of payload length, offset, and "next" flag. Exemplary types of packets include: 1) a leading packet with empty payload (hence, having length 0), offset 0, and the "next" flag set; 2) a second packet containing some or all of the actual segment payload (hence, of non-zero length), offset 0, and the "next" flag set; 3) optional packets containing the remainder of the segment payload, having non-zero length, non-zero offset, and the "next" flag set; 4) a penultimate packet with empty payload, hence, having zero length, non-zero offset, and the "next" flag set; and 5) a final packet with empty payload, hence, having zero length, non-zero offset, and the "next" flag reset.

[0061] The TOS field method may be combined with the segment ID field method to allow use of a larger number of bits of watermark data per segment. For example, at the current time, the IP protocol uses 16 bits in the segment ID field and 8 bits in the TOS field, the two methods used together would allow 24 bits (or three bytes) of data per segment to be used in the watermarking process.

Exemplary System Architecture

[0062] **FIG. 5** illustrates one embodiment of a system consistent with the present invention. In fact, any conventional computer system may be programmed to support the principles of the present invention. The system in **FIG. 5** represents a computer network 500 that comprises one or more client computers 504 and 514 and one or more servers 540 and 544 interconnected via network 502. In this specification, the terms "client" and "server" are used to refer to a computer's general role as a requester of data (client) or provider of data (server), however each computer may request data in one transaction and provide data in another transaction, thus changing the computer's role from client to server. Client 504 may also be a thin client, which is generally understood to be a network computer without a hard disk drive. Client 504 may also be a personal digital assistant ("PDA"), such as a PalmPilot, a cellular phone, or other computerized device. As shown in **FIG. 5**, client 504 may be connected to one or more servers by a suitable bus or wireless connection.

[0063] In some embodiments, a software application operating on client 504 may place a request that involves data stored on or instructions that are executed on Server A 540. Since client 504 is directly connected to Server A 540, for example, through a local area network, this request would not normally result in a transfer of data or instructions over what is shown as "network" of **FIG. 5**. The "network" of **FIG. 5** represents, for example, the Internet, which is an interconnection of networks. A different request may involve data or instructions stored on Server B 544. In this case, the data may be transferred from Server B 544 through the network to Server A 540 and, finally, to computer 502. The distance between Server A 540 and Server B 544 may be very long, e.g. across states, or very short, e.g., a few inches. Further, in traversing the network the data may be transferred through several intermediate servers and many routing devices, such as bridges and routers.

[0064] **FIG. 6** shows, in more detail, an example of a client-server system interconnected through network 600. In this

example, a server system 622 is interconnected through network 600 to client system 620. Client system 620 includes conventional components such as a processor 624, memory 625 (e.g. RAM), a bus 626 which couples processor 624 and memory 625, a mass storage device 627 (e.g. a magnetic hard disk or an optical storage disk) coupled to processor 624 and memory 625 through an I/O controller 628 and a network interface 629, such as a conventional modem.

[0065] Server system 622 also includes conventional components such as a processor 634, memory 635 (e.g. RAM), a bus 636 which couples processor 634 and memory 635, a mass storage device 637 (e.g. a magnetic or optical disk) coupled to processor 634 and memory 635 through an I/O controller 638 and a network interface 639, such as a conventional modem. It will be appreciated from the description below that the present invention may be implemented in software which is stored as executable instructions on a computer readable medium on the client and server systems, such as mass storage devices 627 and 637 respectively, or in memories 625 and 635 respectively.

[0066] Processors 624 and 634 may be microprocessors such as the Pentium® family microprocessors manufactured by Intel Corporation. However, any other suitable microprocessor, micro-, mini-, or mainframe computer, may be used. Memories 625 and 635 may include a random access memory (RAM), a read-only memory (ROM), a video memory, or mass storage. Mass storage 627 and 637 may include both fixed and removable media (e.g., magnetic, optical, or magnetic optical storage systems or other available mass storage technology). Memories 625 and 635 may contain a program, such as an operating system, an application programming interface (API), and other instructions for performing the methods consistent with the invention.

[0067] Thus, methods and systems are disclosed for providing secure transactions across a network and, more particularly, for watermarking at the packet level. The present invention may also be embodied as computer-readable media that include program instructions or program code for performing various computer-implemented operations based on the methods of the present invention. The program instructions may be those specially designed and constructed for the purposes of the invention, or they may be of the kind well-known and available to those having skill in the computer software arts. Examples of program instructions include machine code, such as produced by a compiler, and files containing a high level code that can be executed by the computer using, for example, an interpreter or equivalent execution engine to facilitate execution of high level code.

Appendix A

```
// File: gbLogicAPI.h

#ifndef _GBLOGICAPI_H
#define _GBLOGICAPI_H

/*
 * Data types
 */

// return status for all GB watermarking logic calls
typedef enum {
     GB_nil,      // unexpected error condition
     GB_ok,       // success condition
     GB_deny,     // incoming segment to be dropped
     GB_prepare,  // cliient monitor is to perform synch
     GB_reauth,   // serv. mon. to request client resynch
} GB_action_t;

// 16-bit watermark data type
typedef  struct { char bytes[ 2]; }  GB_watermark_t;

// 256-bit shared secret state agreement data type
typedef  struct { char bytes[ 32]; }  GB_agreement_t;

// opaque context for watermarking logic module
typedef  struct GB_context_s   GB_context_t;


/*
 * Housekeeping
 */
```

```
// constructor
GB_context_t * gbInitialize( );

// destructor
void gbFinalize( GB_context_t * ctx);

/*
 * Client calls
 */

// return values: GB_nil, GB_ok
GB_action_t
gbPrepareWMark( GB_context_t    * ctx,
                GB_agreement_t * data,
                ipaddr_t         src,
                ipaddr_t         dst);

// return values: GB_nil, GB_ok, GB_prepare
GB_action_t
gbWMarkOutgoing( GB_context_t    * ctx,
                 GB_watermark_t * mark,
                 ipaddr_t         src,
                 ipaddr_t         dst);

/*
 * Server calls
 */

// return values: GB_nil, GB_ok, GB_deny
GB_action_t
gbSynchronizeWMark( GB_context_t         * ctx,
                    GB_agreement_t const * data,
```

```
                    ipaddr_t                src,
                    ipaddr_t                dst);

// return values: GB_nil, GB_ok, GB_deny, GB_reauth
GB_action_t
gbWMarkIncoming( GB_context_t *          ctx,
                 GB_watermark_t const * mark,
                 ipaddr_t                src,
                 ipaddr_t                dst,
                 void const            * segment_hdr);


#endif /* _GBLOGICAPI_H */

// End of file
```

Claims

1. A method for providing secure transmissions across a network comprising a transmitting device and a receiving device, the method comprising:

   at the transmitting device, generating a stream of watermark bits;
   generating a plurality of watermarks (345) each of the plurality of watermarks comprising an index number and a portion of the stream of watermark bits;
   inserting at least one of the plurality of watermarks into each header of a plurality of outgoing packets (350);
   receiving, at the receiving device, the plurality of said outgoing packets; and
   determining (450) if a received packet is valid based on the watermark in the header of the received packet.

2. The method of claim 1, wherein said generating the stream of watermark bits includes generating a stream of watermark bits from an authorization and sychronization packet previously exchanged between the transmitting device and the receiving device.

3. The method of claim 1, further comprising activating a session by exchanging an authorization and synchronization packet between the transmitting device and the receiving device.

4. The method of claim 1, further comprising:

   discarding the packet, if the watermark is not valid.

5. The method of claim 1, wherein said determining if a received packet is valid comprises:

   comparing the watermark of the received packet to a first and a second window, each of the windows comprising a set of expected watermarks; and
   accepting the watermark as valid if the received watermark matches one of the expected watermarks in the first or second windows.

6. The method of claim 5, wherein the set of expected watermarks are generated from an authorization and sychronization packet previously exchanged between the transmitting device and the receiving device.

7. The method of claim 5, comprising:

discarding the packet, if the watermark does not match one in the first or second windows.

8. The method of claim 5, wherein said comparing the watermark further comprises:

maintaining at the server a record of a pivotal index number representing the index number of the highest-numbered valid watermark received from the transmitting device;
comparing the watermark of the received packet to a first and a second window, each of the windows comprising a set of expected watermarks and wherein the first window represents expected watermarks whose index numbers precede the pivotal index number and the second window represents expected watermarks whose index numbers immediately supercede the pivotal index number.

9. The method of claim 8, comprising:

increasing the pivotal index number if a match is found in the second window and deleting the matching expected watermark from the second window.

10. The method of claim 1, wherein the stream of watermark bits is generated by a stream cipher.

11. The method of claim 1, wherein inserting at least one of the plurality of watermarks includes determining whether a valid session exists and inserting the at least one of the plurality of watermarks only if the valid session exists.

12. A system for providing secure transmissions across a network, the system comprising:

a transmitting device (150) comprising means for
generating a stream of watermark bits;
generating a plurality of watermarks, each of the plurality of watermarks comprising an index number and a portion of the stream of watermark bits;
inserting at least one of the plurality of watermarks into each header of a plurality of outgoing packets; and
transmitting the outgoing packets to a receiving device; and a receiving device (250) comprising means for
receiving the plurality of outgoing packets; and
determining if a received packet is valid based on the watermark in the header of the received packet.

13. The system of claim 12, wherein the stream of watermark bits are generated from an authorization and synchronization packet previously exchanged between the transmitting device and the receiving device.

14. The system of claim 12, wherein said inserting at least one of the plurality of watermarks includes determining whether a valid session exists and inserting the at least one of the plurality of watermarks only if the valid session exists.

15. The system of claim 12, wherein the receiving device further discards the packet, if the watermark is not valid.

16. The system of claim 12, wherein the receiving device further determines if a received packet is valid by the watermark of the received packet to a first and a second window, each of the windows comprising a set of expected watermarks; and
accepting the received watermark as valid if the received watermark matches one of the expected watermarks in the first or second windows.

17. The system of claim 16, wherein the receiving device further discards the packet, if the received watermark does not match any expected watermarks in the first or second windows.

18. The system of claim 16, wherein said comparing the watermark further comprises:

maintaining at the server a record of a pivotal index number representing the index number of the highest-num-

bered valid watermark received from the transmitting device;
comparing the watermark of the received packet to a first and a second window, each of the windows comprising a set of expected waternaarks and wherein the first window represents expected watermarks whose index numbers precede the pivotal index number and the second window represents expected watermarks whose index numbers immediately supercede the pivotal index number.

19. The system of claim 17, wherein the receiving device increases the pivotal index number if a match is found in the second window and deletes the matching expected watermark from the second window.

20. The method of claim 12, wherein the stream of watermark bits is generated by a stream cipher.

21. A device (150) for providing secure transmissions across a network, the comprising:

means for generating a stream of watermark bits;
means (345) for generating a plurality of watermarks, each of the plurality of watermarks comprising an index number and a portion of the stream of watermark bits;
means for inserting at least one of the plurality of watermarks into each header of a plurality of outgoing packets; and
means for transmitting the outgoing packets to a receiving device (250) capable of determining if a received packet is valid based on the watermark in the header of the received packet.

Patentansprüche

1. Verfahren zum Bereitstellen von sicheren Übertragungen über ein Netzwerk mit einer Übertragungsvorrichtung und einer Empfangsvorrichtung, wobei in dem Verfahren:

in der Übertragungsvorrichtung ein Strom von Wasserzeichen-Bits erzeugt wird;
mehrere Wasserzeichen erzeugt (345) werden, die jeweils eine Indexnummer und einen Abschnitt des Stroms von Wasserzeichen-Bits aufweisen;
wenigstens eines der mehreren Wasserzeichen in jeden Kopfteil von mehreren ausgehenden Paketen eingesetzt (350) wird;
in der Empfangsvorrichtung die mehreren ausgehenden Pakete empfangen werden; und
auf Grundlage des Wasserzeichens im Kopfteil des empfangenen Pakets bestimmt (450) wird, ob das empfangene Paket gültig ist.

2. Verfahren nach Anspruch 1, wobei beim Erzeugen des Stroms von Wasserzeichen-Bits ein Strom von Wasserzeichen-Bits aus einem Autorisierungs- und Synchronisations-Paket erzeugt wird, das zuvor zwischen der Übertragungsvorrichtung und der Empfangsvorrichtung ausgetauscht wurde.

3. Verfahren nach Anspruch 1, wobei ferner eine Sitzung aktiviert wird, indem ein Autorisierungs- und Synchronisations-Paket zwischen der Übertragungsvorrichtung und der Empfangsvorrichtung ausgetauscht wird.

4. Verfahren nach Anspruch 1, wobei ferner:

das Paket verworfen wird, wenn das Wasserzeichen nicht gültig ist.

5. Verfahren nach Anspruch 1, wobei beim Bestimmen, ob ein empfangenes Paket gültig ist:

das Wasserzeichen des empfangenen Pakets mit einem ersten und einem zweiten Fenster verglichen wird, wobei jedes Fenster eine Reihe erwarteter Wasserzeichen aufweist; und
das Wasserzeichen als gültig akzeptiert wird, wenn das empfangene Wasserzeichen mit einem der erwarteten Wasserzeichen in dem ersten oder dem zweiten Fenster übereinstimmt.

6. Verfahren nach Anspruch 5, wobei die Reihe erwarteter Wasserzeichen aus einem Autorisierungs- und Synchronisations-Paket erzeugt wird, das zuvor zwischen der Übertragungsvorrichtung und der Empfangsvorrichtung ausgetauscht wurde.

7. Verfahren nach Anspruch 5, wobei:

das Paket verworfen wird, wenn das Wasserzeichen nicht mit einem in dem ersten oder dem zweiten Fenster übereinstimmt.

8. Verfahren nach Anspruch 5, wobei beim Vergleichen der Wasserzeichen ferner:

im Server eine Aufzeichnung einer zentralen Indexnummer beibehalten wird, die die Indexnummer des gültigen Wasserzeichens mit der höchsten Nummer darstellt, das von der Übertragungsvorrichtung empfangen wurde;
das Wasserzeichen des empfangenen Pakets mit einem ersten und einem zweiten Fenster verglichen wird, wobei jedes Fenster eine Reihe erwarteter Wasserzeichen aufweist, und wobei das erste Fenster erwartete Wasserzeichen darstellt, deren Indexnummern der zentralen Indexnummer vorausgehen, und das zweite Fenster erwartete Wasserzeichen darstellt, deren Indexnummern die zentrale Indexnummer unmittelbar ersetzen.

9. Verfahren nach Anspruch 8, wobei:

die zentrale Indexnummer erhöht wird, wenn eine Übereinstimmung in dem zweiten Fenster gefunden wird, und das übereinstimmende erwartete Wasserzeichen aus dem zweiten Fenster gelöscht wird.

10. Verfahren nach Anspruch 1, wobei der Strom von Wasserzeichen-Bits durch eine Stromverschlüsselung erzeugt wird.

11. Verfahren nach Anspruch 1, wobei beim Einsetzen wenigstens eines der mehreren Wasserzeichen bestimmt wird, ob eine gültige Sitzung vorliegt, und das wenigstens eine der mehreren Wasserzeichen nur eingesetzt wird, wenn die gültige Sitzung vorliegt.

12. System zum Bereitstellen von sicheren Übertragungen über ein Netzwerk, wobei das System aufweist:

eine Übertragungsvorrichtung (150) mit einer Einrichtung, um
einen Strom von Wasserzeichen-Bits zu erzeugen,
mehrere Wasserzeichen zu erzeugen, die jeweils eine Indexnummer und einen Abschnitt des Stroms von Wasserzeichen-Bits aufweisen,
wenigstens eines der mehreren Wasserzeichen in jeden Kopfteil von mehreren ausgehenden Paketen einzusetzen, und
die ausgehenden Pakete an eine Empfangsvorrichtung zu übertragen; und
eine Empfangsvorrichtung (250) mit einer Einrichtung, um
die mehreren ausgehenden Pakete zu empfangen, und
auf Grundlage des Wasserzeichens im Kopfteil des empfangenen Pakets zu bestimmen, ob das empfangene Paket gültig ist.

13. System nach Anspruch 12, wobei der Strom von Wasserzeichen-Bits aus einem Autorisierungs- und Synchronisations-Paket erzeugt wird, das zuvor zwischen der Übertragungsvorrichtung und der Empfangsvorrichtung ausgetauscht wurde.

14. System nach Anspruch 12, wobei beim Einsetzen wenigstens eines der mehreren Wasserzeichen bestimmt wird, ob eine gültige Sitzung vorliegt und das wenigstens eine der mehreren Wasserzeichen nur eingesetzt wird, wenn die gültige Sitzung vorliegt.

15. System nach Anspruch 12, wobei die Empfangsvorrichtung ferner das Paket verwirft, wenn das Wasserzeichen nicht gültig ist.

16. System nach Anspruch 12, wobei die Empfangsvorrichtung ferner bestimmt, ob ein empfangenes Paket gültig ist, indem sie das Wasserzeichen des empfangenen Pakets mit einem ersten und einem zweiten Fenster vergleicht, wobei jedes Fenster eine Reihe erwarteter Wasserzeichen aufweist; und
das Wasserzeichen als gültig akzeptiert wird, wenn das empfangene Wasserzeichen mit einem der erwarteten Wasserzeichen in dem ersten oder dem zweiten Fenster übereinstimmt.

17. System nach Anspruch 16, wobei die Empfangsvorrichtung ferner das Paket verwirft, wenn das empfangene Was-

serzeichen mit keinem der erwarteten Wasserzeichen in dem ersten oder dem zweiten Fenster übereinstimmt.

18. System nach Anspruch 16, wobei beim Vergleichen der Wasserzeichen ferner:

im Server eine Aufzeichnung einer zentralen Indexnummer beibehalten wird, die die Indexnummer des gültigen Wasserzeichens mit der höchsten Nummer darstellt, das von der Übertragungsvorrichtung empfangen wurde; das Wasserzeichen des empfangenen Pakets mit einem ersten und einem zweiten Fenster verglichen wird, wobei jedes Fenster eine Reihe erwarteter Wasserzeichen aufweist, und wobei das erste Fenster erwartete Wasserzeichen darstellt, deren Indexnummern der zentralen Indexnummer vorausgehen, und das zweite Fenster erwartete Wasserzeichen darstellt, deren Indexnummern die zentrale Indexnummer unmittelbar ersetzen.

19. System nach Anspruch 17, wobei die Empfangsvorrichtung die zentrale Indexnummer erhöht, wenn eine Übereinstimmung in dem zweiten Fenster gefunden wird, und das übereinstimmende erwartete Wasserzeichen aus dem zweiten Fenster löscht.

20. System nach Anspruch 12, wobei der Strom von Wasserzeichen-Bits durch eine Stromverschlüsselung erzeugt wird.

21. Vorrichtung (150) zum Bereitstellen von sicheren Übertragungen über ein Netzwerk, wobei die Vorrichtung aufweist:

eine Einrichtung zum Erzeugen eines Stroms von Wasserzeichen-Bits,
eine Einrichtung zum Erzeugen (345) mehrerer Wasserzeichen, die jeweils eine Indexnummer und einen Abschnitt des Stroms von Wasserzeichen-Bits aufweisen,
eine Einrichtung zum Einsetzen wenigstens eines der mehreren Wasserzeichen in jeden Kopfteil von mehreren ausgehenden Paketen, und
eine Einrichtung zum Übertragen der ausgehenden Pakete an eine Empfangsvorrichtung (250), die dazu ausgelegt ist, auf Grundlage des Wasserzeichens im Kopfteil des empfangenen Pakets zu bestimmen, ob ein empfangenes Paket gültig ist.

Revendications

1. Procédé d'établissement de transmissions sécurisées sur un réseau comprenant un dispositif d'émission et un dispositif de réception, le procédé consistant à :

sur le dispositif d'émission, produire un flux de bits de filigrane ;
produire une pluralité de filigranes (345), chacun de la pluralité de filigranes comprenant un numéro d'index et une partie du flux de bits de filigrane ;
insérer au moins l'un de la pluralité de filigranes dans chaque en-tête d'une pluralité de paquets sortants (350) ;
recevoir, sur le dispositif de réception, la pluralité desdits paquets sortants ; et
déterminer (450) si un paquet reçu est valide sur la base du filigrane dans l'en-tête du paquet reçu.

2. Procédé selon la revendication 1, dans lequel ladite génération du flux de bits de filigrane consiste à générer un flux de bits de filigrane à partir d'un paquet d'autorisation et de synchronisation précédemment échangé entre le dispositif d'émission et le dispositif de réception.

3. Procédé selon la revendication 1, consistant en outre à activer une session en échangeant un paquet d'autorisation et de synchronisation entre le dispositif d'émission et le dispositif de réception.

4. Procédé selon la revendication 1, consistant en outre :

à rejeter le paquet si le filigrane n'est pas valide.

5. Procédé selon la revendication 1, dans lequel ladite opération consistant à déterminer si un paquet reçu est valide consiste à :

comparer le filigrane du paquet reçu à une première et à une seconde fenêtre, chacune des fenêtres comprenant un ensemble de filigranes attendus ; et
accepter le filigrane comme étant valide si le filigrane reçu concorde avec l'un des filigranes attendus dans la

première ou la seconde fenêtre.

6. Procédé selon la revendication 5, dans lequel l'ensemble de filigranes attendus est généré à partir d'un paquet d'autorisation et de synchronisation précédemment échangé entre le dispositif d'émission et le dispositif de réception.

7. Procédé selon la revendication 5, consistant à :

rejeter le paquet si le filigrane ne concorde pas avec l'une de la première ou de la seconde fenêtre.

8. Procédé selon la revendication 5, dans lequel ladite comparaison du filigrane consiste en outre à :

maintenir sur le serveur un enregistrement d'un numéro d'index de pivotement représentant le numéro d'index du filigrane valide de numéro le plus haut reçu du dispositif d'émission ;
comparer le filigrane du paquet reçu à une première et à une seconde fenêtres, chacune des fenêtres comprenant un ensemble de filigranes attendus et dans lequel la première fenêtre représente des filigranes attendus dont les numéros d'index précèdent le numéro d'index de pivotement et la seconde fenêtre représente des filigranes attendus dont les numéros d'index sont immédiatement supérieurs au numéro d'index de pivotement.

9. Procédé selon la revendication 8, consistant à :

augmenter le numéro d'index de pivotement si une concordance est trouvée dans la seconde fenêtre et éliminer le filigrane attendu concordant de la seconde fenêtre.

10. Procédé selon la revendication 1, dans lequel le flux de bits de filigrane est généré par un chiffrement de flux par un système de chiffrement continu.

11. Procédé selon la revendication 1, dans lequel l'insertion d'au moins l'un de la pluralité de filigranes consisté à déterminer si une session valide existe et à n'insérer l'au moins un de la pluralité de filigranes que si la session valide existe.

12. Système pour effectuer des transmissions sécurisées sur un réseau, le système comprenant :

un dispositif d'émission (150) comprenant des moyens pour :

générer un flux de bits de filigrane ;
générer une pluralité de filigranes, chacun de la pluralité de filigranes comprenant un numéro d'index et une partie du flux de bits de filigrane ;
insérer au moins l'un de la pluralité de filigranes dans chaque en-tête d'une pluralité de paquets sortants; et
émettre les paquets sortants vers un dispositif de réception ; et
un dispositif de réception (250) comprenant des moyens pour :

recevoir la pluralité de paquets sortants ; et
déterminer si un paquet reçu est valide sur la base du filigrane dans l'en-tête du paquet reçu.

13. Système selon la revendication 12, dans lequel le flux de bits de filigrane est généré à partir d'un paquet d'autorisation et de synchronisation précédemment échangé entre le dispositif d'émission et le dispositif de réception.

14. Système selon la revendication 12, dans lequel ladite insertion d'au moins l'un de la pluralité de filigranes consiste à déterminer si une session valide existe et à n'insérer l'au moins un de la pluralité de filigranes que si la session valide existe.

15. Système selon la revendication 12, dans lequel le dispositif de réception rejette en outre le paquet si le filigrane n'est pas valide.

16. Système selon la revendication 12, dans lequel le dispositif de réception détermine en outre si un paquet reçu est valide en comparant le filigrane du paquet reçu à une première et à une seconde fenêtre, chacune des fenêtres comprenant un ensemble de filigranes attendus ; et
en acceptant le filigrane reçu comme étant valide si le filigrane reçu concorde avec l'un des filigranes attendus dans

les première ou seconde fenêtres.

17. Système selon la revendication 16, dans lequel le dispositif de réception rejette en outre le paquet si le filigrane reçu ne concorde pas avec l'un quelconque des filigranes dans la première ou de la seconde fenêtre.

18. Système selon la revendication 16, dans lequel ladite comparaison du filigrane consiste en outre à :

maintenir sur le serveur un enregistrement d'un numéro d'index de pivotement représentant le numéro d'index du filigrane valide de numéro le plus élevé reçu du dispositif d'émission ;
comparer le filigrane du paquet reçu à une première et à une seconde fenêtre, chacune des fenêtres comprenant un ensemble de filigranes attendus et dans lequel la première fenêtre représente des filigranes attendus dont les numéros d'index précèdent le numéro d'index de pivotement et la seconde fenêtre représente des filigranes attendus dont les numéros d'index sont immédiatement supérieurs au numéro d'index de pivotement.

19. Système selon la revendication 17, dans lequel le dispositif de réception incrémente le numéro d'index de pivotement si une concordance est trouvée dans la seconde fenêtre et élimine le filigrane attendu concordant de la seconde fenêtre.

20. Procédé selon la revendication 12, dans lequel le flux de bits de filigrane est généré par un système de chiffrement continu.

21. Dispositif (150) pour effectuer des transmissions sécurisées sur un réseau, le dispositif comprenant :

des moyens pour générer un flux de bits de filigrane ;
des moyens (345) pour générer une pluralité de filigranes, chacun de la pluralité de filigranes comprenant un numéro d'index et une partie du flux de bits de filigrane ;
des moyens pour insérer au moins l'un de la pluralité de filigranes dans chaque en-tête d'une pluralité de paquets sortants ; et
des moyens pour transmettre les paquets sortants à un dispositif de réception (250) capable de déterminer si un paquet reçu est valide sur la base du filigrane dans l'en-tête du paquet reçu.

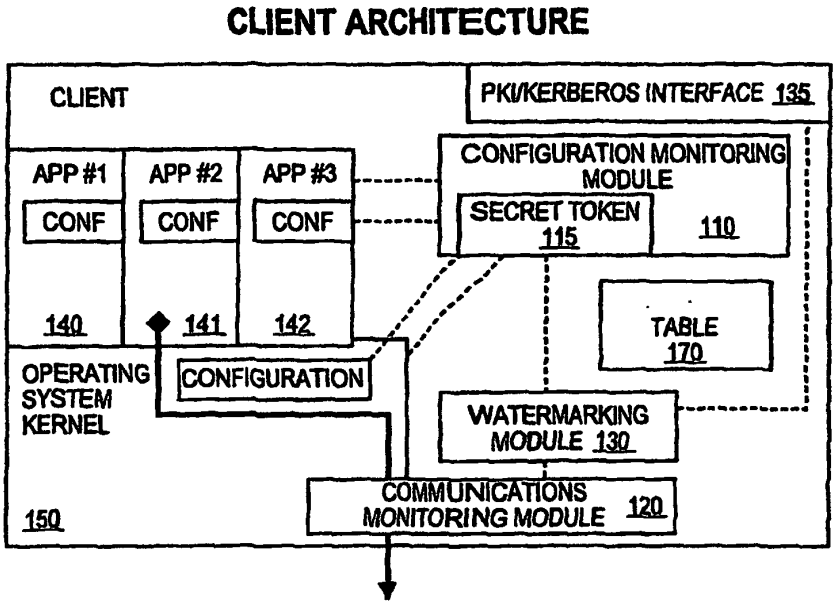

CLIENT ARCHITECTURE
CLIENT
PKI/KERBEROS INTERFACE 135
APP #1
APP #2
APP #3
CONF
CONF
CONF
CONFIGURATION MONITORING MODULE
SECRET TOKEN 115
110
140
141
142
TABLE 170
OPERATING SYSTEM KERNEL
CONFIGURATION
WATERMARKING MODULE 130
COMMUNICATIONS MONITORING MODULE 120
150

FIG. 1

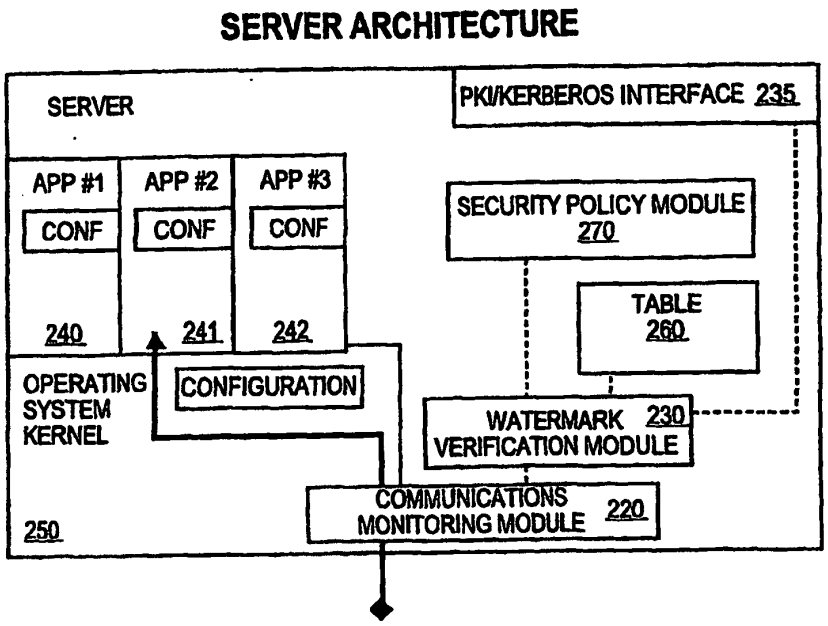

SERVER ARCHITECTURE
SERVER
PKI/KERBEROS INTERFACE 235
APP #1
APP #2
APP #3
CONF
CONF
CONF
240
241
242
SECURITY POLICY MODULE 270
TABLE 260
OPERATING SYSTEM KERNEL
CONFIGURATION
WATERMARK VERIFICATION MODULE 230
COMMUNICATIONS MONITORING MODULE 220
250

FIG. 2

OUTGOING PACKET WATERMARKING

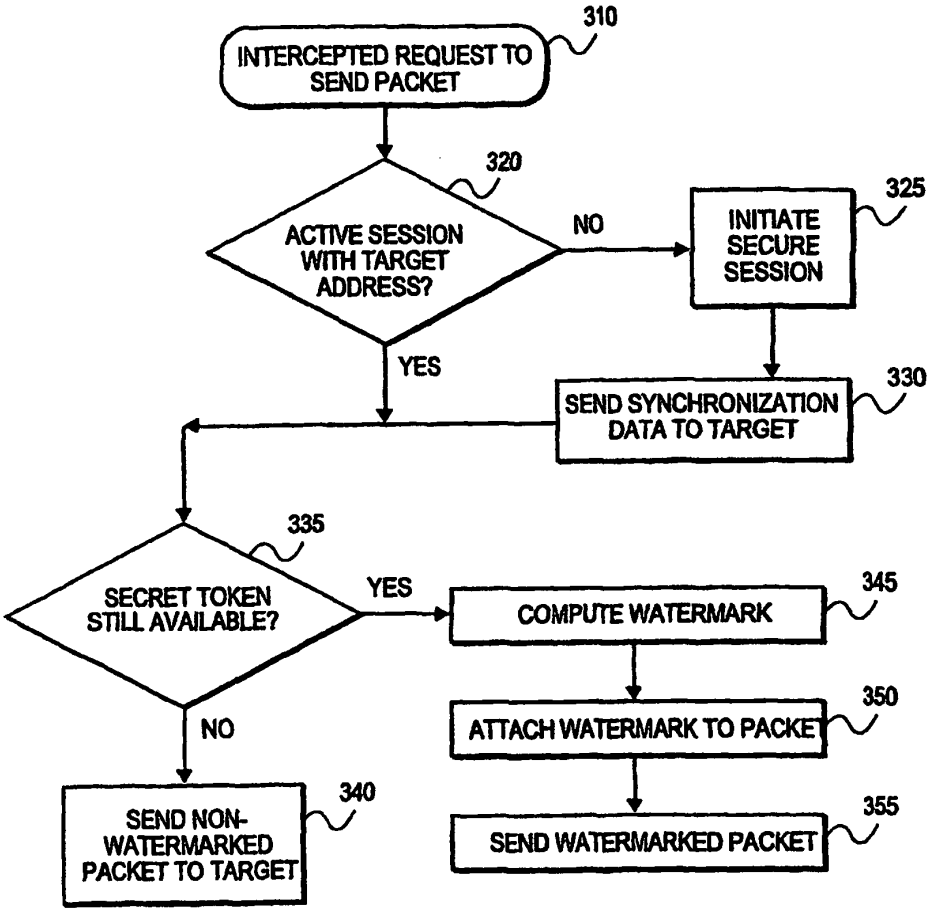


FIG. 3

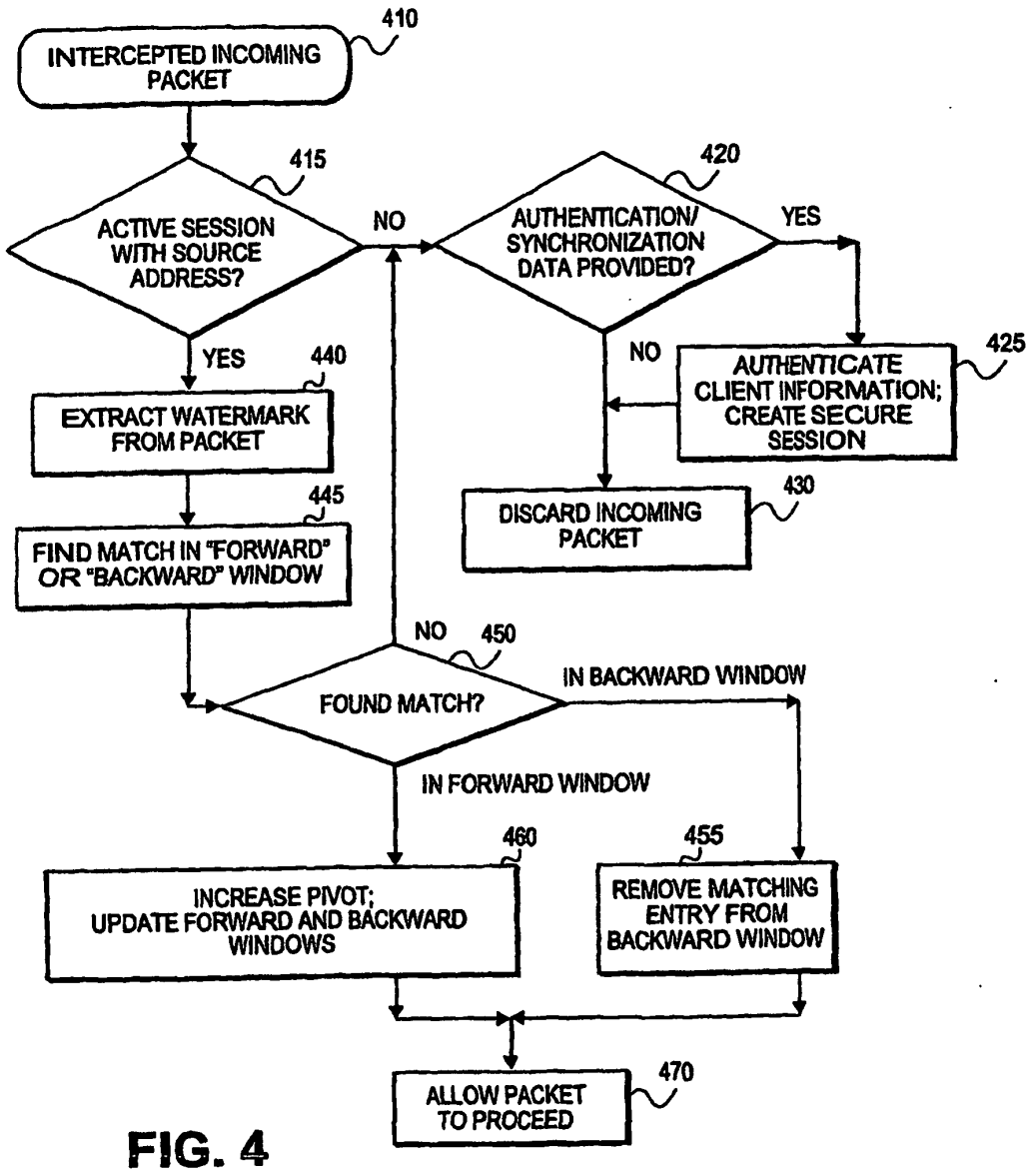

INCOMING PACKET WATERMARK VERIFICATION
410
INTERCEPTED INCOMING PACKET
415
ACTIVE SESSION WITH SOURCE ADDRESS?
NO
420
AUTHENTICATION/ SYNCHRONIZATION DATA PROVIDED?
YES
YES
440
EXTRACT WATERMARK FROM PACKET
NO
425
AUTHENTICATE CLIENT INFORMATION; CREATE SECURE SESSION
445
FIND MATCH IN "FORWARD" OR "BACKWARD" WINDOW
DISCARD INCOMING PACKET
430
NO
450
FOUND MATCH?
IN BACKWARD WINDOW
IN FORWARD WINDOW
460
INCREASE PIVOT; UPDATE FORWARD AND BACKWARD WINDOWS
455
REMOVE MATCHING ENTRY FROM BACKWARD WINDOW
ALLOW PACKET TO PROCEED
470

FIG. 4

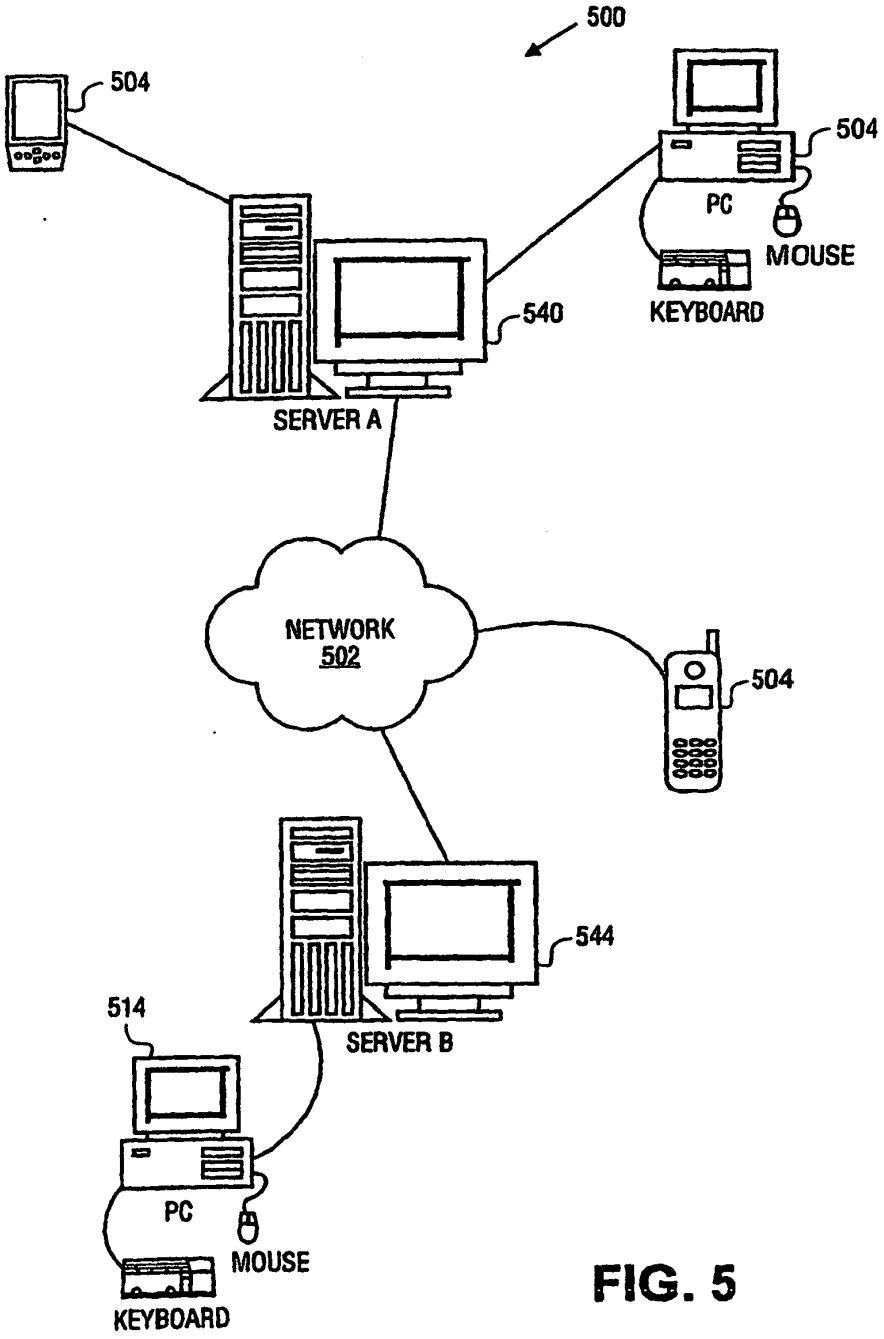

500
504
504
PC
MOUSE
KEYBOARD
540
SERVER A
NETWORK
502
504
544
514
SERVER B
PC
MOUSE
KEYBOARD

FIG. 5

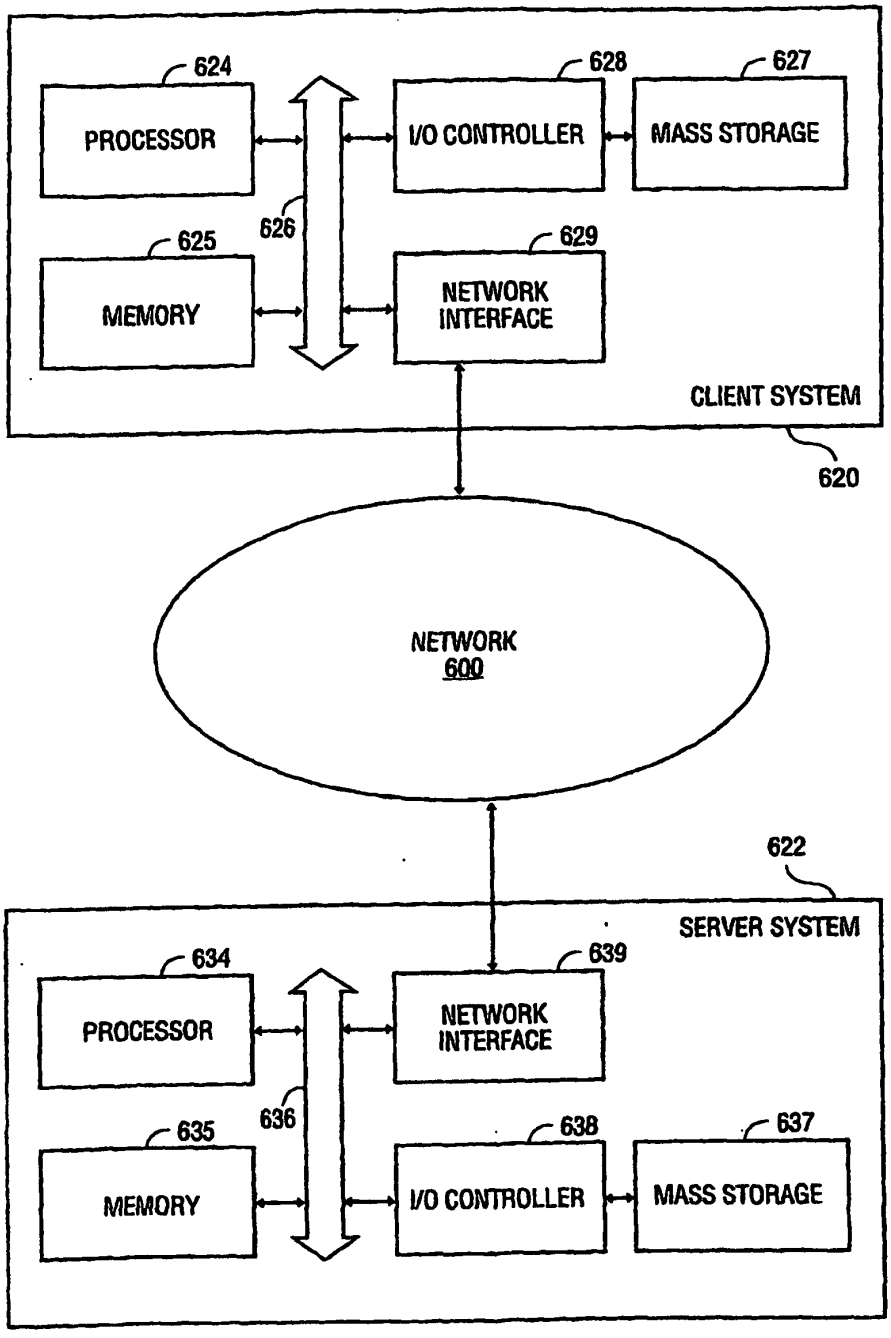

624
PROCESSOR
628
I/O CONTROLLER
627
MASS STORAGE
626
625
MEMORY
629
NETWORK INTERFACE
CLIENT SYSTEM
620
NETWORK
600
622
SERVER SYSTEM
634
PROCESSOR
639
NETWORK INTERFACE
636
635
MEMORY
638
I/O CONTROLLER
637
MASS STORAGE

FIG. 6

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 354 276 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
12.12.2007 Bulletin 2007/50

(21) Application number: **01985137.7**

(22) Date of filing: **26.10.2001**

(51) Int Cl.:
G10L 19/00 *(2006.01)*

(86) International application number:
PCT/US2001/050295

(87) International publication number:
WO 2002/037316 (10.05.2002 Gazette 2002/19)

(54) **METHOD AND APPARATUS FOR CREATING A UNIQUE AUDIO SIGNATURE**

VERFAHREN UND VORRICHTUNG ZUM ERZEUGEN VON EINDEUTIGEN AUDIOSIGNATUREN

PROCEDE ET APPAREIL DE CREATION D'UNE SIGNATURE AUDIO UNIQUE

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

(30) Priority: **03.11.2000 US 706227**

(43) Date of publication of application:
22.10.2003 Bulletin 2003/43

(73) Proprietor: **Audible Magic Corporation**
Los Gatos, CA 95032 (US)

(72) Inventors:
- **WOLD, Erling, H.**
  El Cerrito, CA 94530 (US)
- **BLUM, Thomas, L.**
  San Francisco, CA 94109 (US)
- **KEISLAR, Douglas, F.**
  Berkeley, CA 94708 (US)
- **WHEATON, James, A.**
  Fairfax, CA 94930 (US)

(74) Representative: **Leeming, John Gerard**
J.A. Kemp & Co.
14 South Square
Gray's Inn
London WC1R 5JJ (GB)

(56) References cited:
US-A- 5 210 820
US-A- 5 983 176
US-A- 6 096 961

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention)

EP 1 354 276 B1

Description

[0001] The present invention relates to data communications. In particular, the present invention relates to creating a unique audio signature.

[0002] Digital audio technology has greatly changed the landscape of music and entertainment. Rapid increases in computing power coupled with decreases in cost have made it possible individuals to generate finished products having a quality once available only in a major studio. Once consequence of modern technology is that legacy media storage standards, such as reel-to-reel tapes, are being rapidly replaced by digital storage media, such as the Digital Versatile Disk (DVD), and Digital Audio Tape (DAT). Additionally, with higher capacity hard drives standard on most personal computers, home users may now store digital files such as audio or video tracks on their home computers.

[0003] Furthermore, the Internet has generated much excitement, particularly among those who see the Internet as an opportunity to develop new avenues for artistic expression and communication. The Internet has become a virtual gallery, where artists may post their works on a Web page. Once posted, the works may be viewed by anyone having access to the Internet.

[0004] One application of the Internet that has received considerable attention is the ability to transmit recorded music over the Internet. Once music has been digitally encoded into a file, the file may be both downloaded by users for play, or broadcast ("streamed") over the Internet. When files are streamed, they may be listened to by Internet users in a manner much like traditional radio stations.

[0005] Given the widespread use of digital media, digital audio files, or digital video files containing audio information, may need to be identified. The need for identification of digital files may arise in a variety of situations. For example, an artist may wish to verify royalty payments or generate their own Arbitron®-like ratings by identifying how often their works are being streamed or downloaded. Additionally, users may wish to identify a a particular work. The prior art has made efforts to create methods for identifying digital audio works.

[0006] However, systems of the prior art suffer from certain disadvantages. For example, prior art systems typically create a reference signature by examining the copyrighted work as a whole, and then creating a signature based upon the audio characteristics of the entire work. However, examining a work in total can result in a signature may not accurately represent the original work. Often, a work may have distinctive passages which may not be reflected in a signature based upon the total work. Furthermore, often works are electronically processed prior to being streamed or downloaded, in a manner that may affect details of the work's audio characteristics, which may result in prior art systems missing the identification of such works. Examples of such electronic processing include data compression and various sorts of audio signal processing such as equalization.

[0007] US 5,918,223 discloses a method for determining a work in which the work is segmented, a signature generated and compared to a reference signature to determine if the work is known.

[0008] Hence, there exists a need to provide a system which overcomes the disadvantages of the prior art.

[0009] The present invention relates to data communications. In particular, the present invention relates to creating a unique audio signature.

[0010] According to a first aspect of the invention there is provided a method for determining an identity of a sampled work, said method comprising receiving data of a sampled work, segmenting said data of said sampled work into a plurality of segments wherein each of said segments has predetermined segment size and a predetermined hop size, creating a signature of said sample work based upon said plurality of segments, comparing said signature of said sampled work to a plurality of signatures of reference works, and determining said sampled work is one of said reference works based upon said comparison, said method characterized in that said predetermined hop size of said segments of said sampled work signature is chosen to be less than said hop size of each of said plurality of reference signatures.

[0011] According to a further aspect of the invention there is provided an apparatus that determines an identity of a sampled work, said apparatus comprising circuitry configured to receive data of a sampled work, circuitry configured to segment said data of said sampled work into a plurality of segments wherein each of said segments has predetermined segment size and a predetermined hop size, circuitry configured to create a signature of said sampled work based upon said plurality of segments, circuitry configured to compare said signature of said sampled work to a plurality of signatures of reference works, and circuitry configured to determine said sampled work is one of said reference works based upon said comparison, said apparatus characterized in that said predetermined hop size of said segments of said sampled work signature is chosen to be less than said hop size of each of said plurality of reference signatures.

[0012] According to a further aspect of the invention there is provided a program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method as described above.

Figure 1 is a flowchart of a method according to the present invention.

Figure 2 is a diagram of a system suitable for use with the present invention.

Figure 3 is a diagram of segmenting according to the present invention.

Figure 4 is a detailed diagram of segmenting according to the present invention showing hop size.

Figure 5 is a graphical flowchart showing the creating of a segment feature vector according to the present invention.
Figure 6 is a diagram of a signature according to the present invention.
Figure 7 is a functional diagram of a comparison process according to the present invention.

[0013] Persons of ordinary skill in the art will realize that the following description of the present invention is illustrative only and not in any way limiting. Other embodiments of the invention will readily suggest themselves to such skilled persons having the benefit of this disclosure.

[0014] It is contemplated that the present invention may be embodied in various computer and machine-readable data structures. Furthermore, it is contemplated that data structures embodying the present invention will be transmitted across computer and machine-readable media, and through communications systems by use of standard protocols such as those used to enable the Internet and other computer networking standards.

[0015] The invention further relates to machine-readable media on which are stored embodiments of the present invention. It is contemplated that any media suitable for storing instructions related to the present invention is within the scope of the present invention. By way of example, such media may take the form of magnetic, optical, or semiconductor media.

[0016] The present invention may be described through the use of flowcharts. Often, a single instance of an embodiment of the present invention will be shown. As is appreciated by those of ordinary skill in the art, however, the protocols, processes, and procedures described herein may be repeated continuously or as often as necessary to satisfy the needs described herein. Accordingly, the representation of the present invention through the use of flowcharts should not be used to limit the scope of the present invention.

[0017] The present invention may also be described through the use of web pages in which embodiments of the present invention may be viewed and manipulated. It is contemplated that such web pages may be programmed with web page creation programs using languages standard in the art such as HTML or XML. It is also contemplated that the web pages described herein may be viewed and manipulated with web browsers running on operating systems standard in the art, such as the Microsoft Windows® and Macintosh@ versions of Internet Explorer® and Netscape®. Furthermore, it is contemplated that the functions performed by the various web pages described herein may be implemented through the use of standard programming languages such a Java® or similar languages.

[0018] The present invention will first be described in general overview. Then, each element will be described in further detail below.

[0019] Referring now to Figure 1, a flowchart is shown which provides a general overview of the present invention. The present invention may be viewed as three steps: 1) receiving a sampled work; 2) segmenting the work; 3) creating signatures of the segments; and 4) storing the signatures of the segments.

Receiving a sampled work

[0020] Beginning with act 100, a sampled work is provided to the present invention. It is contemplated that the work will be provided to the present invention as a digital audio stream.

[0021] It should be understood that if the audio is in analog form, it may be digitized in a manner standard in the art.

Segmenting the work

[0022] After the sampled worked is received, the work is then segmented in act 102. It is contemplated that the sampled work may be segmented into predetermined lengths. Though segments may be of any length, the segments of the present invention are preferably of the same length.

[0023] In an exemplary non-limiting embodiment of the present invention, the segment lengths are in the range of 0.5 to 3 seconds. It is contemplated that if one were searching for very short sounds (e.g., sound effects such as gunshots), segments as small as 0.01 seconds may be used in the present invention. Since humans don't resolve audio changes below about 0.018 seconds, segment lengths less than 0.018 seconds may not be useful. On the other hand, segment lengths as high as 30-60 seconds may be used in the present invention. The inventors have found that beyond 30-60 seconds may not be useful, since most details in the signal tend to average out.

Generating signatures

[0024] Next, in act 104, each segment is analyzed to produce a signature, known herein as a segment feature vector. It is contemplated that a wide variety of methods known in the art may be used to analyze the segments and generate segment feature vectors. In an exemplary non-limiting embodiment of the present invention, the segment feature vectors may be created using the method described in US Patent #5,918,223 to Blum.

Storing the signatures

[0025] In act 106, the segment feature vectors are stored to create a representative signature of the sampled work.

[0026] Each above-listed step will now be shown and described in detail.

[0027] Referring now to Figure 2, a diagram of a system suitable for use with the present invention is shown. FIG. 2 includes a client system 200. It is contemplated that client system 200 may comprise a personal computer 202 including hardware and software standard in the art to run an operating system such as Microsoft Windows®, MAC OS®, or other operating systems standard in the art. Client system 200 may further include a database 204 for storing and retrieving embodiments of the present invention. It is contemplated that database 204 may comprise hardware and software standard in the art and may be operatively coupled to PC 202. Database 204 may also be used to store and retrieve the works and segments utilized by the present invention.

[0028] Client system 200 may further include an audio/video (A/V) input device 208. A/V device 208 is operatively coupled to PC 202 and is configured to provide works to the present invention which may be stored in traditional audio or video formats. It is contemplated that A/V device 208 may comprise hardware and software standard in the art configured to receive and sample audio works (including video containing audio information), and provide the sampled works to the present invention as digital audio files. Typically, the A/V input device 208 would supply raw audio samples in a format such as 16-bit stereo PCM format. A/V input device 208 provides an example of means for receiving a sampled work.

[0029] It is contemplated that sampled works may be obtained over the Internet, also. Typically, streaming media over the Internet is provided by a provider, such as provider 218 of FIG. 2. Provider 218 includes a streaming application server 220, configured to retrieve works from database 222 and stream the works in a formats standard in the art, such as Real®, Windows Media®, or QuickTime.® The server then provides the streamed works to a web server 224, which then provides the streamed work to the Internet 214 through a gateway 216. Internet 214 may be any packet-based network standard in the art, such as IP, Frame Relay, or ATM.

[0030] To reach the provider 218, the present invention may utilize a cable or DSL head end 212 standard in the art operatively, which is coupled to a cable modem or DSL modem 210 which is in turn coupled to the system's network 206. The network 206 may be any network standard in the art, such as a LAN provided by a PC 202 configured to run software standard in the art.

[0031] It is contemplated that the sampled work received by system 200 may contain audio information from a variety of sources known in the art, including, without limitation, radio, the audio portion of a television broadcast, Internet radio, the audio portion of an Internet video program or channel, streaming audio from a network audio server, audio delivered to personal digital assistants over cellular or wireless communication systems, or cable and satellite broadcasts.

[0032] Additionally, it is contemplated that the present invention may be configured to receive and compare segments coming from a variety of sources either stored or in real-time. For example, it is contemplated that the present invention may compare a real-time streaming work coming from streaming server 218 or A/V device 208 with a reference segment stored in database 204.

[0033] Figure 3 shows a diagram showing the segmenting of a work according to the present invention. FIG. 3 includes audio information 300 displayed along a time axis 302. FIG. 3 further includes a plurality of segments 304, 306, and 308 taken of audio information 300 over some segment size T.

[0034] In an exemplary non-limiting embodiment of the present invention, instantaneous values of a variety of acoustic features are computed at a low level, preferably about 100 times a second. Additionally, 10 MFCCs (cepstral coefficients) are computed for each segment. It is contemplated that any number of MFCCs may be computed. Preferably, 5-20 MFCCs are computed, however, as many as 30 MFCCs may be computed, depending on the need for accuracy versus speed.

[0035] In an exemplary non-limiting embodiment of the present invention, the segment-level acoustical features comprise statistical measures as disclosed in the '223 patent of these low-level features calculated over the length of each segment. The data structure may store other bookkeeping information as well (segment size, hop size, item ID, UPC, etc).

[0036] As can be seen by inspection of FIG. 3, the segments 304, 306, and 308 may overlap in time. This amount of overlap may be represented by measuring the time between the center point of adjacent segments. This amount of time is referred to herein as the hop size of the segments, and is so designated in FIG. 3. By way of example, if the segment length T of a given segment is one second, and adjacent segments overlap by 50%, the hop size would be 0.5 second.

[0037] The hop size may be set during the development of the software. Additionally, the hop sizes of the reference database and the real-time segments may be predetermined to facilitate compatibility. For example, the reference signatures in the reference database may be precomputed with a fixed hop and segment size, and thus the client applications should conform to this segment size and have a hop size which integrally divides the reference signature hop size. It is contemplated that one may experiment with a variety of segment sizes in order to balance the tradeoff of accuracy with speed of computation for a given application.

[0038] The inventors have found that by carefully choosing the hop size of the segments, the accuracy of the identi-

fication process may be significantly increased. Additionally, the inventors have found that the accuracy of the identification process may be increased if the hop size of reference segments and the hop size of segments obtained in real-time are each chosen independently. The importance of the hop size of segments may be illustrated by examining the process for segmenting pre-recorded works and real-time works separately.

Reference signatures

[0039] Prior to attempting to identify a given work, a reference database of signatures must be created. When building a reference database, a segment length having a period of less than three seconds is preferred. In an exemplary non-limiting embodiment of the present invention, the segment lengths have a period ranging from 0.5 seconds to 3 seconds. For a reference database, the inventors have found that a hop size of approximately 50% to 100% of the segment size is preferred.

[0040] It is contemplated that the reference signatures may be stored on a database such as database 204 as described above. Database 204 and the discussion herein provide an example of means for providing a plurality of reference signatures each having a segment size and a hop size.

Real-time signatures

[0041] The choice of the hop size is important for real-time segments.

[0042] Figure 4 shows a detailed diagram of a real-time segment according to the present invention. FIG. 4 includes real-time audio information 400 displayed along a time axis 402. FIG. 4 further includes segments 404 and 406 taken of audio information 400 over some segment length T. In an exemplary non-limiting embodiment of the present invention, the segment length of real-time segments is chosen to range from 0.5 to 3 seconds.

[0043] As can be seen by inspection of FIG. 4, the hop size of real-time is chosen to be smaller than that of reference segments. In an exemplary non-limiting embodiment of the present invention, the hop size of real-time segments is less than 50% of the segment size. In yet another exemplary non-limiting embodiment of the present invention, the real-time hop size may be 0.1 seconds.

[0044] The inventors have found such a small hop size advantageous for the following reasons. The ultimate purpose of generating real-time segments is to analyze and compare them with the reference segments in the database to look for matches. The inventors have found at least two major reasons why a segment of the same audio recording captured real-time would not match its counterpart in the database. One is that the broadcast channel does not produce a perfect copy of the original. For example, the work may be edited or processed or the announcer may talk over part of the work. The other reason is that larger segment boundaries may not line up in time with the original segment boundaries of the target recordings.

[0045] The inventors have found that by choosing a smaller hop size, some of the segments will ultimately have time boundaries that line up with the original segments, notwithstanding the problems listed above. The segments that line up with a "clean" segment of the work may then be used to make an accurate comparison while those that do not so line up may be ignored. The inventors have found that a hop size of 0.1 seconds seems to be the maximum that would solve this time shifting problem.

[0046] As mentioned above, once a work has been segmented, the individual segments are then analyzed to produce a segment feature vector. Figure 5 is a diagram showing an overview of how the segment feature vectors may be created using the methods described in US Patent #5,918,223 to Blum, et al. It is contemplated that a variety of analysis methods may be useful in the present invention, and many different features may be used to make up the feature vector. The inventors have found that the pitch, brightness, bandwidth, and loudness features of the '223 patent to be useful in the present invention. Additionally, spectral features may be used analyzed, such as the energy in various spectral bands. The inventors have found that the cepstral features (MFCCs) are very robust (more invariant) given the distortions typically introduced during broadcast, such as EQ, multi-band compression/limiting, and audio data compression techniques such as MP3 encoding/decoding, etc.

[0047] In act 500, the audio segment is sampled to produce a segment. In act 502, the sampled segment is then analyzed using Fourier Transform techniques to transform the signal into the frequency domain. In act 504, mel frequency filters are applied to the transformed signal to extract the significant audible characteristics of the spectrum. In act 506, a Discrete Cosine Transform is applied which converts the signal into mel frequency cepstral coefficients (MFCCs). Finally, in act 508, the MFCCs are then averaged over a predetermined period. In an exemplary non-limiting embodiment of the present invention, this period is approximately one second. Additionally, other characteristics may be computed at this time, such as brightness or loudness. A segment feature vector is then produced which contains a list containing at least the 10 MFCCs corresponding average.

[0048] The disclosure of FIGS. 3, 4, and 5 provide examples of means for creating a signature of a sampled work having a segment size and a hop size.

[0049] Figure 6 is a diagram showing a complete signature 600 according to the present invention. Signature 600 includes a plurality of segment feature vectors 1 through n generated as shown and described above. Signature 600 may also include an identification portion containing a unique ID. It is contemplated that the identification portion may contain a unique identifier provided by the RIAA (Recording Industry Association of America). The identification portion may also contain information such as the UPC (Universal Product Code) of the various products that contain the audio corresponding to this signature. Additionally, it is contemplated that the signature 600 may also contain information pertaining to the characteristics of the file itself, such as the hop size, segment size, number of segments, etc., which may be useful for storing and indexing.

[0050] Signature 600 may then be stored in a database and used for comparisons. The following computer code in the C programming language provides an example of a database structure in memory according to the present invention:

```
typedef struct
{
       float hopSize;        /* hop size */
       float segmentSize;    /* segment size */
    MFSignature* signatures; /* array of signatures */
} MFDatabase;
```

[0051] The following provides an example of the structure of a segment according to the present invention:

```
typedef struct
{
       char* id;              /* unique ID for this audio clip */
       long numSegments;/* number of segments */
       float* features;       /* feature array */
       long size;             /* size of per-segment feature vector */
       float hopSize;
       float segmentSize ;
} MFSignature;
```

[0052] The discussion of FIG. 6 provides an example of means for storing segments and signatures according to the present invention.

[0053] Figure 7 shows a functional diagram of a comparison process according to the present invention. Act 1 of FIG. 7 shows unknown audio being converted to a signature according to the present invention. In act 2, reference signatures are retrieved from a reference database. Finally, the reference signatures are scanned and compared to the unknown audio signatures to determine whether a match exists. This comparison may be accomplished through means known in the art. For example, the Euclidean distance between the reference and real-time signature can be computed and compared to a threshold.

[0054] It is contemplated that the present invention has many beneficial uses, including many outside of the music piracy area. For example, the present invention may be used to verify royalty payments. The verification may take place at the source or the listener. Also, the present invention may be utilized for the auditing of advertisements, or collecting Arbitron®-like data (who is listening to what). The present invention may also be used to label the audio recordings on a user's hard disk or on the web.

[0055] While embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art that many more modifications than mentioned above are possible within the scope defined by the appended claims.

Claims

1. A method for determining an identity of a sampled work, said method comprising receiving data of a sampled work, segmenting said data of said sampled work into a plurality of segments wherein each of said segments has predetermined segment size and a predetermined hop size, creating a signature of said sampled work based upon said plurality of segments, comparing said signature of said sampled work to a plurality of signatures of reference works, and determining said sampled work is one of said reference works based upon said comparison, said method **characterized in that** said predetermined hop size of said segments of said sampled work signature is chosen to be less than said hop size of each of said plurality of reference signatures.

2. The method of claim 1, wherein said act of creating a signature of said sampled work comprises calculating segment

feature vectors for each segment of said sampled work.

3. The method of claim 1, wherein said act of creating a signature of said sampled work includes calculating a plurality of MFCCs for each said segment.

4. The method of claim 1, wherein said act of creating a signature of said sampled work includes calculating a plurality of acoustical features from the group consisting of at least one of loudness, pitch, brightness, bandwidth, spectrum and MFCC coefficients for each said segment.

5. The method of claim 1, wherein said sampled work signature comprises a plurality of segments and an identification portion.

6. The method of claim 1, wherein said plurality of segments of said sampled work signature comprise a segment size of approximately 0.5 to 3 seconds.

7. The method of claim 6, wherein said plurality of segments of said sampled work signature comprise a hop size of less than 50% of the segment size.

8. The method of claim 6, wherein said plurality of segments of said sampled work signature comprise a hop size of approximately 0.1 seconds.

9. An apparatus that determines an identity of a sampled work, said apparatus comprising circuitry configured to receive data of a sampled work, circuitry configured to segment said data of said sampled work into a plurality of segments wherein each of said segments has predetermined segment size and a predetermined hop size, circuitry configured to create a signature of said sampled work based upon said plurality of segments, circuitry configured to compare said signature of said sampled work to a plurality of signatures of reference works, and circuitry configured to determine said sampled work is one of said reference works based upon said comparison, said apparatus **characterized in that** said predetermined hop size of said segments of said sampled work signature is chosen to be less than said hop size of each of said plurality of reference signatures.

10. The apparatus of claim 9, wherein said circuitry configured to create a signature of said sampled work comprises circuitry configured to calculate segment feature vectors for each of said plurality of segments of said sampled work.

11. The apparatus of claim 9, wherein said circuitry configured to create a signature includes calculating a plurality of MFCCs for each said segment.

12. The apparatus of claim 9, wherein said circuitry configured to create a signature includes circuitry configured to calculate one of a plurality of acoustical features selected from a group consisting of loudness, pitch, brightness, bandwidth, spectrum and MFCC coefficients for each of said plurality of segments of said sampled works.

13. The apparatus of claim 9, wherein said sampled work signature comprises a plurality of segments and an identification portion.

14. The apparatus of claim 9, wherein said plurality of segments of said sampled work comprise said predetermined segment size of approximately 0.5 to 3 seconds.

15. The apparatus of claim 14, wherein said predetermined hop size of said plurality of segments of said sampled work signature is less than 50% of the segment size.

16. The apparatus of claim 14, wherein said predetermined hop size of each of said plurality of segments of said sampled work signature is approximately 0.1 seconds.

17. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method according to any one of claims 1 to 8.

Patentansprüche

1. Verfahren zum Ermitteln einer Identität eines abgetasteten Werks, wobei das Verfahren umfasst: das Empfangen von Daten eines abgetasteten Werks, das Segmentieren der Daten des abgetasteten Werks in mehrere Segmente, wobei jedes der Segmente eine vorbestimmte Segmentgröße und eine vorbestimmte Hop-Size aufweist, das Erzeugen einer Signatur des abgetasteten Werks beruhend auf den mehreren Segmenten, das Vergleichen der Signatur des abgetasteten Werks mit mehreren Signaturen von Referenzwerken und beruhend auf dem Vergleich das Bestimmen, dass das abgetastete Werk eines der Referenzwerke ist, wobei das Verfahren **dadurch gekennzeichnet ist, dass** die vorbestimmte Hop-Size der Segmente der Signatur des abgetasteten Werks kleiner als die Hop-Size jeder der mehreren Referenzsignaturen gewählt wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** der Vorgang des Erzeugens einer Signatur des abgetasteten Werks das Berechnen von Segmentmerkmalsfaktoren für jedes Segment des abgetasteten Werks umfasst.

3. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** der Vorgang des Erzeugens einer Signatur des abgetasteten Werks das Berechnen mehrerer MFCC für jedes Segment umfasst.

4. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** der Vorgang des Erzeugens einer Signatur des abgetasteten Werks das Berechnen mehrerer akustischer Merkmale aus der Gruppe bestehend aus mindestens einem von Lautstärke, Tonhöhe, Helligkeit, Bandbreite, Spektrum und MFCC-Koeffizienten für jedes Segment umfasst.

5. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die Signatur des abgetasteten Werks mehrere Segmente und einen Erkennungsabschnitt umfasst.

6. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die mehreren Segmente der Signatur des abgetasteten Werks eine Segmentgröße von in etwa 0,5 bis 3 Sekunden umfassen.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet, dass** die mehreren Segmente der Signatur des abgetasteten Werks eine Hop-Size von kleiner als 50% der Segmentgröße umfassen.

8. Verfahren nach Anspruch 6, **dadurch gekennzeichnet, dass** die mehreren Segmente der Signatur des abgetasteten Werks eine Hop-Size von in etwa 0,1 Sekunden umfassen.

9. Vorrichtung, die eine Identität eines abgetasteten Werks ermittelt, wobei die Vorrichtung umfasst: eine zum Empfangen von Daten eines abgetasteten Werks ausgelegte Schaltung, eine zum Segmentieren der Daten des abgetasteten Werks in mehrere Segmente ausgelegte Schaltung, wobei jedes der Segmente eine vorbestimmte Segmentgröße und eine vorbestimmte Hop-Size aufweist, eine zum Erzeugen einer Signatur des abgetasteten Werks beruhend auf den mehreren Segmenten ausgelegte Schaltung, eine zum Vergleichen der Signatur des abgetasteten Werks mit mehreren Signaturen von Referenzwerken ausgelegte Schaltung und eine zum vergleichsbasierten Bestimmen, dass das abgetastete Werk eines der Referenzwerke ist, ausgelegte Schaltung, wobei die Vorrichtung **dadurch gekennzeichnet ist, dass** die vorbestimmte Hop-Size der Segmente der Signatur des abgetasteten Werks kleiner als die Hop-Size jeder der mehreren Referenzsignaturen gewählt ist.

10. Vorrichtung nach Anspruch 9, **dadurch gekennzeichnet, dass** die zum Erzeugen einer Signatur des abgetasteten Werks ausgelegte Schaltung eine zum Berechnen von Segmentmerkmalsvektoren für jedes der mehreren Segmente des abgetasteten Werks ausgelegte Schaltung umfasst.

11. Vorrichtung nach Anspruch 9, **dadurch gekennzeichnet, dass** die zum Erzeugen einer Signatur ausgelegte Schaltung das Berechnen mehrerer MFCC für jedes Segment umfasst.

12. Vorrichtung nach Anspruch 9, **dadurch gekennzeichnet, dass** die zum Erzeugen einer Signatur ausgelegte Schaltung eine Schaltung umfasst, die zum Berechnen eines von mehreren akustischen Merkmalen gewählt aus einer Gruppe bestehend aus Lautstärke, Tonhöhe, Helligkeit, Bandbreite, Spektrum und MFCC-Koeffizienten für jedes der mehreren Segmente der abgetasteten Werke ausgelegt ist.

13. Vorrichtung nach Anspruch 9, **dadurch gekennzeichnet, dass** die Signatur des abgetasteten Werks mehrere

Segmente und einen Erkennungsabschnitt umfasst.

14. Vorrichtung nach Anspruch 9, **dadurch gekennzeichnet, dass** die mehreren Segmente des abgetasteten Werks die vorbestimmte Segmentgröße von in etwa 0,5 bis 3 Sekunden umfassen.

15. Vorrichtung nach Anspruch 14, **dadurch gekennzeichnet, dass** die vorbestimmte Hop-Size der mehreren Segmente der Signatur des abgetasteten Werks kleiner als 50% der Segmentgröße ist.

16. Vorrichtung nach Anspruch 14, **dadurch gekennzeichnet, dass** die vorbestimmte Hop-Size jedes der mehreren Segmente der Signatur des abgetasteten Werks in etwa 0,1 Sekunden ist.

17. Maschinenlesbare Programmspeichervorrichtung, die konkret ein Programm von Befehlen verkörpert, die von der Maschine zum Durchführen eines Verfahrens nach einem der Ansprüche 1 bis 8 ausführbar sind.

Revendications

1. Procédé pour déterminer une identité d'une oeuvre échantillonnée, ledit procédé comportant la réception de données d'une oeuvre échantillonnée, la segmentation desdites données de ladite oeuvre échantillonnée en une pluralité de segments dans lequel chacun desdits segments a une taille de segment prédéterminée et une taille de saut prédéterminée, la création d'une signature de ladite oeuvre échantillonnée sur la base de ladite pluralité de segments, la comparaison de ladite signature de ladite oeuvre échantillonnée à une pluralité de signatures d' oeuvres de référence, et la détermination que ladite oeuvre échantillonnée est l'une desdites oeuvres de référence sur la base de ladite comparaison, ledit procédé étant **caractérisé en ce que** ladite taille de saut prédéterminée desdits segments de ladite signature d'oeuvre échantillonnée est choisie de manière à être inférieure à ladite oeuvre de saut de chacune de ladite pluralité de signatures de référence.

2. Procédé selon la revendication 1, dans lequel ladite action de création de signature de ladite oeuvre échantillonnée comprend le calcul de vecteurs caractéristiques de segment pour chaque segment de ladite tâche échantillonnée.

3. Procédé selon la revendication 1, dans lequel ladite action de création de signature de ladite oeuvre échantillonnée inclut le calcul d'une pluralité de MFCC pour chacun desdits segments.

4. Procédé selon la revendication 1, dans lequel ladite action de création de signature de ladite oeuvre échantillonnée inclut le calcul d'une pluralité de caractéristiques acoustiques parmi le groupe constitué d'au moins l'un parmi la sonie, la hauteur tonale, la brillance, la largeur de bande, le spectre et des coefficients MFCC pour chaque segment.

5. Procédé selon la revendication 1, dans lequel ladite signature d'oeuvre échantillonnée comporte une pluralité de segments et une partie d'identification.

6. Procédé selon la revendication 1, dans lequel ladite pluralité de segments de ladite signature d'oeuvre échantillonnée comporte une taille de segment d'approximativement 0,5 à 3 secondes.

7. Procédé selon la revendication 6, dans lequel ladite pluralité de segments de ladite signature d'oeuvre échantillonnée comporte une taille de saut inférieure à 50 % de la taille de segment.

8. Procédé selon la revendication 6, dans lequel ladite pluralité de segments de ladite signature d'oeuvre échantillonnée comporte une taille de saut d'approximativement 0,1 seconde.

9. Appareil qui détermine une identité d'une oeuvre échantillonnée, ledit appareil comportant un circuit configuré pour recevoir des données d'une oeuvre échantillonnée, un circuit configuré pour segmenter lesdites données de ladite oeuvre échantillonnée en une pluralité de segments dans lesquels chacun desdits segments a une taille de segment prédéterminée et une taille de saut prédéterminée, un circuit configuré pour créer une signature de ladite oeuvre échantillonnée sur la base de ladite pluralité de segments, un circuit configuré pour comparer ladite signature de ladite oeuvre échantillonnée à une pluralité de signatures d' oeuvre de référence, et un circuit configuré pour déterminer que ladite oeuvre échantillonnée est l'une desdites oeuvres de référence sur la base de ladite comparaison, ledit appareil étant **caractérisé en ce que** ladite taille de saut prédéterminée desdits segments de ladite signature d'oeuvre échantillonnée est choisie de manière à être inférieure à ladite tâche de saut de chacune de ladite pluralité

de signatures de référence.

10. Appareil selon la revendication 9, dans lequel ledit circuit configuré pour créer une signature de ladite oeuvre échantillonnée comprend un circuit configuré pour calculer des vecteurs caractéristiques de segments pour chacun de ladite pluralité de segments de ladite oeuvre échantillonnée.

11. Appareil selon la revendication 9, dans lequel ledit circuit configuré pour créer une signature inclut le calcul d'une pluralité de MFCC pour chaque segment.

12. Appareil selon la revendication 9, dans lequel ledit circuit configuré pour créer une signature inclut un circuit configuré pour calculer l'une d'une pluralité de caractéristiques acoustiques sélectionnées parmi le groupe constitué de la sonie, la hauteur tonale, la brillance, la largeur de bande, le spectre et les coefficients MFCC pour chacun de ladite pluralité de segments desdites oeuvres échantillonnées.

13. Appareil selon la revendication 9, dans lequel ladite signature d'oeuvre échantillonnée comporte une pluralité de segments et une partie d'identification.

14. Appareil selon la revendication 9, dans lequel ladite pluralité de segments de ladite oeuvre échantillonnée comporte ladite taille de segment prédéterminée d'approximativement 0,5 à 3 secondes.

15. Appareil selon la revendication 14, dans lequel ladite taille de saut prédéterminée de ladite pluralité de segments de ladite signature d'oeuvre échantillonnée est inférieure à 50 % de la taille de segment.

16. Appareil selon la revendication 14, dans lequel ladite taille de saut prédéterminée de chacun de ladite pluralité de segments de ladite signature d'oeuvre échantillonnée est approximativement de 0,1 seconde.

17. Dispositif de mémorisation de programme lisible par machine, intégrant de manière tangible un programme d'instructions exécutable par la machine pour exécuter un procédé selon l'une quelconque des revendications 1 à 8.

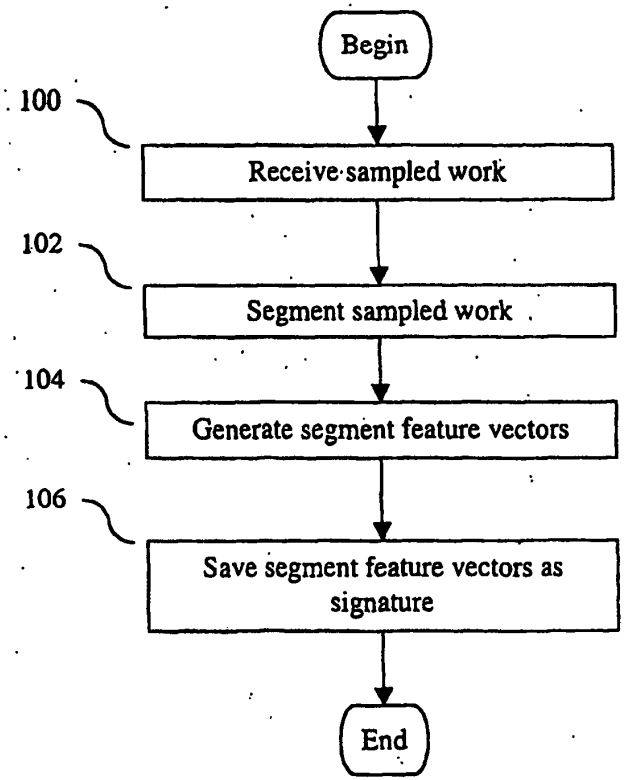


FIG. 1
Present Invention

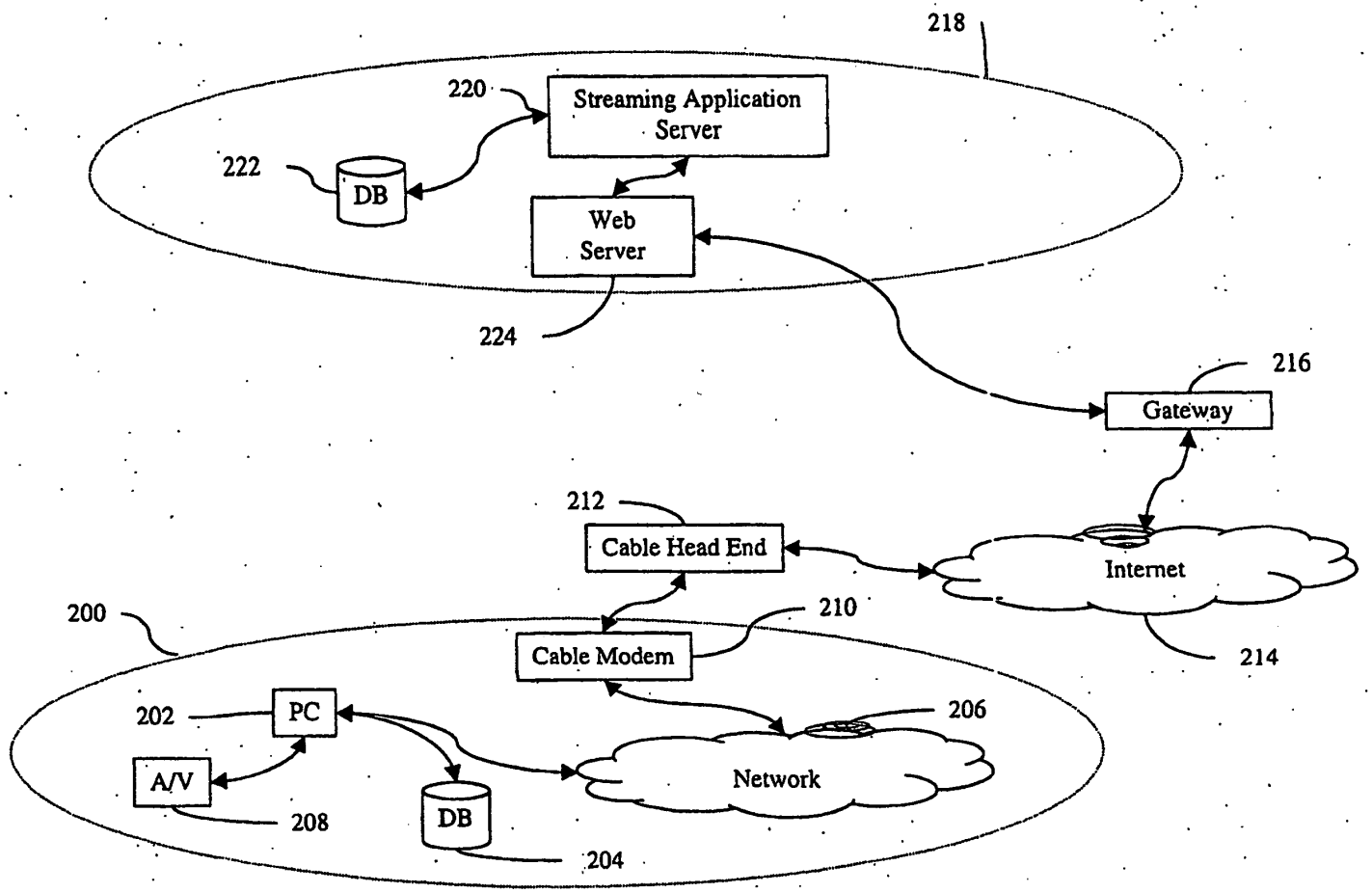


FIG. 2
Present Invention

EP 1 354 276 B1

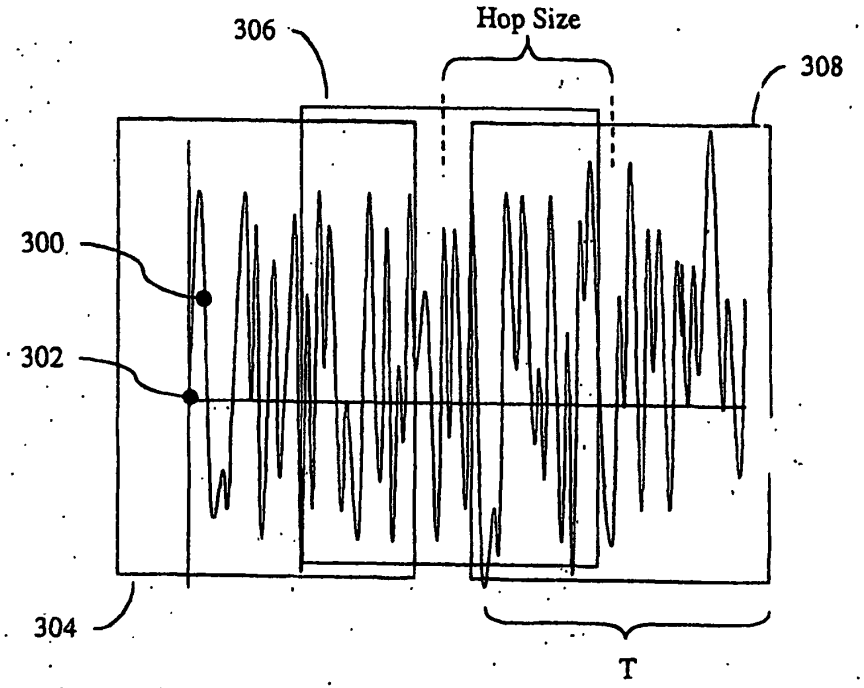


FIG. 3
Present Invention

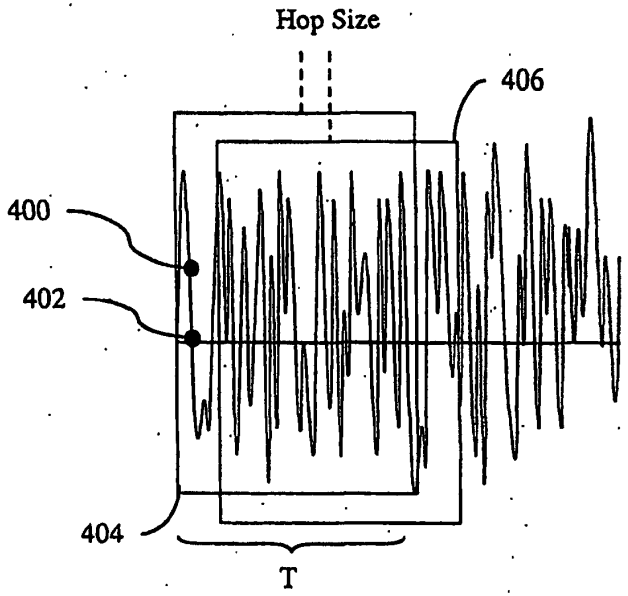


FIG. 4
Present Invention

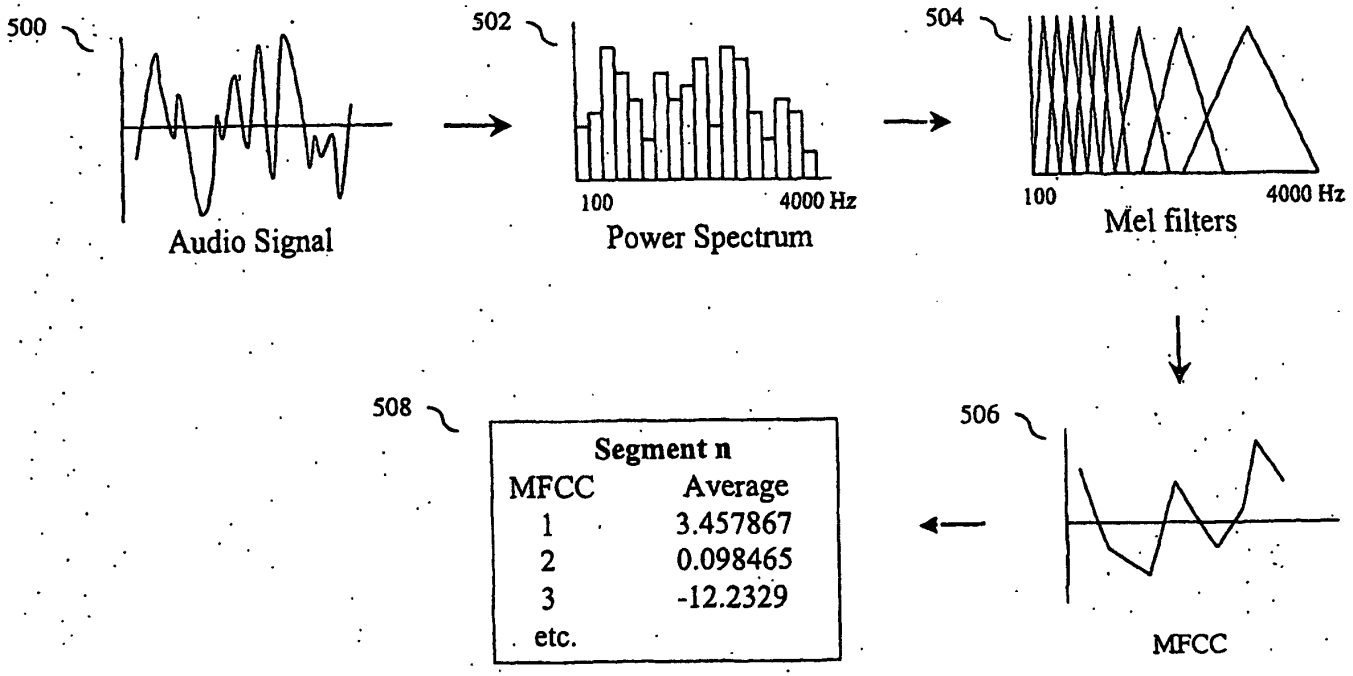


FIG. 5
Present Invention

EP 1 354 276 B1

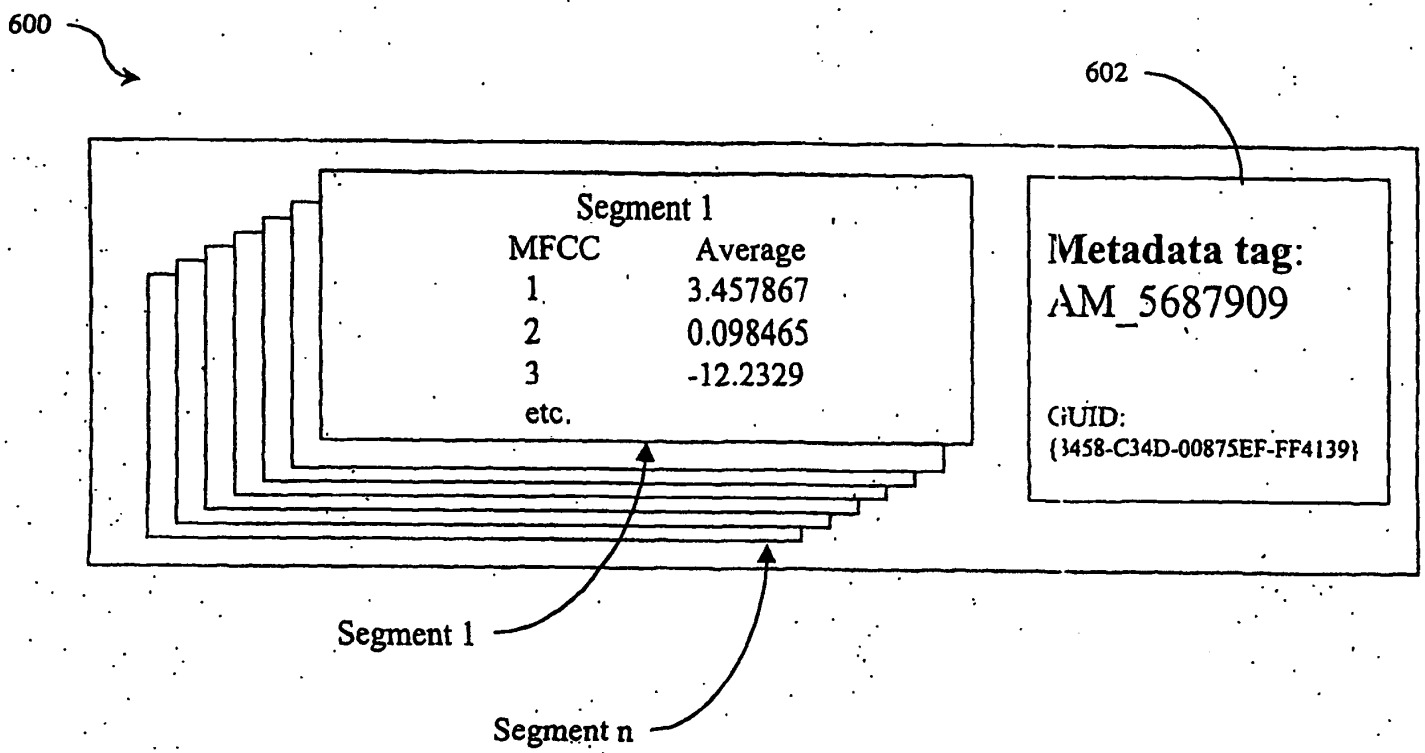


FIG. 6
Present Invention

EP 1 354 276 B1

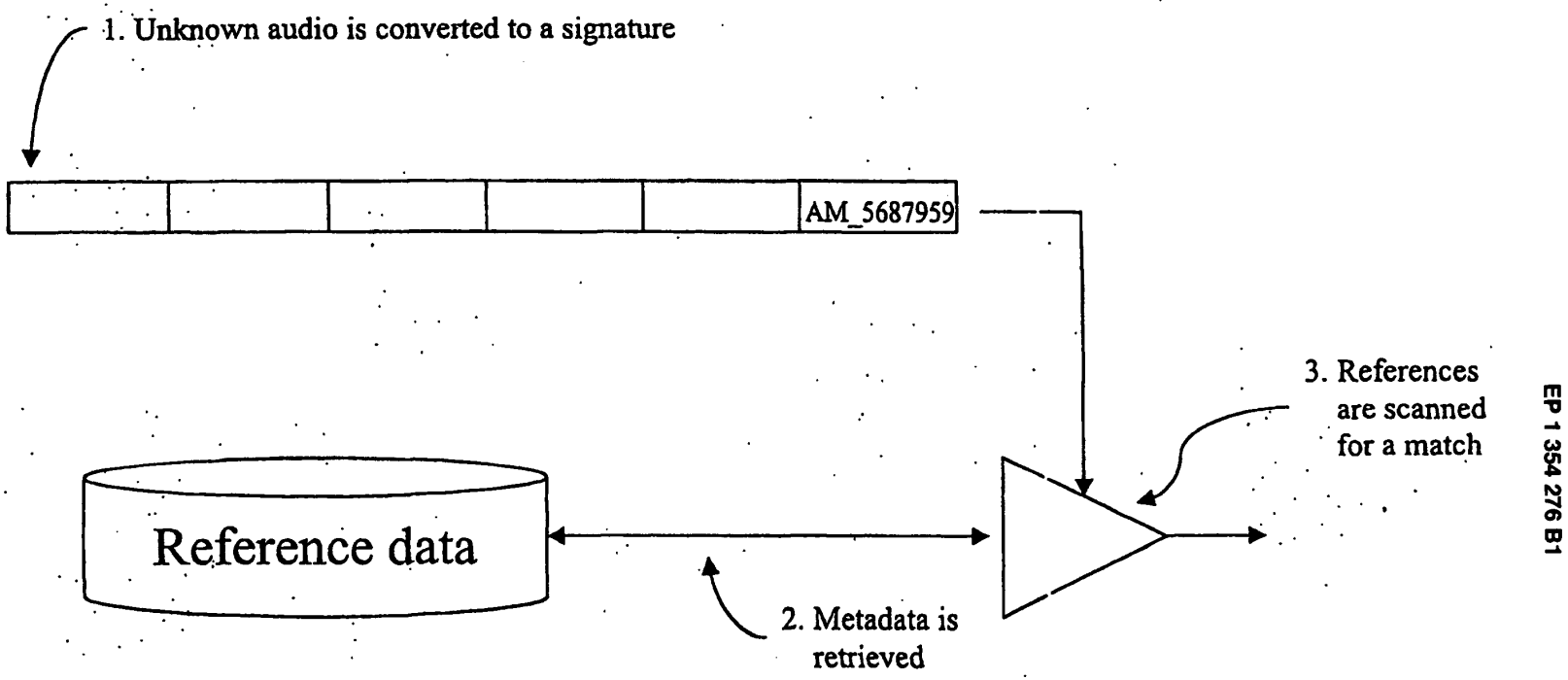


FIG. 7
Present Invention

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 5918223 A **[0007]**

Document Description: Transmittal Letter

09/09/09

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [x] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s)
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name			
Signature	Scott Moskowitz		
Printed name	Scott A. MOSKOWITZ		
Date	September 8, 2009	Reg. No.	

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	Scott Moskowitz		
Typed or printed name	Scott A. MOSKOWITZ	Date	September 8, 2009

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/17 (10-08)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

Effective on 12/08/2004.
Fees Pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2009

SEP 08 2009

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 400.00

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Examiner Name	NA
Art Unit	2432
Attorney Docket No.	80391.0003CONT2

METHOD OF PAYMENT (check all that apply)

☐ Check ☑ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☐ Deposit Account Deposit Account Number: _____ Deposit Account Name: _____

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☐ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	330	165	540	270	220	110	
Design	220	110	100	50	140	70	
Plant	220	110	330	165	170	85	
Reissue	330	165	540	270	650	325	
Provisional	220	110	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	52	26
Each independent claim over 3 (including Reissues)	220	110
Multiple dependent claims	390	195

EXCESS INDEPENDENT CLAIM FEE 2 x 110 = $220.00

Total Claims _____ - 20 or HP = _____ x _____ = _____ Fee Paid ($)

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims _____ - 3 or HP = _____ x _____ = _____ Fee Paid ($)

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims: Fee ($) _____ Fee Paid ($) _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $270 ($135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ - 100 = _____ Extra Sheets / 50 = _____ Number of each additional 50 or fraction thereof (round up to a whole number) x _____ Fee ($) = _____ Fee Paid ($)

4. OTHER FEE(S)

Non-English Specification, $130 fee (no small entity discount)

Other (e.g., late filing surcharge): IDS Before FOAM

EXCESS CLAIM FEE $220.00 ✓

Fees Paid ($): $180.00

SUBMITTED BY

Signature	Scott Moskowitz	Registration No. (Attorney/Agent)	Telephone 305 956 9041
Name (Print/Type)	Scott A. MOSKOWITZ		Date September 8, 2009

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/895,388	Filing Date 08/24/2007	☐ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	09/08/2009	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 33	Minus	** 31	= 2	X $26 =	52	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 7	Minus	***5	= 2	X $110 =	220	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	272	OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/TINA J. BARDEN/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

e 09/21/2009

Scott A. Moskowitz
#2505
16711 Collins Avenue
Sunny Isless Beach, FL 33160

Paper No.

Application No.:	**11/895,388**	**Date Mailed:**	**09/21/2009**
First Named Inventor:	Moskowitz, Scott, A.	Examiner:	OKEKE, IZUNNA
Attorney Docket No.:	80391.0003CONT2	Art Unit:	2432
Confirmation No.:	2103	Filing Date:	08/24/2007

Please find attached an Office communication concerning this application or proceeding.

Commissioner for Patents

PTO-90c (Rev.08-06)

Notice of Non-Compliant Amendment (37 CFR 1.121)	Application No. 11/895,388	Applicant(s) MOSKOWITZ, SCOTT A.	
		Art Unit 2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

The amendment document filed on *08 September, 2009* is considered non-compliant because it has failed to meet the requirements of 37 CFR 1.121 or 1.4. In order for the amendment document to be compliant, correction of the following item(s) is required.

THE FOLLOWING MARKED (X) ITEM(S) CAUSE THE AMENDMENT DOCUMENT TO BE NON-COMPLIANT:

- ☐ 1. Amendments to the specification:
  - ☐ A. Amended paragraph(s) do not include markings.
  - ☐ B. New paragraph(s) should not be underlined.
  - ☐ C. Other _____.
- ☐ 2. Abstract:
  - ☐ A. Not presented on a separate sheet. 37 CFR 1.72.
  - ☐ B. Other _____.
- ☐ 3. Amendments to the drawings:
  - ☐ A. The drawings are not properly identified in the top margin as "Replacement Sheet," "New Sheet," or "Annotated Sheet" as required by 37 CFR 1.121(d).
  - ☐ B. The practice of submitting proposed drawing correction has been eliminated. Replacement drawings showing amended figures, without markings, in compliance with 37 CFR 1.84 are required.
  - ☐ C. Other _____.
- ☒ 4. Amendments to the claims:
  - ☐ A. A complete listing of all of the claims is not present.
  - ☐ B. The listing of claims does not include the text of all pending claims (including withdrawn claims)
  - ☐ C. Each claim has not been provided with the proper status identifier, and as such, the individual status of each claim cannot be identified. Note: the status of every claim must be indicated after its claim number by using one of the following status identifiers: (Original), (Currently amended), (Canceled), (Previously presented), (New), (Not entered), (Withdrawn) and (Withdrawn-currently amended).
  - ☐ D. The claims of this amendment paper have not been presented in ascending numerical order.
  - ☒ E. Other: *See Continuation Sheet*.
- ☐ 5. Other (e.g., the amendment is unsigned or not signed in accordance with 37 CFR 1.4): For further explanation of the amendment format required by 37 CFR 1.121, see MPEP § 714.

TIME PERIODS FOR FILING A REPLY TO THIS NOTICE:

1. Applicant is given **no new time period** if the non-compliant amendment is an after-final amendment or an amendment filed after allowance, or a drawing submission (only) If applicant wishes to resubmit the non-compliant after-final amendment with corrections, the **entire corrected amendment** must be resubmitted.

2. Applicant is given **one month**, or thirty (30) days, whichever is longer, from the mail date of this notice to supply the correction, if the non-compliant amendment is one of the following: a preliminary amendment, a non-final amendment (including a submission for a request for continued examination (RCE) under 37 CFR 1.114), a supplemental amendment filed within a suspension period under 37 CFR 1.103(a) or (c), and an amendment filed in response to a Quayle action. If any of above boxes 1 to 4 are checked, the correction required is only the corrected section of the non-compliant amendment in compliance with 37 CFR 1.121.

Extensions of time are available under 37 CFR 1.136(a) only if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action.

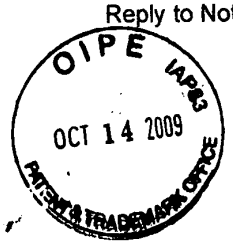
Failure to timely respond to this notice will result in:

Abandonment of the application if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action; or

Non-entry of the amendment if the non-compliant amendment is a preliminary amendment or supplemental amendment.

Legal Instruments Examiner (LIE), if applicable /TINA J. BARDEN/ Telephone No: (571)272-0555

Continuation of 4. Other: Applicant does not have a deposit account number, fee is due for 2 independent and dependent claims for the independent claim $220.00 is due $220.00 was already paid and for the dependent claim $104 is due according to applicant's CC charge he's large entity .



UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	11/895,388	Confirmation No. 2103
Applicant	:	Scott A. MOSKOWITZ	
Filed	:	August 24, 2007	
TC/A.U.	:	2432	
Examiner	:	Izunna OKEKE	
Docket No.	:	80391.0003CONT2	

MAIL STOP Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRELIMINARY AMENDMENT

Prior to examination on the merits, please enter the following amendments to the application. This amendment is in response to the Non-Compliant Amendment (37 CFR 1.121) dated September 21, 2009. Applicant provides the following corrections:

Applicant maintains small entity status as per 37 CFR 1.27 & submits the excess claims fee for the two ("2") previously submitted independent claims as per Office instructions on or about Friday, October 2, 2009.

10/16/2009 CNGUYEN2 00000009 11895388
01 FC:2202 52.00 OP

REMARKS

Applicants request entry of the amendment and submit that this application is in condition for allowance, and a notice to this effect is earnestly sought.

If the Examiner believes that prosecution might be furthered by discussing the Application with the Applicants, we would welcome the opportunity to do so. It is believed that no other fees are required to ensure entry and consideration of this response.

Respectfully submitted,

Date: October 14, 2009

By:_____
Scott A. Moskowitz
16711 Collins Avenue, #2505
Sunny Isles Beach, FL 33160
Tel# (305) 956-9041
Fax# (305) 956-9042

OIPE IAP23
OCT 14 2009
PATENT & TRADEMARK OFFICE

PTO/SB/17 (10-08)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2009

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 52.00

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Examiner Name	Izunna OKEKE
Art Unit	2432
Attorney Docket No.	80391.0003CONT2

METHOD OF PAYMENT (check all that apply)

☐ Check ☑ Credit Card ☐ Money Order ☐ None ☐ Other (please identify):_____

☐ Deposit Account Deposit Account Number:_____ Deposit Account Name:_____

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☐ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fees Paid ($)
Utility	330	165	540	270	220	110	
Design	220	110	100	50	140	70	
Plant	220	110	330	165	170	85	
Reissue	330	165	540	270	650	325	
Provisional	220	110	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	52	26
Each independent claim over 3 (including Reissues)	220	110
Multiple dependent claims	390	195

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 20 or HP =	2	x 26	= 52

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 3 or HP =	_____	x _____	= _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims	
Fee ($)	Fee Paid ($)
_____	_____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $270 ($135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
_____ - 100 =	_____	/ 50 = _____ (round up to a whole number)	x _____	= _____

4. OTHER FEE(S) Fees Paid ($)

Non-English Specification, $130 fee (no small entity discount) _____

Other (e.g., late filing surcharge):_____ _____

SUBMITTED BY

Signature	Scott Moskowitz	Registration No. (Attorney/Agent)	Telephone 305 956 9041
Name (Print/Type)	Scott A. MOSKOWITZ		Date October 14, 2009

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

OIPE
OCT 14 2009
PATENT & TRADEMARK OFFICE

Document Description: Transmittal Letter 10/15/09

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2432
Examiner Name	Izunna OKEKE
Attorney Docket Number	80391.0003CONT2

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [x] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s)
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

Reply to Notice of Non-Compliant Amendment (37 CFR 1.121)

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name			
Signature	Scott Moskowitz		
Printed name	Scott A. MOSKOWITZ		
Date	October 14, 2009	Reg. No.	

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	Scott Moskowitz		
Typed or printed name	Scott A. MOSKOWITZ	Date	October 14, 2009

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/895,388	08/24/2007	Scott A. Moskowitz	80391.0003CONT2	2103

7590 11/10/2009

Scott A. Moskowitz
#2505
16711 Collins Avenue
Sunny Isless Beach, FL 33160

EXAMINER	
OKEKE, IZUNNA	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
11/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/895,388	MOSKOWITZ, SCOTT A.	
	Examiner	Art Unit	
	IZUNNA OKEKE	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 September 2009*.

2a)☐ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 32-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *1-5 and 32-57* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

   I. Claims 1-5, drawn to scrambling or encoding of digital media with a predetermined key wherein the key is required to decode the digital media, classified in class 380, subclass 210.

   II. Claims 32-45 and 52-57, drawn to protecting data or software by inhibiting the unauthorized installation or use of software, classified in class 713, subclass 176.

   III. Claims 46-51, drawn to a method for embedding a watermark on data by configuring a portion of code contained in software according to a watermarking process, classified in class 358, subclass 3.28.

2. The inventions are independent or distinct, each from the other because: Inventions I, II and III are directed to related processes.

Invention I is distinct from Invention II and III and is directed to scrambling or encoding digital information comprising a digital sample and format information with a predetermined key wherein an unauthorized user can play a low version of the encoded sample.

Invention II is distinct from Invention I and III and directed to the protection of data of software during installation wherein a key is required for the authorized use of the software.

Invention III is distinct from Invention I and II and directed to a method of watermarking data or software according to a watermarking process by inserting information into the software.

3. The related processes are distinct if: (1) the inventions as claimed are either not capable of use together or can have a materially different design, mode of operation, function, or effect;

(2) the inventions do not overlap in scope, i.e., are mutually exclusive; and (3) the inventions as claimed are not obvious variants. See MPEP § 806.05(j). In the instant case, the inventions as claimed have a different function, or effect as described above. Furthermore, the inventions as claimed do not encompass overlapping subject matter and there is nothing of record to show them to be obvious variants.

4. Restriction for examination purposes as indicated is proper because all these inventions listed in this action are independent or distinct for the reasons given above and there would be a serious search and examination burden if restriction were not required because one or more of the following reasons apply:

(b) the inventions have acquired a separate status in the art due to their recognized divergent subject matter;

(c) the inventions require a different field of search (for example, searching different classes/subclasses or electronic resources, or employing different search queries);

(d) the prior art applicable to one invention would not likely be applicable to another invention;

Applicant is advised that the reply to this requirement to be complete must include (i) an election of a invention to be examined even though the requirement may be traversed (37 CFR 1.143) **and (ii) identification of the claims encompassing the elected invention**.

The election of an invention may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse. Traversal must be presented at the time of election in order to be

considered timely. Failure to timely traverse the requirement will result in the loss of right to petition under 37 CFR 1.144. If claims are added after the election, applicant must indicate which of these claims are readable on the elected invention.

If claims are added after the election, applicant must indicate which of these claims are readable upon the elected invention.

Should applicant traverse on the ground that the inventions are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the inventions to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103(a) of the other invention.

Conclusion

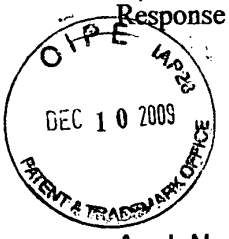
Any inquiry concerning this communication or earlier communications from the examiner should be directed to IZUNNA OKEKE whose telephone number is (571)270-3854. The examiner can normally be reached on 9:00am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. O./
Examiner, Art Unit 2432

/Jung Kim/
Primary Examiner, AU 2432



UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	11/895,388	Confirmation No. 2103
Applicant	:	Scott A. MOSKOWITZ	
Filed	:	August 24, 2007	
TC/A.U.	:	2432	
Examiner	:	Izunna OKEKE	
Docket No.	:	80391.0003CONT2	

MAIL STOP AMENDMENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO ELECTION/RESTRICTION REQUIREMENT

Sir:

In response to the Office Action of November 10, 2009, Applicant provides the following remarks:

RESPONSE TO RESTRICTION REQUIREMENT:

In response to the Office Action of November 10, 2009, Applicant provisionally elects to prosecute the claims in Group II (namely, claims 32 – 45 and 52-57).

REMARKS/ARGUMENTS

Applicant respectfully seeks clarification on the requirement for restriction regarding pending claims 58 and 59.

REMARKS

Applicant requests entry of the amendments and submits that this application is in condition for allowance, and a notice to this effect is earnestly sought.

Respectfully submitted,

Date: December 10, 2009

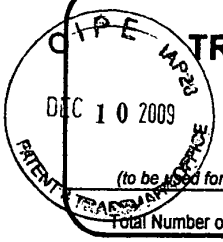
By: _____
Scott A. Moskowitz
Tel (305) 956-9041
Fax (305) 956-9042

Doc Code: TRAN.LET
Document Description: Transmittal Letter

12-11-09

DFW

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2432
Examiner Name	Izunna OKEKE
Attorney Docket Number	80391.0003CONT2

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☑ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s)
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name			
Signature	Scott Moskowitz		
Printed name	Scott A. MOSKOWITZ		
Date	December 10, 2009	Reg. No.	

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	Scott Moskowitz		
Typed or printed name	Scott A. MOSKOWITZ	Date	December 10, 2009

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/895,388	08/24/2007	Scott A. Moskowitz	80391.0003CONT2	2103

7590 04/05/2010

Scott A. Moskowitz
#2505
16711 Collins Avenue
Sunny Isless Beach, FL 33160

EXAMINER	
OKEKE, IZUNNA	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
04/05/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/895,388	MOSKOWITZ, SCOTT A.	
	Examiner	Art Unit	
	IZUNNA OKEKE	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 December 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *32-45 and 52-59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *32-45 and 52-59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/19/2007, 10/19/2007 and 09/08/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Applicant's election without traverse of Group II (Claims 32-45 and 52-59) in the reply filed on 12/10/2009 is acknowledged.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 32-45 and 52-59 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-20 of copending Application No. 08587943. Although the conflicting claims are not identical, they are not patentably distinct from each other because both set of claims are directed to a method of copy protection of computer software wherein a key derived from a license information is used in enabling the authorized used of the software.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim(s) 32-39 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The method recited in claims 32-39 for copy protection of software is broad enough that the claims could be completely performed mentally, verbally or without a machine nor is any transformation apparent. Also, given a broad reasonable interpretation, claims 32-39 suggests programs per se (watermark embedded in software) for carrying out the steps of the copy protection. Therefore, claims 32-39 are rejected as being directed to non-statutory subject matter.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claim 32 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 32 recite "wherein the embedded software operates in a manner substantially the same as the software prior to the embedding step". This limitation is not disclosed in the specification in such a way as to reasonably convey to one of ordinary skill how the embedded software operates in a manner "substantially" the same as the software prior to the embedding step. Appropriate correction is required.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 52 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 52 recites a system comprising steps. It is unclear what is being claimed or the scope of the claim because a system is not a method and cannot comprise steps of processing.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 32-45 and 52-59 are rejected under 35 U.S.C. 102(e) as being anticipated by Moore (US-6067622).

a. *Referring to claim 32:*

Regarding claim 32, Moore teaches a method for copy protection of software comprising: embedding the software with a watermark wherein the embedded software operates in a manner substantially the same as the software prior to the embedding step (Fig 1a and Col 8, Line 43-51 teaches an 'install module' embedded within a program for protecting illegal copying of the program and the module does not affect how the program will function).

a. *Referring to claim 33 and 57:*

Regarding claim 33 and similar claim 57, Moore teaches the process of claim 32, wherein the step of embedding the software with a watermark increases the complexity of code analysis and/or tampering with the software (Col 6, Line 38-63…. the 'install module' increases the complexity of the program by inhibiting illicit copying or tampering with the software).

a. *Referring to claim 34:*

Regarding claim 34, Moore teaches the process of claim 32, wherein the watermarked software queries a user for personalization information during installation of the software (Col 7, Line 50-64…. user personalization information)

a. *Referring to claim 35, 36 and 53:*

Regarding claim 35 and similar claims 36 and 53, Moore teaches the process of claim 32, wherein the watermark is accessible with a key (Col 9, Line 39-58…. 'install module' accessible with an 'install key' which enables authorized use of the software).

a. *Referring to claim 37 and 44:*

Regarding claim 37 and similar claim 44, Moore teaches the process according to claim 35, wherein the key and license information are interchangeable (Col 9, Line 19-39…. The install password (which comprises the license to use the program) can be converted to odd or even install key series and is interchangeable with the install key for authorizing the use of the software).

a. *Referring to claim 38:*

Regarding claim 38, Moore teaches the process according to claim 32, wherein the step of embedding the software with a watermark is performed during execution of the software (Col 7, Line 20-49… embedding an internal run key in the program during execution of the program).

a. *Referring to claim 39:*

Regarding claim 39, Moore teaches the process according to claim 32, wherein the step of embedding the software with a watermark modifies the structure of the software being embedded (See Fig. 1a… the 'install module' modifies the structure of the software program).

a. *Referring to claim 40 and 41:*

Regarding claim 40 and similar claim 41, Moore teaches an article of manufacture comprising a machine readable medium, having thereon stored instructions adapted to be executed by a processor, which instructions when executed result in a process comprising: receiving potentially watermarked software; and identifying the software by extracting the watermark (Col 9, Line 35-39… the 'install module' supplies software serial number (fixed prior to the distribution of the software) for identifying software).

a. *Referring to claim 42 and 56:*

Regarding claim 42 and similar claim 56, Moore teaches the article of manufacture of claim 40, wherein the watermark affects functionality of the watermarked software (Col 9, Line 19-58… wrong authentication key matched against the key generated from the 'install module' will affect the functionality of the program).

a. *Referring to claim 43:*

Regarding claim 43, Moore teaches the article of manufacture of claim 40, wherein the extracted watermark enables generation of a key (Col 9, Line 22-31…. install password algorithm determined from the 'install module' used in generation of the install key).

a. *Referring to claim 45:*

Regarding claim 45, Moore teaches the article of manufacture of claim 40, further comprising limiting functionality of the software if the watermark cannot be extracted (Col 9, Line 49-52).

a. *Referring to claim 52:*

Regarding claim 52, Moore teaches a system for copy protection of software comprising [[the steps of]]: an encoder for associating license information with a copy of a software application[[;]] and encoding the associated license information into the copy of the software application [[using a watermarking process]]; and an installer for installing [[providing]] the copy of the software application having license information encoded therein [[to a user;]] and[[,]] comparing information received by a user with the encoded license information (See the rejection in claims 32 and Col 8, Line 43 thru Col 9, Line 58).

a. *Referring to claim 54:*

Regarding claim 54, Moore teaches the system of claim 52, wherein the step of comparing the user supplied information with the encoded license information enables authorization of the software (Col 7, Line 62-65).

a. *Referring to claim 55:*

Regarding claim 55, Moore teaches the system of claim 53, wherein the key is fixed prior to distribution of the software (Col 9, Line 26-31).

a. *Referring to claim 58 and 59:*

Regarding claim 58 and similar claim 59, Moore teaches a method for licensed software use, the method comprising the steps of: requesting license information associated with the software;

comparing the requested license information with license information stored in the software; and enabling use of the software based on the comparison step (See the rejections in claims 32 and 52).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to IZUNNA OKEKE whose telephone number is (571)270-3854. The examiner can normally be reached on 9:00am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. O./
Examiner, Art Unit 2432

/Jung Kim/
Primary Examiner, AU 2432

Notice of References Cited	Application/Control No. 11/895,388	Applicant(s)/Patent Under Reexamination MOSKOWITZ, SCOTT A.	
	Examiner IZUNNA OKEKE	Art Unit 2432	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,067,622	05-2000	Moore, Steven Jerome	726/31
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11895388	MOSKOWITZ, SCOTT A.
	Examiner	Art Unit
	IZUNNA OKEKE	2432

SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Text Search (See History)	3/22/2010	IO
Keyword + Classification Search (See History)	3/22/2010	IO
Search (713/165, 713/176, 713/161, 380/201, 380/228, 380/229) (See History)	3/22/2010	IO
NPL Search	3/22/2010	IO

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11895388	MOSKOWITZ, SCOTT A.
	Examiner	Art Unit
	IZUNNA OKEKE	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/22/2010								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								
	37	✓								
	38	✓								
	39	✓								
	40	✓								
	41	✓								
	42	✓								
	43	✓								
	44	✓								
	45	✓								
	52	✓								
	53	✓								
	54	✓								
	55	✓								
	56	✓								
	57	✓								
	58	✓								
	59	✓								

U.S. PATENT DOCUMENTS

EXAMINER'S
INITIALS:

_____ U.S. Patent Application No. 08/999,766, filed July 23, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent Application No. 11/894,443, filed August 21, 2007, entitled "Steganographic Method and Device";

_____ U.S. Patent Application No. 11/894,476, filed August 21, 2007, entitled "Steganographic Method and Device";

_____ U.S. Patent Application No. 11/050,779, filed February 7, 2005, entitled "Steganographic Method and Device" – Publication No. 20050177727 – August 11, 2005;

_____ U.S. Patent Application No. 08/674,726, filed July 2, 1996, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management";

_____ U.S. Patent Application No. 09/545,589, filed April 7, 2000, entitled "Method and System for Digital Watermarking" (issued as U.S. Patent No. 7,007,166);

_____ U.S. Patent Application No. 11/244,213, filed October 5, 2005, entitled "Method and System for Digital Watermarking" – Publication No. 20060101269 – May 11, 2006;

_____ U.S. Patent Application No. 11/649,026, filed January 3, 2007, entitled "Method and System for Digital Watermarking" – Publication No. 20070113094 – May 17, 2007;

_____ U.S. Patent Application No. 09/046,627, filed March 24, 1998, entitled "Method for Combining Transfer Function with Predetermined Key Creation" (issued as U.S. Patent No. 6,598,162);

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

_____ U.S. Patent Application 10/602,777, filed June 25, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation" – Publication No. 20040086119 – May 6, 2004;

_____ U.S. Patent Application 11/895,388, filed August 24, 2007, entitled "Data Protection Method and Device";

_____ U.S. Patent Application No. 09/053,628, filed April 2, 1998, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" (issued as U.S. Patent No. 6,205,249);

_____ U.S. Patent Application No. 09/644,098, filed August 23, 2000, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" (issued as U.S. Patent No. 7,035,409);

_____ U.S. Patent Application No. 09/767,733, filed January 24, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" – Publication No. 20010010078 - July 26, 2001;

_____ U.S. Patent Application No. 11/358,874, filed February 21, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" – Publication No. 20060140403 – June 29, 2006;

_____ U.S. Patent Application No. 10/417,231, filed April 17, 2003, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth" – Publication No. 20030200439 – October 23, 2003;

_____ U.S. Patent Application No. 11/900,065, filed September 10, 2007, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth";

_____ U.S. Patent Application No. 11/900,066, filed September 10, 2007, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth";

_____ U.S. Patent Application No. 09/789,711, filed February 22, 2001, entitled "Optimization Methods for the Insertion, Protection, and Detection of

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

Digital Watermarks in Digital Data" – Publication No. 20010010078 - October 11, 2001 (issued as U.S. Patent No. 7,107,451);

_____ U.S. Patent Application No. 11/497,822, filed August 2, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070011458 – January 11, 2007;

_____ U.S. Patent Application No. 11/599,964, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent Application No. 11/599,838, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070226506 – September 27, 2007;

_____ U.S. Patent Application No. 11/897,790, filed August 31, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent Application No. 11/897,791, filed August 31, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent Application No. 11/899,661, filed September 7, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent Application No. 11/899,662, filed September 7, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent Application No. 10/369,344, filed February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data" -- Publication No. 20030219143 – November 27, 2003 (issued as U.S. Patent No. 7,095,874);

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

_____ U.S. Patent Application No. 11/482,654, filed July 7, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data" -- Publication No. 20060285722 – December 21, 2006;

_____ U.S. Patent Application No. 09/594,719, filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems" (issued as U.S. Patent 7,123,718);

_____ U.S. Patent Application No. 11/519,467, filed September 12, 2006, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems" -- Publication No. 20070064940 – March 22, 2007;

_____ U.S. Patent Application No 09/731,040, filed December 7, 2000, entitled "Systems, Methods And Devices For Trusted Transactions" -- Publication No. 20020010684 – January 24, 2002 (issued as U.S. Patent 7,159,116);

_____ U.S. Patent Application No 11/512,701, filed August 29, 2006, entitled "Systems, Methods And Devices For Trusted Transactions" -- Publication No. 20070028113 – February 1, 2007;

_____ U.S. Patent Application No. 10/049,101, filed February 8, 2002, entitled "A Secure Personal Content Server" (which claims priority to International Application No. PCT/US00/21189, filed August 4, 2000, which claims priority to U.S. Patent Application No. 60/147,134, filed August 4, 1999, and to U.S. Patent Application No. 60/213,489, filed June 23, 2000);

_____ U.S. Patent Application No. 09/657,181, filed September 7, 2000, entitled "Method And Device For Monitoring And Analyzing Signals";

_____ U.S. Patent Application No. 10/805,484, filed March 22, 2004, entitled "Method And Device For Monitoring And Analyzing Signals"(which claims priority to U.S. Patent Application No. 09/671,739, filed September 29, 2000, which is a CIP of U.S. Patent Application No. 09/657,181) -- Publication No. 20040243540 – December 2, 2004;

_____ U.S. Patent Application No. 09/956,262, filed September 20, 2001, entitled "Improved Security Based on Subliminal and Supraliminal

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

Channels For Data Objects" -- Publication No. 20020056041 – May 9, 2002 (issued as U.S. Patent No. 7,127,615);

_____ U.S. Patent Application No. 11/518,806, filed September 11, 2006, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects";

_____ U.S. Patent Application No. 11/026,234, filed December 30, 2004, entitled "Z-Transform Implementation of Digital Watermarks" -- Publication No. 20050135615 – June 23, 2005 (issued as U.S. Patent No. 7,152,162);

_____ U.S. Patent Application No. 11/592,079, filed November 2, 2006, entitled "Linear Predictive Coding Implementation of Digital Watermarks" -- Publication No. 20070079131 – April 5, 2007;

_____ U.S. Patent Application No. 09/731,039, filed December 7, 2000, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects" -- Publication No. 20020071556 – June 13, 2002 (issued as U.S. Patent No. 7,177,429);

_____ U.S. Patent Application No. 11/647,861, filed December 29, 2006, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects" -- Publication No. 20070110240 – April 5, 2007;

_____ U.S. Patent No. 5,428,606, issued June 27, 1995, entitled "Digital Commodities Exchange";

_____ U.S. Patent No. 5,539,735, issued July 23, 1996, entitled "Digital Information Commodities Exchange";

_____ U.S. Patent No. 5,613,004, issued March 18, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent No. 5,687,236, issued November 11, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent No. 5,745,569, issued April 28, 1998, entitled "Method for Stega-Protection of Computer Code";

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

_____ U.S. Patent No. 5,822,432, issued October 13, 1998, entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System";

_____ U.S. Patent No. 5,889,868, issued July 2, 1996, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 5,905,800, issued May 18, 1999, entitled "Method & System for Digital Watermarking";

_____ U.S. Patent No. 6,078,664, issued June 20, 2000, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 6,205,249, issued March 20, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

_____ U.S. Patent No. 6,522,767, issued February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 6,598,162, issued July 22, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation";

_____ U.S. Patent No. 6,853,726, issued February 8, 2005, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 7,007,166, issued February 28, 2006, entitled "Method & System for Digital Watermarking";

_____ U.S. Patent No. 7,035,049, issued April 25, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

_____ U.S. Patent No. 7,095,874, issued August 22, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 7,107,451, issued September 12, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

_____ U.S. Patent No. 7,123,718, issued October 17, 2006, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems";

_____ U.S. Patent No. 7,127,615, issued October 24, 2006, "Improved Security Based on Subliminal and Supraliminal Channels for Data Objects";

_____ U.S. Patent No. 7,152,162, issued December 19, 2006, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 7,159,116, issued January 2, 2007, entitled "Systems, Methods and Devices for Trusted Transactions";

_____ U.S. Patent No. 7,177,429, issued February 13, 2007, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects"

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

FOREIGN PATENT DOCUMENTS

EXAMINER'S
INITIALS:

_____ PCT Application No. PCT/US95/08159, filed June 26, 1995, entitled, "Digital Information Commodities Exchange with Virtual Menuing";

_____ PCT Application No. PCT/US96/10257, filed June 7, 1996, entitled, "Steganographic Method and Device" -- corresponding to -- EPO Application No. 96919405.9, entitled "Steganographic Method and Device";

_____ PCT Application No. PCT/US97/00651, filed January 16, 1997, entitled, "Method for Stega-Cipher Protection of Computer Code" – corresponding to AU199718294A (not available);

_____ PCT Application No. PCT/US97/00652, filed January 17, 1997, entitled, "Method for an Encrypted Digital Watermark" – corresponding to AU199718295A (not available);

_____ PCT Application No. PCT/US97/11455, filed July 2, 1997, entitled, "Optimization Methods for the Insertion, Protection and Detection of Digital Watermarks in Digitized Data" – corresponding to AU199735881A (not available);

_____ PCT Application No. PCT/US99/07262, filed April 2, 1999, entitled, "Multiple Transform Utilization and Applications for Secure Digital Watermarking" – corresponding to -- Japan App. No. 2000-542907, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" (included herein);

_____ PCT Application No. PCT/US00/06522, filed March 14, 2000, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems";

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

_____ PCT Application No. PCT/US00/18411, filed July 5, 2000, entitled, "Copy Protection of Digital Data Combining Steganographic and Cryptographic Techniques" – corresponding to AU200060709A5 (not available);

_____ PCT Application No. PCT/US00/21189, filed August 4, 2000, entitled, "A Secure Personal Content Server";

_____ PCT Application No. PCT/US00/33126, filed December 7, 2000, entitled, "Systems, Methods and Devices for Trusted Transactions" – corresponding to AU200120659A5 (not available);

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. This Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed documents and information.

Respectfully submitted,

Date: October 17, 2007

By:

Scott A. Moskowitz
Tel# (305) 956-9041
Fax# (305) 956-9042

/Izunna Okeke/ 03/22/2010

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08B (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

OCT 19 2007 PATENT AND TRADEMARK OFFICE

Sheet 1 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		PCT International Search Report, completed Sept. 13, 1995; authorized officer Huy D. Vu (PCT/US95/08159) (2 pages)	
		PCT International Search Report, completed June 11, 1996; authorized officer Salvatore Cangialosi (PCT/US96/10257) (4 pages)	
		Supplementary European Search Report, completed Mar. 5, 2004; authorized officer J. Hazel (EP 96 91 9405) (1 page)	
		PCT International Search Report, completed April 4, 1997; authorized officer Bernarr Earl Gregory (PCT/US97/00651) (1 page)	
		PCT International Search Report, completed May 6, 1997; authorized officer Salvatore Cangialosi (PCT/US97/00652) (3 pages)	
		PCT International Search Report, completed Oct. 23, 1997; authorized officer David Cain (PCT/US97/11455) (1 page)	
		PCT International Search Report, completed July 12, 1999; authorized officer R. Hubeau (PCT/US99/07262) (3 pages)	
		PCT International Search Report, completed June 30, 2000; authorized officer Paul E. Callahan (PCT/US00/06522) (7 pages)	
		Supplementary European Search Report, completed June 27, 2002; authorized officer M. Schoeyer (EP 00 91 9398) (1 page)	
		PCT International Search Report, date of mailing Mar. 15, 2001; authorized officer Marja Brouwers (PCT/US00/18411) (5 pages)	

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08B (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		PCT International Search Report, completed July 20, 2001; authorized officer A. Sigolo (PCT/US00/18411) (5 pages)	
		PCT International Search Report, completed March 20, 2001; authorized officer P. Corcoran (PCT/US00/33126) (6 pages)	
		PCT International Search Report, completed January 26, 2001; authorized officer Gilberto Barron (PCT/US00/21189) (3 pages)	

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Schneier, Bruce, Applied Cryptography, 2nd Ed., John Wiley & Sons, pp. 9-10, 1996	
		Menezes, Alfred J., Handbook of Applied Crypography, CRC Press, p. 46, 1997	
		Merriam-Webster's Collegiate Dictionary, 10th Ed., Merriam Webster, Inc., p.207	
		Brealy, et al., Principles of Corporate Finance, "Appendix A-Using Option Valuation Models", 1984, pp. 448-449	
		Copeland, et al., Real Options:A Practioner's Guide, 2001 pp. 106-107, 201-202, 204-208.	
		Sarkar, M. "An Assessment of Pricing Mechanisms for the Internet-A Regulatory Imperative", presented MIT Workshop on Internet Economics, Mar. 1995 http://www.press.vmich.edu/iep/works/SarkAsses.html on	
		Crawford, D.W. "Pricing Network Usage:A Market for Bandwith of Market Communication?" presented MIT Workshop on Internet Economics, Mar. 1995 http://www.press.vmich.edu/iep/works/CrawMarket.html on March	
		LOW, S.H., "Equilibrium Allocation and Pricing of Variable Resources Among User-Suppliers", 1988. http://www.citesear.nj.nec.com/366503.html	
		Caronni, Germano, "Assuring Ownership Rights for Digital Images", published proceeds of reliable IT systems, v15 '95, H.H. Bruggemann and W. Gerhardt-Hackel (Ed.) Viewing Publishing Company, Germany, 1995	
		Zhao, Jian. "A WWW Service to Embed and Prove Digital Copyright Watermarks", Proc. of the european conf. on Mulitmedia Applications, Services & Techinques Louvain-La-Neyve, Belgium, May 1996	

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Gruhl,Daniel et al.,Echo Hiding. In Proceeding of the Workshop on Information Hiding. No. 1174 in Lecture Notes in Computer Science,Cambridge,England (May/June 1996)	
		Oomen,A.W.J. et al., A Variable Bit Rate Buried Data Channel for Compact Disc, J.Audio Eng.Sc.,Vol.43,No.1/2,pp. 23-28 (1995).	
		Ten Kate,W. et al., A New Surround-Stereo-Surround Coding Techniques, J. Audio Eng.Soc.,Vol. 40,No. 5,pp. 376-383 (1992)	
		Gerzon, Michael et al., A High Rate Buried Data Channel for Audio CD, presentation notes, Audio Engineering Soc. 94th Convention (1993).	
		Sklar,Bernard, Digital Communications, pp. 601-603 (1988)	
		Jayant, N.S. et al., Digital Coding of Waveforms, Prentice Hall Inc., Englewood Cliffs,NJ, pp. 486-509 (1984)	
		Bender, Walter R. et al., Techniques for Data Hiding, SPIE Int. Soc. Opt. Eng., Vol. 2420, pp. 164-173, 1995.	
		Zhao, Jian et al., Embedding Robust Labels into Images for Copyright Protection, (xp 000571976), pp. 242-251, 1995.	
		Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, p. 175, 1997.	
		Schneier, Bruce, Applied Cryptography, 1st Ed., pp. 67-68, 1994.	

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		ten Kate, W. et al., "Digital Audio Carrying Extra Information", IEEE, CH 2847-2/90/0000-1097, (1990)	
		van Schyndel, et al. A digital Watermark, IEEE Int'l Computer Processing Conference, Austin,TX, Nov 13-16, 1994, pp. 86-90	
		Smith, et al. Modulation and Information Hiding in Images, Springer Verlag, 1st Int'l Workshop, Cambridge, UK, May 30-June 1,1996, pp. 207-227	
		Kutter, Martin et al., Digital Signature of Color Images Using Amplitude Modulation, SPIE-E197, vol. 3022, pp. 518-527	
		Puate, Joan et al., Using Fractal Compression Scheme to Embed a Digital Signature into an Image, SPIE-96 Proceedings, vol. 2915, Mar. 1997, pp. 108-118	
		Swanson, Mitchell D.,et al., Transparent Robust Image Watermarking, Proc. of the 1996 IEEE Int'l Conf. on Image Processing, Vol. 111, 1996 , pp. 211-214	
		Swanson, Mitchell D., et al. Robust Data Hiding for Images, 7th IEEE Digital Signal Processing Workshop, Leon, Norway. Sept. 1-4,1996, pp. 37-40	
		Zhao, Jian et al., Embedding Robust Labels into Images for Copyright Protection, Proceeding of the Know Right '95 Conference, pp. 242-251.	
		Koch, E., et al., Towards Robust and Hidden Image Copyright Labeling, 1995 IEEE Workshop on Nonlinear Signal and Image Processing, Jun. 1995 Neos Marmaras pp 4	
		Van Schyandel, et al., Towards a Robust Digital Watermark, Second Asain Image Processing Conference, Dec. 6-8,1995,Singapore, Vol. 2,pp. 504-508	

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 6 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Tirkel,A.Z., A Two-Dimensional Digital Watermark, DICTA '95, Univ. of Queensland, Brisbane, Dec. 5-8,1995, pp. 7	
		Tirkel,A.Z., Image Watermarking-A Spread Spectrum Application, ISSSTA '96, Sept.96, Mainz, German, pp. 6.	
		O'Ruanaidh, et al. Watermarking Digital Images for Copyright Protection, IEEE Proceedings, Vol. 143, No. 4, Aug. 96, pp. 250-256.	
		Cox, et al., Secure Spread Spectrum Watermarking for Multimedia, NEC Research Institude, Techinal Report 95-10, pp. 33	
		Kahn, D., The Code Breakers, The MacMillan Company, 1969, pp. xIII, 81-83,513,515,522-526,863.	
		Boney, et al., Digital Watermarks for Audio Signals, EVSIPCO, 96, pp. 473-480.	
		Dept. of Electrical Engineering, Del Ft University of Technology, Del ft The Netherlands,Cr.C. Langelaar et al.,Copy Protection for Mulitmedia Data based on Labeling Techniques ,July 1996, 9 pp	
		F. Hartung, et al., Digital Watermarking of Raw and Compressed Video, SPIE Vol. 2952, pp. 205-213.	
		Craver, et al., Can Invisible Watermarks Resolve Rightful Ownerships? IBM Research Report, RC 20509 (July 25,1996) 21 pp.	
		Press, et al., Numerical Recipes In C, Cambridge Univ. Press, 1988, pp. 398-417.	

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 7 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Pohlmann, Ken C., Principles of Digital Audio, 3rd Ed., 1995, pp. 32-37, 40-48,138,147-149,332,333,364, 499-501,508-509,564-571.	
		Pohlmann, Ken C., Principles of Digital Audio, 2nd Ed., 1991, pp. 1-9,19-25,30-33,41-48,54-57,86-107,375-387.	
		Schneier, Bruce, Applied Cryptography, John Wiley & Sons, inc. , New York,1994, pp. 68,69,387-392,1-57,273-275,321-324.	
		Boney, et al., Digital Watermarks for Audio Signals, Proceedings of the International Conf. on Multimedia Computing and Systems, June 17-23,1996,Hiroshima, Japan, 0-8186-7436-9196, pp. 473-480.	
		Johnson, et al., Transform Permuted Watermarking for Copyright Protection of Digital Video, IEEE Globecom 1998, Nov 8-12,1998, New York, New York, Vol. 2,1998, pp. 684-689,(ISBN 0-7803-4985-7)	
		Rivest, et al., "Pay Word and Micromint: Two Simple Micropayment Schemes, "MIT Laboratory for Computer Science, Cambridge, MA, May 7,1996, pp. 1-18	
		Bender, et al., Techniques for Data Hiding, IBM Systems Journal, Vol. 35, Nos 3 & 4,1996,pp. 313-336.	
		Moskowitz, Bandwith as Currency, IEEE Multimedia, Jan-Mar 2003, pp. 14-21.	
		Moskowitz, Multimedia Security Technologies for Digital Rights Management, 2006, Academic Press, "Introduction-Digital Rights Management" pp. 3-22	

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 8 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Tomsich, et al., "Towards a secure and de-centralized digital watermarking infrastructure for the protection of Intellectual Property", in Electronic Commerce and Web Technologies, Proceedings (ECWEB	
		Moskowitz, "What is Acceptable Quality in the Application of Digital Watermarking: Trade-offs of Security, Robustness and Quality", IEEE Computer Society Proceedings of ITCC 2002 April 10, 2002 pp. 80-84	
		Lemma, et al. "Secure Watermark Embedding through Partial Encryption", International Workshop on Digital Watermarking ("IWDW" 2006). Springer Lecture Notes in Computer Science 2006. (to appear) 13	
		Kocher, et al., "Self Protecting Digital Content", Technical Report from the CRI Content Security Research Initiative, Crytography Research, Inc. 2002-2003. 14 pages.	
		Sirbu, M. et al., "Net Bill: An Internet Commerce System Optimized for Network Delivered Services", Digest of Papers of the Computer Society Computer Conference (Spring). 5 March 1995. pp. 20-25. vol. CONF40.	
		Schunter, M. et al., "A Status Report on the SEMPER framework for Secure Electronic Commerce", Computer Networks and ISDN Systems, 30 Sept 1998 pp. 1501-1510 Vol. 30 No. 16-18 NL North Holland	
		Konrad, K. et al., "Trust and Elecronic Commerce-more than a techinal problem," Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems 19-22 October 1999 pp. 360-365 Lausanne	
		Kini, a. et al., "Trust in Electronic Commerce: Definition and Theoretical Considerations", Proceedings of the 31st Hawaii Int'l Conf on System Sciences (Cat. No. 98TB100216). 6-9 January 1998. pp. 51-61. Los	
		Steinauer D. D., et al., "Trust and Traceability in Electronic Commerce", Standard View, Sept 1997, pp 118-124, vol. 5 No. 3, ACM, USA	
		Hartung, et al. "Multimedia Watermarking Techniques", Proceedings of the IEEE, Special Issue, Identification & Protection of Multimedia Information, pp.1079-1107 July 1999 Vol. 87 No. 7 IEEE	

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08B (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 9 of 9

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Rivest,et al., PayWord and MicroMint: Two simple micropayment schemes, MIT Laboratory for Computer Science, Cambridge, MA 02139, April 27,2001, pp. 1-18.	
		Horowitz, et al., The Art of Electronics, 2nd Ed., 1989, pp.7.	
		Delaigle, J.-F., et al. "Digital Watermarking," Proceedings of the SPIE, vol. 2659, Feb 1, 1996, pp. 99-110 (Abstract).	
		Schneider, M., et al. "Robust Content Based Digital Signature for Image Authentication," Proceedings of the International Conference on Image Processing (IC. Lausanne), Sept. 16-19, 1996, pp. 227-230, IEEE ISBN:	
		Cox, I. J., et al. "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, Vol. 6 No. 12, Dec. 1, 1997, pp. 1673-1686.	
		Wong, Ping Wah. "A Public Key Watermark for Image Verification and Authentication," IEEE International Conference on Image Processing, Vol. 1, Oct. 4-7, 1998, pp. 455-459.	
		Fabien A.P. Petitcolas, Ross J. Anderson and Markkus G. Kuhn, "Attacks on Copyright Marking Systems," LNCS, Vol. 1525, April 14-17, 1998, pp. 218-238, ISBN: 3-540-65386-4	
		Ross Anderson, "Stretching the Limits of Steganography," LNCS, Vol. 1174, May/June 1996, 10 pages, ISBN: 3-540-61996-8.	
		Joseph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", pre-publication, Summer 1997, 4 pages	
		Joseph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", Submitted to Signal Processing, August 21, 1997, 19 pages	

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

OIPE IAP OCT 19 2007 PATENT & TRADEMARK OFFICE

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Numb	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number / Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,939,515	07/03/1990	Adelson	
		US-5,161,210	11/03/1992	Druyvesteyn,et.al.	
		US-5,450,490	09/12/1995	Jensen et.al.	
		US-5,530,751	06/25/1996	Morris	
		US-5,579,124	11/26/1996	Aijala et.al	
		US-5,721,788	02/24/1998	Powell et.al.	
		US-5,828,325	10/27/1998	Wolose Wicz et.al.	
		US-5,912,972	06/15/1999	Barton	
		US-5,930,377	07/27/1999	Powell et.al.	
		US-5,583,488	12/10/1996	Sala et.al.	
		US-5,748,783	05/05/1998	Rhoads	
		US-6,330,672	12/11/2001	Shur	
		US-5,243,423	09/07/1993	DeJean et.al.	
		US-5,319,735	06/07/1994	Preuss et.al	
		US-5,113,437	05/12/1992	Best et.al.	
		US-4,876,617	10/24/1989	Best et.al.	
		US-5,379,345	01/03/1995	Greenberg	
		US-5,646,997	07/08/1997	Barton	
		US-4,672,605	06/09/1987	Hustig et.al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document / Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		European Patent No. EP0565947A1	10/20/1993	Kuusama, Juha		
		WO 95/14289	05/26/1995	Rhoads, Geoffrey		
		European Patent No. 0581317A2	02/02/1994	Powell, Robert et.al.		
		European Patent No. 0372601A1	06/13/1990	Druyvesteyn, Wm. et.al.		
		W098/37513	08/27/1998	Biggar, Michael et.al.		
		European Patent No. 0651554A	05/03/1995	Eastman Kodak Co.		

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,748,668	05/31/1998	Shamir, et.al.	
		US-4,789,928	12/06/1988	Fujisaki	
		US-4,908,873	03/13/1990	Philibert, et.al.	
		US-4,980,782	12/25/1990	Ginkel	
		US-5,073,925	12/17/1991	Nagata, et.al.	
		US-5,243,515	09/07/1993	Lee	
		US-5,287,407	02/15/1994	Holmes	
		US-5,428,606	06/27/1995	Moskowitz	
		US-5,365,586	11/15/1994	Indeck, et.al.	
		US-5,394,324	02/28/1995	Clearwater	
		US-5,408,505	04/18/1995	Indeck, et.al	
		US-5,412,718	05/02/1995	Narasimhalv, et.al	
		US-5,487,168	01/23/1996	Geiner, et.al.	
		US-5,493,677	02/20/1996	Balogh, et.al	
		US-5,530,759	06/25/1996	Braudaway, et.al	
		US-5,606,609	02/25/1997	Houser, et.al.	
		US-5,613,004	03/18/1997	Cooperman, et.al.	
		US-5,617,119	04/01/1997	Briggs, et.al	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		WO 99/62044	12/02/1999	Handel, Theodore et.al		
		WIPO 96/29795	09/26/1996	Micali		
		WIPO 97/24833	07/10/1997	Micali		
		EP 0649261	04/19/1995	Enari		
		NL 100523	09/1998			

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,528,588	07/09/1985	Lofberg	
		US-5,832,119	11/03/1998	Rhoads	
		US-5,859,920	01/12/1999	Daly et.al	
		US-4,979,210	12/18/1990	Nagata et.al	
		US-5,774,452	06/30/1998	Wolosewicz	
		US-4,405,829	09/20/1983	Rivest et.al	
		US-6,330,335	12/11/2001	Rhoads	
		US-3,986,624	10/19/1976	Cates Jr. et.al	
		US-5,363,448	11/08/1994	Koopman et.al	
		US-5,568,570	10/22/1996	Rabbani	
		US-5,636,292	06/03/1997	Rhoads	
		US-4,972,471	11/20/1990	Gross et.al.	
		US-5,893,067	04/06/1999	Bender et.al.	
		US-5,689,587	11/18/1997	Bender et.al.	
		US-3,984,624	10/05/1976	Waggener	
		US-4,038,596	07/26/1977	Lee	
		US-4,200,770	04/29/1980	Hellman, et.al.	
		US-4,218,582	08/19/1980	Hellman, et.al.	
		US-4,424,414	01/03/1984	Hellman, et.al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		WO 9744736	11/27/1997	Wehrenberg		
		WO 9952271	10/14/1999	Moskowitz		
		WO 9963443	12/09/1999	Ho,Anthony Tung Shuen		

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,640,569	06/17/1997	Miller, et.al.	
		US-5,659,726	08/19/1997	Sandford,II, et.al	
		US-5,664,018	09/02/1997	Leighton	
		US-5,687,236	11/11/1997	Moskowitz, et.al.	
		US-5,734,752	03/31/1998	Knox	
		US-5,745,569	04/28/1998	Moskowitz, et.al	
		US-5,506,795	04/09/1996	Yamakawa	
		US-5,680,462	10/21/1997	Miller, et.al	
		US-5,696,828	12/09/1997	Koopman, Jr.	
		US-5,740,244	04/14/1998	Indeck, et.al.	
		US-5,751,811	05/12/1998	Koopman, Jr.	
		US-5,757,923	05/26/1998	Koopman, Jr.	
		US-5,889,868	03/30/1999	Moskowitz, et.al.	
		US-6,208,745	03/27/2001	Florenio, et.al.	
		US-6,285,775	09/04/2001	Wu, et.al.	
		US-6,385,329	05/07/2002	Sharma, et.al	
		US-6,530,021	03/04/2003	Epstein, et.al.	
		US-6,425,081	07/23/2002	Iwamura	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,522,769	02/18/2003	Rhoads, et.al.	
		US-2005/0160271	07/21/2005	Brundage, et.al	
		US-6,665,489	12/16/2003	Collart	
		US-2004/0128514	07/01/2004	Rhoads	
		US-2004/0037449	02/26/2004	Davis, et.al.	
		US-6,823,455	11/23/2004	Macy, et.al.	
		US-2003/0133702	07/17/2003	Collart	
		US-6,668,246	12/23/2003	Yeung, et.al.	
		US-6,405,203	06/11/2002	Collart	
		US-6,141,754	10/31/2000	Choy	
		US-6,493,457	12/10/2002	Quackenbush	
		US-5,629,980	05/13/1997	Stefik, et.al.	
		US-5,943,422	08/24/1999	Van Wie, et.al.	
		US-5,636,276	06/03/1997	Brugger	
		US-5,341,429	08/23/1994	Stringer, et.al.	
		US-6,754,822	06/22/2004	Zhao	
		US-6,131,162	10/10/2000	Yoshiura et.al.	
		US-7,058,570	06/06/2006	Yu, et.al.	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 6 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,930,369	07/27/1999	Cox, et.al.	
		US-6,415,041	07/02/2002	Oami, et.al.	
		US-6,141,753	10/31/2000	Zhao, et.al.	
		US-2002/0097873	07/25/2002	Petrovic	
		US-6,785,815	08/31/2004	Serret-Avila, et.al.	
		US-6,523,113	02/18/2003	Wehrenberg	
		US-6,233,347	05/15/2001	Chen, et.al.	
		US-6,233,684	05/15/2001	Stefik, et.al.	
		US-2006/0013395	01/19/2006	Brundage, et.al.	
		US-7,043,050	05/09/2006	Yuval	
		US-5,809,160	09/15/1998	Powell, et.al.	
		US-6,272,634	08/07/2001	Tewfik, et.al.	
		US-6,282,650	08/28/2001	Davis	
		US-6,557,103	04/29/2003	Boncelet, Jr., et.al.	
		US-2003/0126445	07/03/2003	Wehrenberg	
		US-6,978,370	12/20/2005	Kocher	
		US-2006/0005029	01/05/2006	Petrovic, et.al.	
		US-6,278,791	08/21/2001	Honsinger, et.al.	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 7 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,598,162	07/22/2003	Moskowitz	
		US-6,275,988	08/14/2001	Nagashima, et al.	
		US-6,051,029	04/18/2000	Paterson, et al.	
		US-5,917,915	06/29/1999	Hirose	
		US-6,775,772	08/10/2004	Binding, et al.	
		US-6,668,246	12/23/2003	Yeung, et al.	
		US-6,351,765	02/26/2002	Pietropaolo, et al.	
		US-6,049,838	04/11/2000	Miller, et al.	
		US-5,398,285	03/14/1995	Borgelt, et al.	
		US-5,737,733	04/07/1998	Eller	
		US-2002/0103883	08/01/2002	Haverstock, et al.	
		US-5,673,316	09/30/1997	Auerbach, et al.	
		US-6,647,424	11/11/2003	Pearson, et al.	
		US-6,977,894	12/20/2005	Achilles, et al.	
		US-6,453,252	09/17/2002	Laroche	
		US-5,077,665	12/31/1991	Silverman, et al.	
		US-5,136,581	08/04/1992	Muehrcke	
		US-5,341,477	08/23/1994	Pitkin, et al.	
		US-5,581,703	12/03/1996	Baugher, et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 8 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,548,579	08/20/1996	Lebrun, et al.	
		US-5,905,975	05/18/1999	Ausubel	
		US-6,457,058	09/24/2002	Ullum et al.	
		US-6,381,618	04/30/2002	Jones et al.	
		US-2002/0026343	02/28/2002	Duenke	
		US-6,230,268	05/08/2001	Miwa et al.	
		US-6,199,058	03/06/2001	Wong et al.	
		US-5,920,900	07/06/1999	Poole et al.	
		US-5,884,033	03/16/1999	Duvall et al.	
		US-5,478,990	12/26/1995	Montanari et al.	
		US-6,430,302	08/06/2002	Rhoads	
		US-6,725,372	04/20/2004	Lewis et al.	
		US-6,606,393	08/12/2003	Xie et al.	
		US-6,584,125	06/24/2003	Katto	
		US-6,442,283	08/27/2002	Tewfik et al.	
		US-6,377,625	04/23/2002	Kim	
		US-6,282,300	08/28/2001	Bloom et al.	
		US-6,205,249	03/20/2001	Moskowitz	
		US-6,029,126	02/22/2000	Malvar	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 9 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,754,697	05/19/1998	Fu et al.	
		US-5,479,210	12/26/1995	Cawley et al.	
		US-3,947,825	03/30/1976	Cassada	
		US-5,903,721	05/11/1999	Sixtus	
		US-5,790,677	08/04/1998	Fox et al.	
		US-5,243,515	09/07/1993	Clearwater	
		US-4,339,134	07/13/1982	Macheel	
		US-4,827,508	05/02/1989	Shear	
		US-4,896,275	01/23/1990	Jackson	
		US-4,977,594	12/11/1990	Shear	
		US-5,050,213	09/17/1991	Shear	
		US-5,369,707	11/29/1994	Follendore, III	
		US-5,406,627	04/11/1995	Thompson et al.	
		US-5,410,598	04/25/1995	Shear	
		US-5,469,536	11/21/1995	Blank	
		US-5,497,419	03/05/1996	Hill	
		US-5,513,261	04/30/1996	Maher	
		US-5,530,739	06/25/1996	Okada	
		US-5,598,470	01/28/1997	Cooper et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 10 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Num	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,625,690	04/29/1997	Michel et al.	
		US-5,633,932	05/27/1997	Davis et al.	
		US-5,719,937	02/17/1998	Warren et al.	
		US-5,737,416	04/07/1998	Cooper et al.	
		US-5,765,152	06/09/1998	Erickson	
		US-5,799,083	08/25/1998	Brothers et al.	
		US-5,973,731	10/26/1999	Schwab	
		US-5,894,521	04/13/1999	Conley	
		US-5,905,800	05/18/1999	Moskowitz et al.	
		US-5,963,909	10/05/1999	Warren et al.	
		US-5,974,141	10/26/1999	Saito	
		US-5,999,217	12/07/1999	Berners-Lee	
		US-6,041,316	03/21/2000	Allen	
		US-6,081,251	06/27/2000	Sakai et al.	
		US-6,278,780	08/21/2001	Shimada	
		US-6,301,663	10/09/2001	Kato et al.	
		US-6,240,121	05/29/2001	Senoh	
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08A (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 11 of 12

Complete if Known	
Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Numl	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Pate... Applicant of Cited Document	Relevant Passages or Relevant Figures Appear
		US- 6,088,455	07/11/2000	Logan et al.	
		US- 5,634,040	05/27/1997	Her et al.	
		US- 6,381,747	04/30/2002	Wonfor et al.	
		US- 4,969,204	11/06/1990	Melnychuck et al.	
		US- 6,966,002	11/15/2005	Torrubia-Saez	
		US- 6,263,313	07/17/2001	Milstead, et al.	
		US- 7,093,295	08/15/2006	Saito	
		US- 6,587,837	07/01/2003	Spagna et al.	
		US- 6,931,534	08/16/2005	Jandel et al.	
		US- 2004/0049695	03/11/2004	Choi et al.	
		US- 2004/0083369	04/29/2004	Erlingsson et al.	
		US- 5,677,952	10/14/1997	Blakely et al.	
		US- 5,768,396	06/16/1998	Sone	
		US- 7,266,697	09/04/2007	Kirovski et al.	
		US- 5,136,646	08/04/1992	Haber et al.	
		US- 5,136,647	08/04/1992	Haber et al.	
		US- 7,206,649	04/17/2007	Kirovski et al.	
		US- 6,532,284	03/11/2003	Walker et al.	
		US- 7,020,285	03/28/2006	Kirovski et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Izunna Okeke/	Date Considered	03/31/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08A (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Tr
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of inf

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 12 of 12

Application Number	11/895,388
Filing Date	August 24, 2007
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2132
Examiner Name	NA
Attorney Docket Num	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- 7,046,808	05/12/2006	Metois et al.	
		US- 6,430,301	08/06/2002	Petrovic	
		US- 2004/0059918	03/25/2004	Xu	
		US- 6,345,100	02/05/2002	Levine	
		US- 2004/0093521	05/13/2004	Hamadeh et al.	
		US- 2007/0083467	04/12/2007	Lindahl et al.	
		US- 7,231,524	06/12/2007	Burns	
		US- 2005/0246554	11/03/2005	Batson	
		US- 6,668,325	02/23/2003	Collberg et al.	
		US- 7,050,396	05/23/2006	Cohen et al.	
		US- 6,842,862	01/11/2005	Chow et al.	
		US- 7,051,208	05/23/2006	Venkatesan et al.	
		US- 7,240,210	07/03/2007	Michak et al.	
		US- 7,150,003	12/12/2006	Naumovich et al.	
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Izunna Okeke/	Date Considered	03/22/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

SEP 08 2009 PATENT & TRADEMARK OFFICE

PTO/SB/08A (01-08)
Approved for use through 01/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 4

Complete if Known	
Application Number	11/895,388
Filing Date	Aug 24, 2007
First Named Inventor	Scott A. Moskowitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	80391.0003Cont 2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- [redacted]	[redacted]	[redacted]	
		US- 6,389,538	05/14/2002	Gruse et al.	
		US- 5,513,126	04/30/1996	Harkins et al.	
		US- 5,657,461	08/12/1997	Harkins et al.	
		US- 4,390,898	06/28/1983	Bond et al.	
		US- 5,471,533	11/28/1995	Wang et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		EP 1547337 B1	03/22/2006	Erlingsson et al.		
		EP 1354276 B1	12/12/2007	Bum et al.		

Examiner Signature	/Izunna Okeke/	Date Considered	03/22/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08a (01-08)
Approved for use through 05/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 4

Complete if Known	
Application Number	11/895 388
Filing Date	August 24, 2007
First Named Inventor	Scott A Moskowitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- 6,044,471	03/28/2000	Colvin	
		US- 7,103,184	09/05/2006	Jian	
		US- 7,233,669	06/19/2007	Candelore	
		US- 6,446,211	09/03/2002	Colvin	
		US- 6,484,264	11/19/2002	Colvin	
		US- 6,502,195	12/31/2002	Colvin	
		US- 6,785,825	08/31/2004	Colvin	
		US- 6,792,548	09/14/2004	Colvin	
		US- 6,792,549	09/14/2004	Colvin	
		US- 6,795,925	09/21/2004	Colvin	
		US- 6,799,277	09/28/2004	Colvin	
		US- 6,813,717	11/02/2004	Colvin	
		US- 6,813,718	11/02/2004	Colvin	
		US- 6,857,078	02/15/2005	Colvin	
		US- 6,986,063	01/10/2006	Colvin	
		US- 2004/0117628	06/17/2004	Colvin	
		US- 2004/0117664	06/17/2004	Colvin	
		US- 2004/0225894	11/11/2004	Colvin	
		US- [redacted]	[redacted]	[redacted]	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Izunna Okeke/	Date Considered	03/22/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 4

Complete if Known	
Application Number	11/895,388
Filing Date	Aug 24 2007
First Named Inventor	Scott A Moskowitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-7,177,430	02/13/2007	Kim	
		US-5,210,820	05/11/1993	Kenyon	
		US-2001/0043594	11/22/2001	Ogawa et al.	
		US-6,658,010	12/03/2003	Enns et al.	
		US-6,463,468	10/08/2002	Buch et al.	
		US-5,862,260	01/19/1999	Rhoads	
		US-6,373,960	04/16/2002	Conover et al.	
		US-2007/0253594	11/01/2007	Lu et al.	
		US-2006/0041753	02/23/2006	Haitsma	
		US-6,784,354	08/31/2004	Lu et al.	
		US-2007/0127717	06/07/2007	Herre et al.	
		US-2006/0013451	01/19/2006	Haitsma	
		US-5,918,223	06/29/1999	Blum	
		US-5,765,152	06/09/1998	Erickson	
		US-5,142,576	08/25/1992	Nadan	
		US-5,923,763	07/13/1999	Walker et al.	
		US-2004/0028222	02/12/2004	Sewell et al.	
		US-7,460,994	12/02/2008	Herre et al.	
		US-7,107,451	09/12/2006	Moskowitz	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Izunna Okeke/	Date Considered	03/22/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 4

Complete if Known	
Application Number	11/894,388
Filing Date	Aug 24, 2007
First Named Inventor	Scott A Moskowitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	8039I.0002 CONT2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,748,783	05/05/1998	Rhoads	
		US-5,850,481	12/15/1998	Rhoads	
		US-5,860,099	01/12/1999	Milios et al.	
		US-6,363,483	03/26/2002	Keshav	
		US-7,162,642	01/09/2007	Schumann et al.	
		US-6,834,308	12/21/2004	Ikezoye et al.	
		US-6,983,337	11/22/2005	Wold	
		US-7,363,278	04/22/2008	Schmelzer et al.	
		US-2002/0073043	06/13/2002	Herman et al.	
		US-2004/0125983	07/01/2004	Reed et al.	
		US-2002/0161741	10/31/2002	Wang et al.	
		US-7,289,643	10/30/2007	Brunk et al.	
		US-7,286,451	10/23/2007	Wirtz et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Izunna Okeke/	Date Considered	03/22/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08B (01-08)
Approved for use through 01/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	11/895,388
Filing Date	Aug 24, 2007
First Named Inventor	Scott A. Mosenlitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	80391.0003.CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		~~PCT International Search Report, completed July 26, 2001; authorized officer A. Sigolo (PCT/US00/18111) (5 pages)~~	
		~~PCT International Search Report, completed March 29, 2001; authorized officer P. Corcoran (PCT/US00/22100) (3 pages)~~	
		~~PCT International Search Report, completed January 26, 2001; authorized officer A. Sigolo (PCT/US00/21100) (3 pages)~~	
		European Search Report, completed October 15, 2007; authorized officer James Hazel (EP 07 11 2420) (9 pages)	

Examiner Signature	/Izunna Okeke/	Date Considered	03/22/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	11/895,388
Filing Date	Aug 24, 2007
First Named Inventor	Scott A. Moskowitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	80391.0003CONT2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		STAIND (The Singles 1996-2006), Warner Music - Atlantic, Pre-Release CD image, 2006, 1 page.	
		Arctic Monkeys (Whatever People Say I Am, That's What I'm Not), Domino Recording Co. Ltd., Pre-Release CD image, 2005, 1 page.	
		Radiohead ("Hail To The Thief"), EMI Music Group - Capitol, Pre-Release CD image, 2003, 1 page.	
		OASIS (Dig Out Your Soul), Big Brother Recordings Ltd., Promotion CD image, 2009, 1 page.	

Examiner Signature	/Izunna Okeke/	Date Considered	03/22/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	11/895,388
Filing Date	Aug 24, 2007
First Named Inventor	Seth A Moskowitz
Art Unit	2432
Examiner Name	NA
Attorney Docket Number	80391.0003cont2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Rivest, R. "Chaffing and Winnowing: Confidentiality without Encryption", MIT Lab for Computer Science, http://people.csail.mit.edu/rivest/Chaffing.txt, April 24, 1998, 9 pp.	
		PortalPlayer, PP502 digital media management system-on-chip, May 1, 2003, 4 pp.	
		VeriDisc, "The search for a Rational Solution to Digital Rights Management (DRM)", http://64.244.235.240/news/whitepaper/docs/veridisc_white_paper.pdf, 2001, 15 pp.	
		Cayre, et al., "Kerckhoff's-Based Embedding Security Classes for WOA Data Hiding". IEEE Transactions on Information Forensics and Security, Vol. 3 No. 1, March 2008, 15 pp.	
		Wayback Machine, dated January 17, 1999, http://web.archive.org/web/19990117020420/http://www.netzero.com/, accessed on February 19, 2008.	
		Namgoong, H., "An Integrated Approach to Legacy Data for Multimedia Applications", Proceedings of the 23rd EUROMICRO Conference, Vol., Issue 1-4, September, 1997, pp 387-391	
		Wayback Machine, dated August 26, 2007, http://web.archive.org/web/20070826151732/http://www.screenplaysmag.com/tabid/96/articleType/ArticleView/articleId/495/Default.aspx/	
		"YouTube Copyright Policy: Video Identification tool - YouTube Help", accessed June 4, 2009, http://www.google.com/support/youtube/bin/answer.py?h1=en&answer=83766, 3 pp.	

Examiner Signature	/Izunna Okeke/	Date Considered	03/22/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.O./

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 2103

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/895,388	08/24/2007 RULE	713	2432	80391.0003CONT2

APPLICANTS

Scott A. Moskowitz, Sunny Isles Beach, FL;

**** CONTINUING DATA ***************************

This application is a DIV of 10/602,777 06/25/2003 PAT 7,664,263
which is a CON of 09/046,627 03/24/1998 PAT 6,598,162
which is a CIP of 08/587,943 01/17/1996 PAT 5,745,569

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
09/13/2007

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ Yes ☑ No	☐ Yes ☐ No	/IZUNNA OKEKE/ Examiner's Signature	☐ Initials	FL	1	31	5

ADDRESS

Scott A. Moskowitz
#2505
16711 Collins Avenue
Sunny Isless Beach, FL 33160
UNITED STATES

TITLE

Data protection method and device

FILING FEE RECEIVED		
1247	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S3	38	((reduced or low $3) near3 (quality)) same ((digital near3 content) or audio or video) same (watemark or steganograph$3 or (copy near3 protect $3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 09:18
S4	209	((reduced or low $3) near3 (quality)) same ((digital near3 content) or audio or video) and (watemark or steganograph$3 or (copy near3 protect $3)) and (key same (encrypt$3 or scranmbl$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 09:41
S5	91	((play$3 or reproduc$3 or copy $3) same (reduced or low$3) near3 (quality)) same ((digital near3 content) or audio or video) and (watemark or steganograph$3 or (copy near3 protect $3)) and (key same (encrypt$3 or scranmbl$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 09:52
S6	277	((reduced or low$3 or degraded) near3 (quality)) same ((digital near3 content) or audio or video) and ((endode or decode) same key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 10:55

S7	2270	380/201	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 10:58
S8	1206	380/210	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 10:59
S9	453	380/217	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 10:59
S10	77	380/218	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 10:59
S11	105	380/236	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 10:59
S12	8	S6 and S7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 11:00
S13	13	S6 and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 11:00
S14	5	S6 and S9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 11:00
S16	2	S6 and S11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 11:00

DISH-Blue Spike-842
Exhibit 1004, Page 1220

S17	75	scott near2 moskowitz.inv.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 11:47
S18	60	(unauthorized near3 (user or device or player)) and ((digital near3 content) or audio or video) and ((encode or decode) same key) and ((reduced or low or degraded) near3 quality)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 12:47
S19	415	((reduced or low$3 or degraded) near3 (quality)) same ((digital near3 content) or audio or video) and ((encode or decode) same key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 12:47
S20	166	(((degrad$3 or reduc$3) near3 (quality)) same ((digital near3 content) or video or audio)) and (unauthorized near3 (user or player or device))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 13:06
S21	8860	(((degrad$3 or reduc$3) near3 (quality)) same ((digital near3 content) or video or audio))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 13:17
S22	79	S7 and S21	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 13:18
S23	3490	(((degrad$3 or reduc$3) near3 (quality)) near3 ((digital near3 content) or video or audio))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 13:18

DISH-Blue Spike-842
Exhibit 1004, Page 1221

S24	32	S7 and S23	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 13:18
S25	73	380/206	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 13:21
S26	39	380/226	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 13:21
S27	387	380/232	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2009/11/03 13:21
S31	1	"11895388"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/18 07:46
S37	492	(software with (copy near3 protect $3)) and (key same authoriz$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 09:10
S38	84	(software with (copy near3 protect $3)) and (key same authoriz$5) and (digital near3 watermark)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 09:10
S39	2149	(software near3 protect$3) and (key same authoriz$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 09:11

DISH-Blue Spike-842
Exhibit 1004, Page 1222

S41	41	("4558176" | "4644493" | "4652990" | "4688169" | "4796220" | "4866769" | "5109413" | "5113518" | "5182770" | "5199066" | "5267311" | "5276738" | "5343524" | "5402492" | "5615263" | "5619408" | "5675645").PN. OR ("6067622").URPN.	US-PGPUB; USPAT; USOCR	AND	ON	2010/03/22 09:40
S42	2023	713/165	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:58
S43	6293	713/176	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:58
S44	1123	713/161	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:58
S45	2403	380/201	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:58
S46	365	380/228	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:58
S47	268	380/229	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:58

DISH-Blue Spike-842
Exhibit 1004, Page 1223

S48	492	(software with (copy near3 protect $3)) and (key same authoriz$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:59
S49	492	S48	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:59
S50	22	S48 and S42	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:59
S51	39	S48 and S43	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:59
S52	8	S48 and S44	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:59
S53	62	S48 and S45	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:59
S54	12	S48 and S46	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:59
S55	6	S48 and S47	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 20:59
S56	2149	(software near3 protect$3) and (key same authoriz$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:06

S57	2149	S56	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:06
S58	112	S56 and S42	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:06
S59	172	S56 and S43	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:06
S60	37	S56 and S44	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:06
S61	113	S56 and S45	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:06
S62	21	S56 and S46	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:06
S63	11	S56 and S47	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:06
S64	144	(software with (copy near3 protect $3)) and (digital near3 watermark)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:15
S66	181	(software with (copy near3 protect $3)) and (digital same watermark)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:16

S67	75	(software with (copy near3 protect $3)) and (authenticat$5 same watermark)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:16
S68	493	(software with (copy near3 protect $3)) and (authenticat$5 same key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:16
S69	107	(software with (copy near3 protect $3)) and (authoriz $5 same watermark)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:16
S70	492	(software with (copy near3 protect $3)) and (authoriz $5 same key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:16
S71	2054	((copy near3 protect $3)) and (key same authoriz$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:17
S72	51	((copy near3 protect $3)) and ((key same authoriz$5) with watermark)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:17
S73	130	((copy near3 protect $3)) and ((key same authoriz$5) same watermark)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:31
S74	1434	(software with (copy near3 protect $3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:32
S75	44	S74 and S42	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:32

DISH-Blue Spike-842
Exhibit 1004, Page 1226

S76	77	S74 and S43	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:32
S77	17	S74 and S44	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:32
S78	120	S74 and S45	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:32
S79	13	S74 and S46	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:32
S80	7	S74 and S47	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:32
S81	1770	705/57	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:34
S82	106	S74 and S81	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:34
S83	188	S71 and S81	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:34
S84	63	S70 and S81	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:34

DISH-Blue Spike-842
Exhibit 1004, Page 1227

S85	59	S68 and S81	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:34
S86	135	S56 and S81	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	AND	ON	2010/03/22 21:34

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S29	5	(scott near2 moskowitz.inv.) and (degraded.clm.)	USPAT; UPAD	AND	ON	2009/11/03 11:51
S30	3	(scott near2 moskowitz.inv.) and (degraded adj quality.clm.)	USPAT; UPAD	AND	ON	2009/11/03 11:51
S35	26	(scott near2 moskowitz.inv.) and (watermark.clm.)	USPAT; UPAD	AND	ON	2010/03/22 07:17
S36	25	(scott near2 moskowitz.inv.) and (key.clm.)	USPAT; UPAD	AND	ON	2010/03/22 07:23

3/23/2010 8:02:01 AM
C:\Documents and Settings\iokeke\My Documents\EAST\Workspaces\11895388.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/895,388	08/24/2007	Scott A. Moskowitz	80391.0003CONT2	2103

7590 06/08/2010

Scott A. Moskowitz
#2505
16711 Collins Avenue
Sunny Isless Beach, FL 33160

EXAMINER	
OKEKE, IZUNNA	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
06/08/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Interview Summary	Application No.	Applicant(s)	
	11/895,388	MOSKOWITZ, SCOTT A.	
	Examiner	Art Unit	
	IZUNNA OKEKE	2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) *IZUNNA OKEKE*. (3)_____.

(2) *SCOTT MOSKOWITZ*. (4)_____.

Date of Interview: *27 May 2010*.

Type: a)☒ Telephonic b)☐ Video Conference
c)☐ Personal [copy given to: 1)☐ applicant 2)☐ applicant's representative]

Exhibit shown or demonstration conducted: d)☐ Yes e)☒ No.
If Yes, brief description: _____.

Claim(s) discussed: *32-45 and 52-59*.

Identification of prior art discussed: *Moore (US6067622)*.

Agreement with respect to the claims f)☐ was reached. g)☒ was not reached. h)☐ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: *Discussed the double patenting, 101 and 112 rejection presented in the previous action. Also discussed the applied reference with respect to the claims. Applicant presented argument that Moore obtains his key from a call purveyor and examiner clarified that the claims (claim 35) recite "accessing the watermark with a key" and the reference meets the limitation as recited*.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN A NON-EXTENDABLE PERIOD OF THE LONGER OF ONE MONTH OR THIRTY DAYS FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

/IZUNNA OKEKE/ Examiner, Art Unit 2432	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

PTO/SB/81 (01-09)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	11/895,388
Filing Date	8/24/2007
First Named Inventor	S. MOSKOWITZ
Title	Data protection method and device
Art Unit	2432
Examiner Name	F. OKEKE
Attorney Docket Number	SCOT0014-4

I hereby revoke all previous powers of attorney given in the above-identified application.

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 31518

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified application to:

☐ The address associated with the above-mentioned Customer Number.

OR

☒ The address associated with Customer Number: 31518

OR

☐ Firm or Individual Name				
Address				
City		State		Zip
Country				
Telephone		Email		

I am the:

☒ Applicant/Inventor.

OR

☒ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____.

SIGNATURE of Applicant or Assignee of Record

Signature	Scott Moskowitz	Date	August 16, 2010
Name	SCOTT A. MOSKOWITZ	Telephone	305-956-9041
Title and Company			

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt	
EFS ID:	8224895
Application Number:	11895388
International Application Number:	
Confirmation Number:	2103
Title of Invention:	Data protection method and device
First Named Inventor/Applicant Name:	Scott A. Moskowitz
Correspondence Address:	Scott A. Moskowitz - #2505 16711 Collins Avenue Sunny Isless Beach FL 33160 US 305 956 9041 scott@bluespike.com
Filer:	Richard A. Neifeld
Filer Authorized By:	
Attorney Docket Number:	80391.0003CONT2
Receipt Date:	18-AUG-2010
Filing Date:	24-AUG-2007
Time Stamp:	10:39:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	1POA_SCOT0014-4_8-16-2010.pdf	51778 1dcc93cc3435590e4436ea1545462dc04efa48f2	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	51778		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/895,388	08/24/2007	Scott A. Moskowitz	SCOT0014-4

CONFIRMATION NO. 2103

31518
NEIFELD IP LAW, PC
4813-B EISENHOWER AVENUE
ALEXANDRIA, VA 22304

POA ACCEPTANCE LETTER

OC000000043201918

Date Mailed: 08/30/2010

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/18/2010.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/tnnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

NEIFELD REF: SCOT0014-4
CLIENT REF: 80391.0003CONT2
Application/Patent No: 11/895,388
USPTO CONF. NO: 2103
File/Issue Date: 08-24-2007
Inventor: SCOTT MOSKOWITZ
Title: Data protection method and device
Examiner/ArtUnit: Izunna OKEKE/2432
ENTITY STATUS: SMALL (CONVERT UPON ALLOWANCE TO LARGE)
Priority claims and PCT Intl data: "[0001] This application is a divisional of U.S. Patent Application Serial No. 10/602,777, which is a continuation application of U.S. Patent Application Serial No. 09/046,627 filed 3/24/1998 (which issued July 22, 2003. as U.S. Patent No. 6,598,162), which is a continuation-in-part of U. S. Patent Application Serial No. 08/587,943, filed Jan. 17, 1996, (which issued April 28, 1998, as U.S. Patent No. 5,745,569). The entire disclosure of U.S. Patent Application No. 09/046,627 (which issued July 22, 2003, as U.S. Patent No. 6,598,1621 and U.S. Patent Application Serial No. 08/587,943, filed Jan. 17, 1996, (which issued April 28, 1998, as U.S. Patent No. 5,745,569) are hereby incorporated by reference in their entireties."

37 CFR 1.7(c) FILING RECEIPT AND TRANSMITTAL LETTER WITH AUTHORIZATION TO CHARGE DEPOSIT ACCOUNT

1. **THE COMMISSIONER IS HEREBY AUTHORIZED TO CHARGE ANY FEES WHICH MAY BE REQUIRED, OR CREDIT ANY OVERPAYMENT, TO DEPOSIT ACCOUNT NUMBER 50-2106.**

2. **FEES (PAID HEREWITH BY EFS CREDIT CARD SUBMISSION) $:** 575
Small entity fees apply to this application.
31 claims and 5 ind. claims previously paid for.
Claims 32-45 and 52-63 are now pending for a total of 14+12=28 claims.
The independent claims are 32, 40, 52, 58, 59, 61, 62, and 63 = 8.
Claim fees due for 3 independent claims, at $110 per claim, for $330 in claims fees.
Extension fees: $245 for 2 months extension to 9/5/2010.

3. **THE FOLLOWING DOCUMENTS ARE SUBMITTED HEREWITH:**
PETITION FOR EXTENSION OF TIME FOR 2 MONTHS
37 CFR 1.111 AMENDMENT REMARKS
SPECIFICATION
CLAIMS

ATTORNEY SIGNATURE (AUTHORIZING DEPOSIT ACCOUNT)
DATE: 9-1-2010 **SIGNATURE**: /RichardNeifeld#35,299/
PRINTED NAME: RICHARD NEIFELD
Printed: September 1, 2010 (8:55pm)
Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\Response_SCOT0014-4_8-28-2010.wpd

DISH-Blue Spike-842
Exhibit 1004, Page 1236

NEIFELD REF: SCOT0014-4
CLIENT REF: 80391.0003CONT2
Application/Patent No: 11/895,388
USPTO CONF. NO: 2103
File/Issue Date: 08-24-2007
Inventor: SCOTT MOSKOWITZ
Title: Data protection method and device
Examiner/ArtUnit: Izunna OKEKE/2432

37 CFR 1.136(A) PETITION FOR EXTENSION OF TIME FOR 2 MONTHS

This is a petition for extension of time to respond to the 4/5/2010 office action from 7/5/2010 to 9/5/2010.

DATE: 9-1-2010 **SIGNATURE**: /RichardNeifeld#35,299/
PRINTED NAME: RICHARD NEIFELD, REG. NO. 35,299
ATTORNEY OF RECORD

Printed: September 1, 2010 (8:55pm)
Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\Response_SCOT0014-4_8-28-2010.wpd

DISH-Blue Spike-842
Exhibit 1004, Page 1237

REMARKS

The undersigned spoke briefly with Examiner Okeke on 9/1/2010 requesting a substantive telephone discussion of this application and proposed claim amendments. The undersigned requests that the examiner telephone me at 7034150012 extension 100 upon review of the amended claims in order to expedite resolution of any and all remaining issues relating to allowance.

OA item 1 notes the applicant's election of Group II claims 32-45 and 52-5**9** "without traverse". That is incorrect. In fact, claims 58 and 59 were not restricted, and the applicant traversed the restriction requirement for that reason. Specifically:

The 11/10/2009 OA, which is the OA that contained the requirement for restriction, defined Group II as "Claims 32-45 and 52-57, drawn to protecting data or software by inhibiting the unauthorized installation or use of software, classified in class 713, subclass 176." The OA containing the restriction requirement was defective insofar as it failed to examine that claims 58 and 59 and define their status. In the applicant's response dated 12/10/2009, the applicant "provisionally" elected Group II, and sought "clarification on the requirement for restriction regarding pending claims 58 and 59." In other words, the applicant traversed. Accordingly, the statement in the office action that the election was without traverse, is inaccurate, and accordingly, the restriction, since maintained, has the status of "final" for procedural purposes.

The examiner is requested to clarify that the restriction was made final by its maintenance with change in Group II to include claims 58 and 59, in the 4/5/2010 office action, when the examiner drafts the next communication in this application.

OA items 2 and 3 provisionally reject claims 32-45 and 52-59 based upon claims 1-20 of application 08/587,943 for provisional obviousness double patenting (DP); provisional because the OA indicates that 08/587,943 is pending. In response, first note that 08/587,943 issued long ago as USP 5,745,569. The applicant traverses because it is unclear, given the inconsistent identification of status of 08/587,943 and the provisional status of the DP rejection in the OA, whether claims 1-20 in 08/587,943 is the subject matter upon which the examiner intended to base the DP rejection. The examiner is requested to double check if 08/587,943 is the application intended to form the basis of a DP rejection.

OA item 4 reject claims 32-39 under 35 USC 101 for not defining patentable subject matter. In response, the claims have been amended to define patentable subject matter by referring to use of computer components in performing processing steps, and by referring to functionality relating to implementation on a computer.

OA items 5-6 rejects claim 32 under the first paragraph of 35 USC 112 first paragraph for lack of disclosure in the specification of the recitation "wherein the embedded software operates in manner substantially the same as software prior to the embedding step" indicating that "substantially" was not disclosed in the specification. In response, claim 32 has been amended and, as amended, no longer contains that recitation.

OA items 7-8 reject claim 52 under 35 USC 112 second paragraph indicating that claim 52 is a system claim reciting method steps. In response, the claims have been amended to avoid reciting steps in system claims.

OA item 9 rejects claims 32-45 and 52-69 under 35 USC 102 based upon Moore US patent 6067622. The OA cites Moore Fig. 1a and 8:43-51, which disclose a code module, not a watermark. In response, the claims have been amended to clearly define an invention not disclosed by Moore. Moore discloses a copyright module, not watermarking, and in any case does not disclose encoding a license key in software, using license information to identify a watermark in software, or decoding software using license information. In contrast, the independent claims define these concepts, which are not disclosed or suggested by Moore

If the examiner has any comments or concerns, please do not hesitate to contact the undersigned to expedite prosecution, at telephone 7034150012 extension 100.

/RichardNeifeld#35,299/
RICHARD NEIFELD, REG. NO. 35,299
ATTORNEY OF RECORD

RAN
Date/time code: September 1, 2010 (8:55pm)
Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\Response_SCOT0014-4_8-28-2010.wpd

IN THE SPECIFICATION

Please replace paragraph [0011] with the following paragraph.

[0011] It is thus the goal of the present invention to provide a higher level of copyright security to object code on par with methods described in digital watermarking systems for digitized media content such as pictures, audio, video and multimedia content in its multifarious forms, as described in previous disclosures, "Steganographic Method and Device" Ser. No. 08/489,172, filed Jun. 7, 1995, now U.S. Pat. No. 5,613,004, and "Human Assisted Random Key Generation and Application for Digital Watermark System", Ser. No. 08/587,944, filed on Jan. 17, 1996, now U.S. Pat. No. 5,822,432, the disclosure of which is hereby incorporated by reference.

RAN
Date/time code: September 1, 2010 (9:00pm)
SpecAmendment_SCOT0014-4_9-1-2010wpd.wpd

1-31. (Canceled)

32. (Currently Amended) A computer-based method for ~~copy protection of software~~ modifying software , comprising:

receiving, in a computer having a processor and memory, software, wherein said software provides a specified functionality;

embedding ~~the software with~~ a watermark into said software, using said computer, said watermark encoding at least one first license code, thereby resulting in a first license code encoded watermarked software, wherein ~~the embedded software operates in a manner substantially the same as the software prior to the embedding step~~ said first license code encoded watermarked software.

33. (Currently Amended) ~~The process of claim 32, wherein the step of embedding the software with a watermark increases the complexity of code analysis and/or tampering with the software.~~ The process of claim 32, wherein said embedding increases the complexity of code analysis and/or tampering with said first license code encoded watermarked software.

34. (Currently Amended) ~~The process of claim 32, wherein the watermarked software queries a user for personalization information during installation of the software.~~ The process of claim 32, wherein said first license code encoded watermarked software is configured to query a user for personalization information during its installation.

35. (Currently Amended) The process of claim 32, wherein [[the]] said watermark is accessible with a key.

36. (Currently Amended) ~~The process of claim 35, wherein the key enables authorized use of the watermarked software.~~ The process of claim 35 wherein said key enables said first license code encoded watermarked software to provide said specified functionality.

37. (Currently Amended) ~~The process according to claim 35, wherein the key and license information are interchangeable.~~ The process according to claim 34, wherein said first license code encoded watermarked software is configured to determine said key from said personalization information.

38. (Original) The process according to claim 32, wherein the step of embedding the software with a watermark is performed during execution of the software.

39. (Currently Amended) ~~The process according to claim 32, wherein the step of embedding the software with a watermark modifies the structure of the software being embedded.~~ The process according to claim 32, wherein said embedding modifies the structure of said software.

40. (Currently Amended) An article of manufacture comprising a machine readable medium, having thereon stored instructions adapted to be executed by a processor of a computer system, said computer system including a memory, which instructions when executed by said computer system result in a process comprising: ~~receiving potentially watermarked software ; and identifying the software by extracting the watermark.~~

said computer system storing a software in said memory;

said computer system receiving licensing information as an input and using said licensing information in an algorithm to identify a watermark in said software.

41. (Currently Amended) The article of manufacture of claim 40, wherein said watermark encodes therein information. ~~the watermark is associated with information fixed prior to distribution of the watermarked software.~~

42. (Original) The article of manufacture of claim 40, wherein the watermark affects functionality of the watermarked software.

43. (Currently Amended) ~~The article of manufacture of claim 40, wherein the~~

~~extracted watermark enables generation of a key.~~ The article of manufacture of claim 41, wherein said instructions comprise decode instructions for said computer system to use said information to generate a decode key for decoding said software.

44. (Currently Amended) The article of manufacture of claim 43, wherein said identifying information comprises a license key, and said decode instructions instruct said computer to determine said license key from said information and to generate said decode key using said license key ~~the generated key and licensing information are associated.~~

45. (Currently Amended) The article of manufacture of claim 40~~, further comprising limiting functionality of the software if the watermark cannot be extracted.~~

wherein said watermark encodes a license key;

said instructions include a prompt to enter licensing information;

wherein said software provides a certain functionality after receipt of licensing information in response to said prompt only if said licensing information comprises a license key encoded in said watermark.

46 – 51. (Canceled)

52. (Currently Amended) ~~A system for copy protection of software comprising the steps of:~~

~~associating license information with a copy of a software application; encoding the associated license information into the copy of the software application using a watermarking process;~~

~~providing the copy of the software application having license information encoded therein~~

A computer-based system for modifying software, comprising:

a computer having a processor and memory;

wherein said computer is programmed to receive software that provides a specified functionality when installed on a computer system;

wherein said computer is programmed to embed a watermark into said software;

wherein said watermark encodes at least one first license code, thereby resulting in a first license code encoded watermarked software.

53. (Currently Amended) ~~The system of claim 52, wherein the encoding is controlled by a key.~~ The system of claim 52 wherein said computer is programmed to use said at least one first license code as an input in an algorithm for embedding said watermark with said at least one first license code.

54. (Currently Amended) ~~The system of claim 52, wherein the step of comparing the user supplied information with the encoded license information enables authorization of the software.~~ The system of claim 52 wherein said first license code encoded watermarked software is designed to prompt for entry of licensing information and only provides a certain functionality if licensing information entered in response to said prompt comprises at least one of said at least one first license code encoded in said watermark.

55. (Currently Amended) The system of claim 53, wherein ~~the key~~ said at least one first license code is fixed prior to distribution of the software.

56. (Currently Amended) ~~The system of claim 52, wherein the license information comprises code which affects functionality of the software.~~ The system of claim 52 wherein said at least one first license code comprises computer code that provides different functionality to said first license code encoded watermarked software compared to said software.

57. (Currently Amended) The system of claim 52, wherein ~~the software~~ said first license code encoded watermarked software is resistant to code analysis and/or tampering.

58. (New) A method for licensed software use, the method comprising:

loading a software product on a computer, said computer comprising a processor, memory, an input, and an output, so that said computer is programmed to execute said software

product;

said software product outputting a prompt for input of license information; and

said software product using license information entered via said input in response to said prompt in a routine designed to decode a first license code encoded in said software.

59. (New) A method for encoding software code using a computer having a processor and memory, comprising:

storing a software code in said memory;

wherein said software code comprises a first code resource and provides a specified underlying functionality when installed on a computer system; and

encoding, by said computer using at least a first license key and an encoding algorithm, said software code, to form a first license key encoded software code.

60. (New) The method of claim 59 wherein, when installed on a computer system, said first license key encoded software code will provide said specified underlying functionality only after receipt of said first license key.

61. (New) A method for encoding software code using a computer having a processor and memory, comprising:

storing a software code in said memory;

wherein said software code comprises a first code resource and provides a specified underlying functionality when installed on a computer system; and

modifying, by said computer, using a first license key and an encoding algorithm, said software code, to form a modified software code; and

wherein said modifying comprises encoding said first code resource to form an encoded first code resource;

wherein said modified software code comprises said encoded first code resource, and a decode resource for decoding said encoded first code resource;

wherein said decode resource is configured to decode said encoded first code resource upon receipt of said first license key.

62. (New) A method for encoding software code using a computer having a processor and memory, comprising:

storing a software code in said memory;

wherein said software code defines software code interrelationships between code resources that result in a specified underlying functionality when installed on a computer system; and

encoding, by said computer using at least a first license key and an encoding algorithm, said software code, to form a first license key encoded software code in which at least one of said software code interrelationships are encoded.

63. (New) A method for encoding software code using a computer having a processor and memory, comprising:

storing a software code in said memory;

wherein said software code provides a specified underlying functionality when installed on a computer system;

encoding, by said computer using at least a first license key and an encoding algorithm, said software code, to form a first license key encoded software code;

encoding, by said computer using at least a second license key and an encoding algorithm, said software code, to form a second license key encoded software code;

wherein said first license key encoded software code is not identical to said second license key encoded software code if said first license key is not identical to said second license key.

64. (New) The method of claim 63 wherein both said first license key encoded software code and said second license key encoded software code are capable of providing said specified underlying functionality when installed on a computer system.

ran

Date/time code: September 1, 2010 (8:47pm)

Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\Claims_SCOT0014-4_8-28-2010.wpd

Electronic Patent Application Fee Transmittal

Application Number:	11895388
Filing Date:	24-Aug-2007
Title of Invention:	Data protection method and device
First Named Inventor/Applicant Name:	Scott A. Moskowitz
Filer:	Richard A. Neifeld
Attorney Docket Number:	SCOT0014-4

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Independent claims in excess of 3	2201	3	110	330
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	2252	1	245	245
Miscellaneous:				
		Total in USD ($)		**575**

Electronic Acknowledgement Receipt	
EFS ID:	8351939
Application Number:	11895388
International Application Number:	
Confirmation Number:	2103
Title of Invention:	Data protection method and device
First Named Inventor/Applicant Name:	Scott A. Moskowitz
Customer Number:	31518
Filer:	Richard A. Neifeld
Filer Authorized By:	
Attorney Docket Number:	SCOT0014-4
Receipt Date:	03-SEP-2010
Filing Date:	24-AUG-2007
Time Stamp:	11:17:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$575
RAM confirmation Number	7537
Deposit Account	502106
Authorized User	NEIFELD,RICHARD ALAN
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Response_SCOT0014-4_8-28-2010.pdf	40969 e473135246ec6a561d4140b900b8543c9ac0dcbf	yes	4
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Extension of Time		1	2	
	Applicant Arguments/Remarks Made in an Amendment		3	4	
Warnings:					
Information:					
2	Specification	SpecAmendment_SCOT0014-4_9-1-2010wpd.pdf	18869 dc4b37972e60561919758947d352a1d14cd77375	no	2
Warnings:					
Information:					
3	Claims	Claims_SCOT0014-4_8-28-2010 CutePDF.pdf	841212 e9b9db044b325bcc04c8aea06d16e2655b936bcb	no	7
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	31789 c182e5dc7a614c8d5478c1998a428c99e9a1afdb	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	932839		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/895,388	08/24/2007	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 09/03/2010	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 27	Minus	** 33	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 8	Minus	***7	= 1	X $110 =	110	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	110	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/ROZENIA HARMON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

NEIFELD REF: SCOT0014-4
CLIENT REF: 80391.0003CONT2
Application/Patent No: 11/895,388
USPTO CONF. NO: 2103
File/Issue Date: 8/24/2007
Inventor: Moskowitz, Scott
Title: DATA PROTECTION METHOD AND DEVICE
Examiner/ArtUnit: Izunna Okeke/2432
ENTITY STATUS: LARGE
Priority claims and PCT Intl data:
This application is a Division of 10/602,777 06-25-2003 Patented 7,664,263; SCOT0014-2 is a continuation of 09/046,627 03-24-1998 Patented 6,598,162; SCOT0014-1 is a Continuation-in-part of 08/587,943 01-17-1996 Patented 5,745,569

37 CFR 1.7(c) FILING RECEIPT AND TRANSMITTAL LETTER WITH AUTHORIZATION TO CHARGE DEPOSIT ACCOUNT

1. THE COMMISSIONER IS HEREBY AUTHORIZED TO CHARGE ANY FEES WHICH MAY BE REQUIRED, OR CREDIT ANY OVERPAYMENT, TO DEPOSIT ACCOUNT NUMBER 50-2106.

2. FEES (PAID HEREWITH BY EFS CREDIT CARD SUBMISSION) $: 180.00
1806 1.17(p) Submission of an Information Disclosure Statement 180.00
3. THE FOLLOWING DOCUMENTS ARE SUBMITTED HEREWITH:
37 CFR 1.97 INFORMATION DISCLOSURE STATEMENT
37 CFR 1.98 REFERENCE CITATION LIST CITING REFERENCES INCLUDING (1) MASTER LIST OF RELATED CASES and citations of references U1-U302; P1-P82; F1-F29; and L1-L212
COPIES OF THE FOLLOWING REFERENCES
L99; L101; L104; L105; L115; L165; L166, L167, L176, L201; L203-212
F- 03; F16-20; F24-25; F29
4. FOR INTERNAL NEIFELD IP LAW, PC USE ONLY

USPTO CHARGES $: 180 CLIENT BILLING MATTER: BANK ACCOUNT/Check: 6/970 G/L ACCOUNT: 5010	FIRM CHARGES $: 400 DESCRIPTION: FIRM CHARGE FOR PAYING IDS FEE LAWYER: RAN

INITIALS OF PERSON WHO *ENTERED* ACCOUNTING DATA: RAN
ATTORNEY SIGNATURE (AUTHORIZING DEPOSIT ACCOUNT)
DATE: 11-18-2010 SIGNATURE: /RichardNeifeld#35,299/
PRINTED NAME: RICHARD NEIFELD, REG. NO. 35,299
Printed: November 19, 2010 (12:45pm)
Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd

DISH-Blue Spike-842
Exhibit 1004, Page 1256

Neifeld Docket No: SCOT0014-4
Application/Patent No: 11/895,388 USPTO CONFIRMATION NO: 2103
File/Issue Date: 8/24/2007
Inventor/Title: Moskowitz/DATA PROTECTION METHOD AND DEVICE
Examiner/ArtUnit: Izunna Okeke/2432

37 CFR 1.97 INFORMATION DISCLOSURE STATEMENT

_____This application is:
____ within 3 months of the US or 371 national stage filing date;
___ before first action on the merits (no fee required);
_X_ after first action on the merits and before final action (1.17(p) fee required);
____ after final action;
____ after notice of allowance and before payment of the issue fee; or
____ after payment of the issue fee.

__X__ The applicant is paying herewith the fee for obtaining consideration of an IDS filed after a first action on the merits.

IDENTIFICATION OF REFERENCES CITED IN APPLICATIONS TO WHICH 11/895,338 CLAIMS CONTINUING STATUS

REGARDING CITED REFERENCES

This IDS is an attempt to compile all references previously cited in Scott Moskowitz's cases. Upon compilation, some of the reference citations were vague, and some were to filed patent applications instead of published documents. This IDS attempts to account for each item to provide all citations to the examiner.

CITED US PATENTS AND US PATENT APPLICATION PUBLICATIONS

Most pending Scott Moskowitz cases claim 35 USC 120 priority to prior cases containing a large number of cited US patents and published US applications. The citations list herein should incorporate all of those documents and may incorporates any additional documents found in other patent applications in patent families not linked by 35 USC 120 to this application. Since no US patent or US published applications need to be filed in order for the examiner to consider citations thereto.

FOREIGN PATENT REFERENCES

The IDS cites foreign patent references identified herewith as F001- F029.

The table below identifies F references earlier cited in either this application or an application to which this application claims 35 USC 120 priority.

DOCKET NO	APPLICATION NUMBER	CITED F REFERENCES
SCOT0014-4	11/895,388	F#1-2; F4-15; F21-23; F26-28

Accordingly, the following F references are not yet of record and are submitted herewith: F- 03; F16-20; F24-25; F29.

NON PATENT LITERATURE REFERENCES

The IDS cites foreign patent references identified herewith as L001- L212 .

The table below identifies L references earlier cited in either this application or an application to which this application claims 35 USC 120 priority.

DOCKET NO	APPLICATION NUMBER	CITED F REFERENCES
SCOT0014-4	11/895,388	L1; L3-11; L13-26; L28-97; L155-164; L168-175; L177-L184; L191-199
	L reference citations of patent applications as filed for which a subsequent publication of the application is identified and cited herein.	L1-35; L185- 200; L202.
	L reference citation numbers that have no associated reference.	L98; L100; L102; L103; L106-L114; L116-L154

References previously cited, applications for which a subsequent publication is cited, and reference numbers having no associated reference:
L1-98; L100; L102; L103; L106-114; L116-164; L168-175; L177-L200; L202

Accordingly, the following references are not yet cited, not applications whose subsequent publication is also cited herein, and are submitted herewith:
L99; L101; L104; L105; L115; L165; L166, L167, L176, L201; L203-212

US PATENT REFERENCES

The IDS cites US patent references identified herewith as U1-U302.

The table below identifies U references earlier cited in either this application or an application to which this application claims 35 USC 120 priority.

DOCKET NO	APPLICATION	CITED REFERENCES

SCOT0014-4	11/895,388	U1-40; U41; U43-50; U52-109, U111-114; U116-119; U121-128; U130-135; U137-140; U142; U144-148; U151-152; U154-157; U160-175; U177-181; U183; U185-218; U220-238; U240-244, 246-259; U261-265; U267; U269; U273; U276; U286; U288; U300

No US patent reference is submitted, since they are not required by PTO rules to be submitted.

US PATENT APPLICATION PUBLICATION REFERENCES

The IDS cites US patent application publication references identified herewith as P1-P82

The table below identifies P references earlier cited in either this application or an application to which this application claims 35 USC 120 priority.

DOCKET NO	APPLICATION NUMBER	CITED F REFERENCES
SCOT0014-4	11/895,388	P2, P4, P7-99; P11; P12; P15-19; P24; P25; P29; P31; P32; P33-35; P43; P46; P48.

No US patent publication reference is submitted, since they are not required by PTO rules to be submitted.

Please consider the references cited herein.

Date signed: 11-18-2010

Signature: /RichardNeifeld#35,299/
Printed Name: RICHARD NEIFELD, REG. NO. 35,299
Attorney of Record

ran
Printed: November 19, 2010 (12:45pm)
Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd

37 CFR 1.98 REFERENCE CITATION LIST

MASTER LIST OF RELATED CASES

DOCKET REFERENCE	APPLICATION	FILING DATE	DATE CASE ADDED TO THIS MASTER LIST OF RELATED CASES
SCOT0010-4	11/599,838	11/15/2006	10/15/2010 JRE
SCOT0010-5	11/899,662	9/7/2007	10/15/2010 JRE
SCOT0010-8	12/215,812	6/30/2008	10/15/2010 JRE
SCOT0010-10	12/901,568	10/10/2010	11/4/2010 JRE
SCOT0010-12	12/217,834	7/9/2008	11/8/2010 JRE
SCOT0011-4	12/009,914	1/23/2008	10/15/2010 JRE
SCOT0011-5	12/005,230	12/26/2007	10/15/2010 JRE
SCOT0011-8	12/803,194	06/21/2010	10/15/2010 JRE
SCOT0011-6	12/803,168	6/21/2010	10/15/2010 JRE
SCOT0011-9	12/892,900	9/28/2010	11/8/2010 JRE
SCOT0012-3	08/999,766	7/23/1997	10/15/2010 JRE
SCOT0012-4	11/894,476	8/21/2007	10/15/2010 JRE
SCOT0012-5	11/050,779	2/7/2005	10/15/2010 JRE
SCOT0012-6	12/802,519	6/8/2010	11/4/2010 JRE
SCOT0012-7	12/383,916	3/30/2009	10/15/2010 JRE
SCOT0012-8	11/894,443	8/21/2007	10/15/2010 JRE
SCOT0012-9	12/913,751	10/27/2010	11/8/2010 JRE
SCOT0014-3	11/512,701	8/29/2006	10/15/2010 JRE
SCOT0014-4	11/895,388	8/24/2007	10/15/2010 JRE
SCOT0015-3	12/383,879	3/30/2009	10/15/2010 JRE
SCOT0015-4	12/886,732	9/21/2010	10/15/2010 JRE
SCOT0016-2	12/287,443	10/9/2008	10/15/2010 JRE
SCOT0017-3	12/655,357	12/22/2009	10/15/2010 JRE
SCOT0018-2	11/900,065	9/10/2007	10/15/2010 JRE

AS OF 11/4/2010, THE FOLLOWING TABLE COLLATES ADDITIONAL REFERENCES CITED IN ANY SCOT (SCOTT MOSKOWITZ) CASE

DATE OF DOCUMENT CITING REFERENCES	ATTY REF	APPLICATION NUMBER	IDENTIFICATION OF PAPER IN WHICH REFERENCES WERE CITED	References checked to see if they existed in the master IDS (initials of person checking)	Reference Identifiers of New references in document, now added to master IDS
Sept 14, 2010	SCOT0012-7	12/383,916	892	JRE	U#299
11/17/2010	ALL	N/A	Review of draft master IDS, correction to cite publications in lieu of filed applications, per RAN instructions.	JRE	P76-P82

NOTE: MPEP 609.02 Information Disclosure Statements in Continued Examinations or Continuing Applications [R-5] states in part that:

"2. Continuation Applications, Divisional Applications, or Continuation-in-Part Applications Filed Under 37 CFR 1.53(b) The examiner will consider information which has been considered by the Office in a parent application when examining: (A) a continuation application filed under 37 CFR 1.53(b), (B) a divisional application filed under 37 CFR 1.53(b), or (C) a continuation-in-part application filed under 37 CFR 1.53(b). A listing of the information need not be resubmitted in the continuing application unless the applicant desires the information to be printed on the patent." See http://www.uspto.gov/web/offices/pac/mpep/documents/0600_609_02.htm.

Accordingly, we are submitting **only** references not cited in applications to which this application claims priority under 35 USC 120.

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
ATTORNEY DOCKET REFERENCE:
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

LISTING OF UNITED STATES PATENTS - U series

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 01	3947825	March 1976	Cassada	
	U 02	3984624	October 1976	Waggener	
	U 03	3986624	October 1976	Cates, Jr. et al.	
	U 04	4038596	July 1977	Lee	
	U 05	4200770	April 1980	Hellman et al.	
	U 06	4218582	August 1980	Hellman et al.	
	U 07	4339134	July 1982	Macheel	
	U 08	4390898	June 1983	Bond et al.	
	U 09	4405829	September 1983	Rivest et al.	
	U 010	4424414	January 1984	Hellman et al.	
	U 011	4528588	July 1985	Lofberg	
	U 012	4672605	June 1987	Hustig et al.	
	U 013	4748668	May 1988	Shamir et al.	
	U 014	4789928	December 1988	Fujisaki	
	U 015	4827508	May 1989	Shear	
	U 016	4876617	October 1989	Best et al.	
	U 017	4896275	January 1990	Jackson	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 018	4908873	March 1990	Philibert et al.	
	U 019	4939515	July 1990	Adelson	
	U 020	4969204	November 1990	Jones et al.	
	U 021	4972471	November 1990	Gross et al.	
	U 022	4977594	December 1990	Shear	
	U 023	4979210	December 1990	Nagata et al.	
	U 024	4980782	December 1990	Ginkel	
	U 025	5050213	September 1991	Shear	
	U 026	5073925	December 1991	Nagata et al.	
	U 027	5077665	December 1991	Silverman et al.	
	U 028	5113437	May 1992	Best et al.	
	U 029	5136581	August 1992	Muehrcke	
	U 030	5136646	August 1992	Haber et al.	
	U 031	5136647	August 1992	Haber et al.	
	U 032	5142576	August 1992	Nadan	
	U 033	5161210	November 1992	Druyvesteyn et al.	
	U 034	5210820	May 1993	Kenyon	
	U 035	5243423	September 1993	DeJean et al.	
	U 036	5243515	September 1993	Lee	
	U 037	5287407	February 1994	Holmes	
	U 038	5319735	June 1994	Preuss et al.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 039	5341429	August 1994	Stringer et al.	
	U 040	5341477	August 1994	Pitkin et al.	
	U 041	5363448	November 1994	Koopman et al.	
	U 042	5365586	November 1994	Indeck et al.	
	U 043	5369707	November 1994	Follendore, III	
	U 044	5379345	January 1995	Greenberg	
	U 045	5394324	February 1995	Clearwater	
	U 046	5398285	March 1995	Borgelt et al.	
	U 047	5406627	April 1995	Thompson et al.	
	U 048	5408505	April 1995	Indeck et al.	
	U 049	5410598	April 1995	Shear	
	U 050	5412718	May 1995	Narasimhalv et al.	
	U 051	5418713	May 1995	Allen	
	U 052	5428606	June 1995	Moskowitz	
	U 053	5450490	September 1995	Jensen et al.	
	U 054	5469536	November 1995	Blank	
	U 055	5471533	November 1995	Wang et al.	
	U 056	5478990	December 1995	Montanari et al.	
	U 057	5479210	December 1995	Cawley et al.	
	U 058	5487168	January 1996	Geiner et al.	
	U 059	5493677	February 1996	Balogh et al.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 060	5497419	March 1996	Hill	
	U 061	5506795	April 1996	Yamakawa	
	U 062	5513126	April 1996	Harkins et al.	
	U 063	5513261	April 1996	Maher	
	U 064	5530739	June 1996	Okada	
	U 065	5530751	June 1996	Morris	
	U 066	5530759	June 1996	Braudaway et al.	
	U 067	5539735	July 1996	Moskowitz	
	U 068	5548579	August 1996	Lebrun et al.	
	U 069	5568570	October 1996	Rabbani	
	U 070	5579124	November 1996	Aijala et al.	
	U 071	5581703	December 1996	Baugher et al.	
	U 072	5583488	December 1996	Sala et al.	
	U 073	5598470	January 1997	Cooper et al.	
	U 074	5606609	February 1997	Houser et al.	
	U 075	5613004	March 1997	Cooperman et al.	
	U 076	5617119	April 1997	Briggs et al.	
	U 077	5625690	April 1997	Michel et al.	
	U 078	5629980	May 1997	Stefik et al.	
	U 079	5633932	May 1997	Davis et al.	
	U 080	5634040	May 1997	Her et al.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 081	5636276	June 1997	Brugger	
	U 082	5636292	June 1997	Rhoads	
	U 083	5640569	June 1997	Miller et al.	
	U 084	5646997	July 1997	Barton	
	U 085	5657461	August 1997	Harkins et al.	
	U 086	5659726	August 1997	Sandford, II et al.	
	U 087	5664018	September 1997	Leighton	
	U 088	5673316	September 1997	Auerbach et al.	
	U 089	5677952	October 1997	Blakely et al.	
	U 090	5680462	October 1997	Miller et al.	
	U 091	5687236	November 1997	Moskowitz et al.	
	U 092	5689587	November 1997	Bender et al.	
	U 093	5696828	December 1997	Koopman, Jr.	
	U 094	5719937	February 1998	Warren et al.	
	U 095	5721788	February 1998	Powell et al.	
	U 096	5734752	March 1998	Knox	
	U 097	5737416	April 1998	Cooper et al.	
	U 098	5737733	April 1998	Eller	
	U 099	5740244	April 1998	Indeck et al.	
	U 0100	5745569	April 1998	Moskowitz et al.	
	U 0101	5748783	May 1998	Rhoads	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 0102	5751811	May 1998	Magnotti et al.	
	U 0103	5754697	May 1998	Fu et al.	
	U 0104	5757923	May 1998	Koopman, Jr.	
	U 0105	5765152	June 1998	Erickson	
	U 0106	5768396	June 1998	Sone	
	U 0107	5774452	June 1998	Wolosewicz	
	U 0108	5790677	August 1998	Fox et al.	
	U 0109	5799083	August 1998	Brothers et al.	
	U 0110	5809139	September 1998	Grirod et al.	
	U 0111	5809160	September 1998	Powell et al.	
	U 0112	5822432	October 1998	Moskowitz et al.	
	U 0113	5828325	October 1998	Wolosewicz et al.	
	U 0114	5832119.	November 1998	Rhoads	
	U 0115	5848155	December 1998	Cox	
	U 0116	5850481	December 1998	Rhoads	
	U 0117	5859920	January 1999	Daly et al.	
	U 0118	5860099	January 1999	Milios et al.	
	U 0119	5862260	January 1999	Rhoads	
	U 0120	5870474	February 1999	Wasilewski et al.	
	U 0121	5884033	March 1999	Duvall et al.	
	U 0122	5889868	March 1999	Moskowitz et al.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 0123	5893067	April 1999	Bender et al.	
	U 0124	5894521	April 1999	Conley	
	U 0125	5903721	May 1999	Sixtus	
	U 0126	5905800	May 1999	Moskowitz et al.	
	U 0127	5905975	May 1999	Ausubel	
	U 0128	5912972	June 1999	Barton	
	U 0129	5915027	June 1999	Cox et al.	
	U 0130	5917915	June 1999	Hirose	
	U 0131	5918223	June 1999	Blum	
	U 0132	5920900	July 1999	Poole et al.	
	U 0133	5923763	July 1999	Walker et al.	
	U 0134	5930369	July 1999	Cox et al.	
	U 0135	5930377	July 1999	Powell et al	.
	U 0136	5940134	August 1999	Wirtz	
	U 0137	5943422	August 1999	Van Wie et al.	
	U 0138	5963909	October 1999	Warren et al.	
	U 0139	5973731	October 1999	Schwab	
	U 0140	5974141	October 1999	Saito	
	U 0141	5991426	November 1999	Cox et al.	
	U 0142	5999217	December 1999	Berners-Lee	
	U 0143	6009176	December 1999	Gennaro et al.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 0144	6029126	February 2000	Malvar	
	U 0145	6041316	March 2000	Allen	
	U 0146	6044471	March 2000	Colvin	
	U 0147	6049838	April 2000	Miller et al.	
	U 0148	6051029	April 2000	Paterson et al.	
	U 0149	6061793	May 2000	Tewfik et al.	
	U 0150	6069914	May 2000	Cox	
	U 0151	6078664	June 2000	Moskowitz et al.	
	U 0152	6081251	June 2000	Sakai et al.	
	U 0153	6081587	June 2000	Reyes et al.	
	U 0154	6088455	July 2000	Logan et al.	
	U 0155	6131162	October 2000	Yoshiura et al.	
	U 0156	6141753	October 2000	Zhao et al.	
	U 0157	6141754	October 2000	Choy	
	U 0158	6154571	November 2000	Cox et al.	
	U 0159	6192138	February 2001	Yamadaji	
	U 0160	6199058	March 2001	Wong et al.	
	U 0161	6205249	March 2001	Moskowitz	
	U 0162	6208745	March 2001	Florenio et al.	
	U 0163	6230268	May 2001	Miwa et al.	
	U 0164	6233347	May 2001	Chen et al.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 0165	6233684	May 2001	Stefik et al.	
	U 0166	6240121	May 2001	Senoh	
	U 0167	6263313	July 2001	Milstead et al.	
	U 0168	6272634	August 2001	Tewfik et al.	
	U 0169	6275988	August 2001	Nagashima et al.	
	U 0170	6278780	August 2001	Shimada	
	U 0171	6278791	August 2001	Honsinger et al.	
	U 0172	6282300	August 2001	Bloom et al.	
	U 0173	6282650	August 2001	Davis	
	U 0174	6285775	September 2001	Wu et al.	
	U 0175	6301663	October 2001	Kato et al.	
	U 0176	6310962	October 2001	Chung et al.	
	U 0177	6330335	December 2001	Rhoads	
	U 0178	6330672	December 2001	Shur	
	U 0179	6345100	February 2002	Levine	
	U 0180	6351765	February 2002	Pietropaolo et al.	
	U 0181	6363483	March 2002	Keshav	
	U 0182	6373892	April 2002	Ichien et al.	
	U 0183	6373960	April 2002	Conover et al.	
	U 0184	6374036	April 2002	Ryan et al.	
	U 0185	6377625	April 2002	Kim	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 0186	6381618	April 2002	Jones et al.	
	U 0187	6381747	April 2002	Wonfor et al.	
	U 0188	6385329	May 2002	Sharma et al.	
	U 0189	6389538	May 2002	Gruse et al.	
	U 0190	6405203	June 2002	Collart	
	U 0191	6415041	July 2002	Oami et al.	
	U 0192	6425081	July 2002	Iwamura	
	U 0193	6430301	August 2002	Petrovic	
	U 0194	6430302	August 2002	Rhoads	
	U 0195	6442283	August 2002	Tewfik et al.	
	U 0196	6446211	September 2002	Colvin	
	U 0197	6453252	September 2002	Laroche	
	U 0198	6457058	September 2002	Ullum et al.	
	U 0199	6463468	October 2002	Buch et al.	
	U 0200	6484264	November 2002	Colvin	
	U 0201	6493457	December 2002	Quackenbush	
	U 0202	6502195	December 2002	Colvin	
	U 0203	6522767	February 2003	Moskowitz et al.	
	U 0204	6522769	February 2003	Rhoads et al.	
	U 0205	6523113	February 2003	Wehrenberg	
	U 0206	6530021	March 2003	Epstein et al.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 0207	6532284	March 2003	Walker et al.	
	U 0208	6539475	March 2003	Cox et al.	
	U 0209	6557103	April 2003	Boncelet, Jr. et al.	
	U 0210	6584125	June 2003	Katto	
	U 0211	6587837	July 2003	Spagna et al.	
	U 0212	6598162	July 2003	Moskowitz	
	U 0213	6606393	August 2003	Xie et al.	
	U 0214	6647424	November 2003	Pearson et al.	
	U 0215	6658010	December 2003	Enns et al.	
	U 0216	6665489	December 2003	Collart	
	U 0217	6668246	December 2003	Yeung et al.	
	U 0218	6668325	December 2003	Collberg et al	.
	U 0219	6687683	February 2004	Harada et al.	
	U 0220	6725372	April 2004	Lewis et al	.
	U 0221	6754822	June 2004	Zhao	
	U 0222	6775772	August 2004	Binding et al.	
	U 0223	6784354	August 2004	Lu et al.	
	U 0224	6785815	August 2004	Serret-Avila et al.	
	U 0225	6785825	August 2004	Colvin	
	U 0226	6792548	September 2004	Colvin	
	U 0227	6792549	September 2004	Colvin	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 0228	6795925	September 2004	Colvin	
	U 0229	6799277	September 2004	Colvin	
	U 0230	6813717	November 2004	Colvin	
	U 0231	6813718	November 2004	Colvin	
	U 0232	6823455	November 2004	Macy et al.	
	U 0233	6834308	December 2004	Ikezoye et al.	
	U 0234	6842862	January 2005	Chow et al.	
	U 0235	6853726	February 2005	Moskowitz et al.	
	U 0236	6857078	February 2005	Colvin	
	U 0237	6931534	August 2005	Jandel et al.	
	U 0238	6966002	November 2005	Torrubia-Saez	
	U 0239	6983337	November 2005	Wold	
	U 0240	6977894	December 2005	Achilles et al.	
	U 0241	6978370	December 2005	Kocher	
	U 0242	6986063	January 2006	Colvin	
	U 0243	7007166	February 2006	Moskowitz et al.	
	U 0244	7020285	March 2006	Kirovski et al.	
	U 0245	7035409	April 2006	Moskowitz	
	U 0246	7043050	May 2006	Yuval	
	U 0247	7046808	May 2006	Metois et al.	
	U 0248	7050396	May 2006	Cohen et al.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 0249	7051208	May 2006	Venkatesan et al.	
	U 0250	7058570	June 2006	Yu et al.	
	U 0251	7093295	August 2006	Saito	
	U 0252	7095874	August 2006	Moskowitz et al	.
	U 0253	7103184	September 2006	Jian	
	U 0254	7107451	September 2006	Moskowitz	
	U 0255	7123718	October 2006	Moskowitz et al.	
	U 0256	7127615	October 2006	Moskowitz	
	U 0257	7150003	December 2006	Naumovich et al.	
	U 0258	7152162	December 2006	Moskowitz et al.	
	U 0259	7159116	January 2007	Moskowitz	
	U 0260	7162642	January 2007	Schumann et al.	
	U 0261	7177429	February 2007	Moskowitz et al.	
	U 0262	7177430	February 2007	Kim	
	U 0263	7206649	April 2007	Kirovski et al.	
	U 0264	7231524	June 2007	Bums	
	U 0265	7233669.	June 2007	Candelore	
	U 0266	7240210	July 2007	Michak et al.	
	U 0267	7266697	September 2007	Kirovski et al	.
	U 0268	7287275	October 2007	Moskowitz	
	U 0269	7289643	October 2007	Brunk et al.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 0270	7343492	March 2008	Moskowitz et al.	
	U 0271	7346472	March 2008	Moskowitz et al.	
	U 0272	7362775	April 2008	Moskowitz	
	U 0273	7363278	April 2008	Schmelzer et al.	
	U 0274	7409073	August 2008	Moskowitz et al.	
	U 0275	7457962	November 2008	Moskowitz	
	U 0276	7460994	December 2008	Herre et al.	
	U 0277	7475246	January 2009	Moskowitz	
	U 0278	7530102	May 2009	Moskowitz	
	U 0279	7532725	May 2009	Moskowitz et al.	
	U 0280	7568100	July 2009	Moskowitz et al.	
	U 0281	7647502	January 2010	Moskowitz	
	U 0282	7647503	January 2010	Moskowitz	
	U 0283	7779261	August 2010	Moskowitz	
	U 0284	6990453	January 2006	Wang	
	U 0285	6081597	June 2000	Hoffstein	
	U 0286	7035049	Apr 2006	Yamamoto	
	U 0287	7664263	Feb 2010	Moskowitz	
	U 0288	7286451	Oct 2007	Wirtz	
	U 0289	6385324	May 2002	Koppen	
	U 0290	6674858	Jan 2004	Kimura	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(U SERIES)**	PATENT NUMBER	ISSUE DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	U 0291	6148333	Nov 2000	Guedalia	
	U 0292	6418421	Jun 2002	Hurtado	
	U 0293	6385596	May 2002	Wiser	
	U 0294	6226618	May 2001	Downs	
	U 0295	6957330	Oct 2005	Hughes	
	U 0296	5842213	Nov 1998	Odom	
	U 0297	5818818	Oct 1998	Soumiya	
	U 0298	6590996	Jun 2003	Reed	
	U 0299	5949055	Sept 1999	Fleet	
	U 0300	6067622	May 2000	Moore	
	U 0301	7761712	Jun 2010	Moskowitz	
	U 0302	7743001	Jun 2010	Vermeulen	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

LISTING OF UNITED STATES PUBLISHED APPLICATIONS - P Series

EXAMINER INITIALS	REFERENCE NUMBER **(P SERIES)**	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE CITED
	P 01	20010010078	July 2001	Moskowitz	
	P 02	20010043594	November 2001	Ogawa et al.	
	P 03	20020010684	January 2002	Moskowitz	
	P 04	20020026343	February 2002	Duenke	
	P 05	20020056041	May 2002	Moskowitz	
	P 06	20020071556	June 2002	Moskowitz et al.	
	P 07	20020073043	June 2002	Herman et al.	
	P 08	20020097873	July 2002	Petrovic	
	P 09	20020103883	August 2002	Haverstock et al.	
	P 010	20020161741	October 2002	Wang et al.	
	P 011	20030126445	July 2003	Wehrenberg	
	P 012	20030133702	July 2003	Collart	
	P 013	20030200439	October 2003	Moskowitz	
	P 014	20030219143	November 2003	Moskowitz et al.	
	P 015	20040028222	February 2004	Sewell et al.	
	P 016	20040037449	February 2004	Davis et al.	
	P 017	20040049695	March 2004	Choi et al.	
	P 018	20040059918	March 2004	Xu	
	P 019	20040083369	April 2004	Erlingsson et al.	
	P 020	20040086119	May 2004	Moskowitz	
	P 021	20040093521	May 2004	Hamadeh et al.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(P SERIES)**	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE CITED
	P 022	20040117628	June 2004	Colvin	
	P 023	20040117664	June 2004	Colvin	
	P 024	20040125983	July 2004	Reed et al.	
	P 025	20040128514.	July 2004	Rhoads	
	P 026	20040225894	November 2004	Colvin	
	P 027	20040243540	December 2004	Moskowitz et al.	
	P 028	20050135615	June 2005	Moskowitz et al.	
	P 029	20050160271	July 2005	Brundage et al.	
	P 030	20050177727	August 2005	Moskowitz et al.	
	P 031	20050246554	November 2005	Batson	
	P 032	20060005029	January 2006	Petrovic et al.	
	P 033	20060013395	January 2006	Brundage et al.	
	P 034	20060013451	January 2006	Haitsma	
	P 035	20060041753	February 2006	Haitsma	
	P 036	20060101269	May 2006	Moskowitz et al.	
	P 037	20060140403	June 2006	Moskowitz	
	P 038	20060285722	December 2006	Moskowitz et al.	
	P 039	20070011458	January 2007	Moskowitz	
	P 040	20070028113	February 2007	Moskowitz	
	P 041	20070064940	March 2007	Moskowitz et al.	
	P 042	20070079131.	April 2007	Moskowitz et al.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(P SERIES)**	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE CITED
	P 043	20070083467	April 2007	Lindahl et al.	
	P 044	20070110240	May 2007	Moskowitz et al.	
	P 045	20070113094	May 2007	Moskowitz et al.	
	P 046	20070127717	June 2007	Herre et al.	
	P 047	20070226506	September 2007	Moskowitz	
	P 048	20070253594	November 2007	Lu et al.	
	P 049	20070294536.	December 2007	Moskowitz et al.	
	P 050	20070300072	December 2007	Moskowitz	
	P 051	20070300073	December 2007	Moskowitz	
	P 052	20080005571	January 2008	Moskowitz	
	P 053	20080005572	January 2008	Moskowitz	
	P 054	20080016365	January 2008	Moskowitz	
	P 055	20080022113	January 2008	Moskowitz	
	P 056	20080022114	January 2008	Moskowitz	
	P 057	20080028222	January 2008	Moskowitz	
	P 058	20080046742	February 2008	Moskowitz	
	P 059	20080075277	March 2008	Moskowitz et al.	
	P 060	20080109417	May 2008	Moskowitz	
	P 061	20080133927	June 2008	Moskowitz et al.	
	P 062	20080151934	June 2008	Moskowitz et al.	
	P 063	20090037740	February 2009	Moskowitz	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER **(P SERIES)**	PUBLICATION NUMBER	PUBLICATION DATE	NAME OF PATENTEE OR APPLICANT	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE CITED
	P 064	20090089427	April 2009	Moskowitz et al.	
	P 065	20090190754	July 2009	Moskowitz et al.	
	P 066	20090210711	August 2009	Moskowitz	
	P 067	20090220074	September 2009	Moskowitz et al.	
	P 068	20100002904	January 2010	Moskowitz	
	P 069	20100005308	January 2010	Moskowitz	
	P 070	20100098251	Apr 2010	Moskowitz	
	P 071	20100220861	Sept 2010	Moskowitz	
	P 072	20100202607	Aug 2010	Moskowitz	
	P 073	20020047873	June 2002	Petrovic	
	P 074	20020009208	Jan 2002	Alattar	
	P 075	20010029580	October 2001	Moskowitz	
	P 076	20100182570	July 2010	Chota	
	P 077	20100077220	March 2010	Moskowitz	
	P 078	20100077219	March 2010	Moskowitz	
	P 079	20100064140	March 2010	Moskowitz	
	P 080	20100153734	June 2010	Moskowitz	
	P 081	20100106736	April 2010	Moskowitz	
	P 082	20060251291	November 2006	Rhoads	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

LISTING OF **FOREIGN AND INTERNATIONAL PATENT DOCUMENTS - F Series**

EXAMINER INITIALS	REFERENCE NUMBER (**F SERIES**)	PUBLICATION NUMBER	PUBLICATION DATE	COUNTRY OR REGION	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	F 01-	EP0372601	Jun., 1990	EP		
	F 02-	EP0565947	Oct., 1993	EP		
	F 03-	EP0581317	Feb., 1994	EP		
	F 04-	EP0649261	Apr., 1995	EP		
	F 05-	EP0651554	May., 1995	EP		
	F 06-	EP1354276	Dec., 2007	EP		
	F 07-	NL 1005523	Sep., 1998	NL		
	F 08-	WO 9514289	May., 1995	WO		
	F 09-	WO 9629795	Sep., 1996	WO		
	F 010-	WO 9724833	Jul., 1997	WO		
	F 011-	WO 9744736	Nov., 1997	WO		
	F 012-	WO9837513	Aug., 1998	WO		
	F 013-	WO 9952271	Oct., 1999	WO		
	F 014-	WO 9962044	Dec., 1999	WO		
	F 015-	WO 9963443	Dec., 1999	WO		
	F 016-	WO9726733	Jan. 1997	WO		
	F 017-	WO98002864	Jul. 1997	WO		
	F 018-	WO 0057643	Sept 2000	WO		
	F 019-	WO 9642151	Dec 1996	WO		
	F 020-	EP0872073	July 1996	EP		

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REFERENCE NUMBER (**F SERIES**)	PUBLICATION NUMBER	PUBLICATION DATE	COUNTRY OR REGION	PAGE/LINE AND FIGURE/ELEMENT OF RELEVANT MATERIAL	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	F 021-	WO0118628	March 2001	WO		
	F 022-	WO0143026	June 2001	WO		
	F 023-	WO0203385	Jan 2002	WO		
	F 024-	WO9701892	June 1995	WO		
	F 025-	WO9726732	July 1997	WO		
	F 026-	WO9802864	Jan 1998	WO		
	F 027-	EP1547337	Mar 2006	EP		
	F 028-	EP0581317A2	Feb 1994	EP		
	F 029-	WO023385A1	Oct 2002	WO		

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

LISTING OF NON PATENT LITERATURE - O Series

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	1	L- 01	7/28/2009	US. Appl. No. 08/999,766, filed Jul. 23, 1997, entitled "Steganographic Method and Device", published as 7,568,100 07-28-2009.	
	2	L- 02	N/A	EPO Application No. 96919405.9, entitled "Steganographic Method and Device"; published as EP0872073 (A2), published 10-21-1998.	
	3	L- 03	8/11/2005	U.S. Appl. No. 11/050,779, filed Feb. 7, 2005, entitled "Steganographic Method and Device", published as 20050177727 A1 08-11-2005.	
	4	L- 04	4/22/2008	U.S. Appl. No. 08/674,726, filed Jul. 2, 1996, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management", published as 7,362,775 04-22-2008 .	
	5	L- 05	N/A	U.S. Appl. No. 09/545,589, filed Apr. 7, 2000, entitled "Method and System for Digital Watermarking", published as 7,007,166 02-28-2006	
	6	L- 06	N/A	U.S. Appl. No. 11/244,213, filed Oct. 5, 2005, entitled "Method and System for Digital Watermarking", published as 2006-0101269 A1 05-11-2006	

DATE:	EXAMINER'S SIGNATURE:

DISH-Blue Spike-842
Exhibit 1004, Page 1283

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	7	L- 07	N/A	U.S. Appl. No. 11/649,026, filed Jan. 3, 2007, entitled "Method and System for Digital Watermarking", published as 2007-0113094 A1 05-17-2007.	
	8	L- 08	N/A	U.S. Appl. No. 09/046,627, filed Mar. 24, 1998, entitled "Method for Combining Transfer Function with Predetermined Key Creation", published as 6,598,162 07-22-2003 .	
	9	L- 09	N/A	U.S. Appl. No. 10/602,777, filed Jun. 25, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation", published as 2004-0086119 A1 05-06-2004	
	10	L- 010	N/A	U.S. Appl. No. 09/053,628, filed Apr. 2, 1998, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking", 6,205,249 03-20-2001	
	11	L- 011	N/A	U.S. Appl. No. 09/644,098, filed Aug. 23, 2000, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking", published as 7,035,409 04-25-2006	
	12	L- 012	N/A	Jap. App. No. 2000-542907, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking", JP national stage of PCT/US1999/007262, published as WO99052271, 10/14/1999, F13 here in above.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	13	L- 013	N/A	U.S. Appl. No. 09/767,733, filed Jan. 24, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking", published as 2001-0010078 A1 07-26-2001.	
	14	L- 014	N/A	U.S. Appl. No. 11/358,874, filed Feb. 21, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking", published as 2006-0140403 A1 06-29-2006	
	15	L- 015	N/A	U.S. Appl. No. 10/417,231, filed Apr. 17, 2003, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth", published as 2003-0200439 A1 10-23-2003	
	16	L- 016	N/A	U.S. Appl. No. 09/789,711, filed Feb. 22, 2001, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2001-0029580 A1 10-11-2001.	
	17	L- 017	N/A	U.S. Appl. No. 11/497,822, filed Aug. 2, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2007-0011458 A1 01-11-2007	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	18	L- 018	N/A	U.S. Appl. No. 11/599,964, filed Nov. 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2008-0046742 A1 02-21-2008.	
	19	L- 019	N/A	U.S. Appl. No. 11/599,838, filed Nov. 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2007-0226506 A1 09-27-2007	
	20	L- 020	N/A	U.S. Appl. No. 10/369,344, filed Feb. 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data", published as 2003-0219143 A1 11-27-2003.	
	21	L- 021	N/A	U.S. Appl. No. 11/482,654, filed Jul. 7, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data", published as 2006-0285722 A1 12-21-2006.	
	22	L- 022	N/A	U.S. Appl. No. 09/594,719, filed Jun. 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems", published as 7,123,718 10-17-2006 .	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	23	L- 023	N/A	U.S. Appl. No. 11/519,467, filed Sep. 12, 2006, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems", published as 2007-0064940 A1 03-22-2007.	
	24	L- 024	N/A	U.S. Appl. No. 09/731,040, filed Dec. 7, 2000, entitled "Systems, Methods And Devices For Trusted Transactions", 2002-0010684 A1 01-24-2002.	
	25	L- 025	N/A	U.S. Appl. No. 11/512,701, filed Aug. 29, 2006, entitled "Systems, Methods And Devices For Trusted Transactions", published as 2007-0028113 A1 02-01-2007.	
	26	L- 026	N/A	U.S. Appl. No. 10/049,101, filed Feb. 8, 2002, entitled "A Secure Personal Content Server", published as 7,475,246 01-06-2009.	
	27	L- 027	N/A	PCT Application No. PCT/US00/21189, filed Aug. 4, 2000, entitled, "A Secure Personal Content Server", Pub. No.: WO018628 ; Publication Date: 15.03.2001, F21 here in above.	
	28	L- 028	N/A	U.S. Appl. No. 09/657,181, filed Sep. 7, 2000, entitled "Method and Device For Monitoring And Analyzing Signals", published as 7,346,472 03-18-2008.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	29	L- 029	N/A	U.S. Appl. No. 10/805,484, filed Mar. 22, 2004, entitled "Method And Device For Monitoring And Analyzing Signals", published as 2004-0243540 A1 12-02-2004.	
	30	L- 030	N/A	U.S. Appl. No. 09/956,262, filed Sep. 20, 2001, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects", published as 2002-0056041 A1 05-09-2002	
	31	L- 031	N/A	U.S. Appl. No. 11/518,806, filed Sep. 11, 2006, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects", 2008-0028222 A1 01-31-2008 .	
	32	L- 032	N/A	U.S. Appl. No. 11/026,234, filed Dec. 30, 2004, entitled "Z-Transform Implementation of Digital Watermarks" , published as 2005-0135615 A1 06-23-2005.	
	33	L- 033	N/A	U.S. Appl. No. 11/592,079, filed Nov. 2, 2006, entitled "Linear Predictive Coding Implementation of Digital Watermarks", published as 2007-0079131 A1 04-05-2007.	
	34	L- 034	N/A	U.S. Appl. No. 09/731,039, filed Dec. 7, 2000, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects", published as 2002-0071556 A1 06-13-2002	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	35	L- 035	N/A	U.S. Appl. No. 11/647,861, filed Dec. 29, 2006, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects", published as 2007-0110240 A1 05-17-2007.	
	36	L- 036	1996	Schneier, Bruce, Applied Cryptography, 2nd Ed., John Wiley & Sons, pp. 9-10, 1996.	
	37	L- 037	1997	Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, p. 46, 1997.	
	38	L- 038	1997	Merriam-Webster's Collegiate Dictionary, 10th Ed., Merriam Webster, Inc., p. 207.	
	39	L- 039	1984	Brealy, et al., Principles of Corporate Finance, "Appendix A--Using Option Valuation Models", 1984, pp. 448-449.	
	40	L- 040	2001	Copeland, et al., Real Options: A Practitioner's Guide, 2001 pp. 106-107, 201-202, 204-208.	
	41	L- 041	1995	Sarkar, M. "An Assessment of Pricing Mechanisms for the Internet-A Regulatory Imperative", presented MIT Workshop on Internet Economics, Mar. 1995 http://www.press.vmich.edu/iep/works/SarkAsses.html on.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	42	L- 042	1995	Crawford, D.W. "Pricing Network Usage: A Market for Bandwidth of Market Communication?" presented MIT Workshop on Internet Economics, Mar. 1995 http://www.press.vmich.edu/iep/works/CrawMarket.html on March.	
	43	L- 043	1988	Low, S.H., "Equilibrium Allocation and Pricing of Variable Resources Among User-Suppliers", 1988. http://www.citesear.nj.nec.com/366503.html.	
	44	L- 044	1995	Caronni, Germano, "Assuring Ownership Rights for Digital Images", published proceeds of reliable IT systems, v15 '95, H.H. Bruggemann and W. Gerhardt-Hackel (Ed) Viewing Publishing Company Germany 1995.	
	45	L- 045	1996	Zhao, Jian. "A WWW Service to Embed and Prove Digital Copyright Watermarks", Proc. of the European conf. on Multimedia Applications, Services & Techniques Louvain-La-Nevve Belgium May 1996.	
	46	L- 046	1996	Gruhl, Daniel et al., Echo Hiding. In Proceeding of the Workshop on Information Hiding. No. 1174 in Lecture Notes in Computer Science, Cambridge, England (May/Jun. 1996).	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	47	L- 047	1995	Oomen, A.W.J. et al., A Variable Bit Rate Buried Data Channel for Compact Disc, J.AudioEng. Sc., vol. 43, No. 1/2, pp. 23-28 (1995).	
	48	L- 048	1992	Ten Kate, W. et al., A New Surround-Stereo-Surround Coding Techniques, J. Audio Eng.Soc., vol. 40,No. 5,pp. 376-383 (1992).	
	49	L- 049	1993	Gerzon, Michael et al., A High Rate Buried Data Channel for Audio CD, presentation notes, Audio Engineering Soc. 94th Convention (1993).	
	50	L- 050	1988	Sklar, Bernard, Digital Communications, pp. 601-603 (1988).	
	51	L- 051	1984	Jayant, N.S. et al., Digital Coding of Waveforms, Prentice Hall Inc., Englewood Cliffs, NJ, pp. 486-509 (1984)	
	52	L- 052	1995	Bender, Walter R. et al., Techniques for Data Hiding, SPIE Int. Soc. Opt. Eng., vol. 2420, pp. 164-173, 1995.	
	53	L- 053	1995	Zhao, Jian et al., Embedding Robust Labels into Images for Copyright Protection, (xp 000571976), pp. 242-251, 1995.	
	54	L- 054	1997	Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, p. 175, 1997.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	55	L- 055	1994	Schneier, Bruce, Applied Cryptography, 1st Ed., pp. 67-68, 1994.	
	56	L- 056	1990	Ten Kate, W. et al., "Digital Audio Carrying Extra Information", IEEE, CH 2847-2/90/0000-1097, (1990).	
	57	L- 057	1994	Van Schyndel, et al., "A digital Watermark," IEEE Int'l Computer Processing Conference, Austin,TX, Nov. 13-16, 1994, pp. 86-90.	
	58	L- 058	1996	Smith, et al. "Modulation and Information Hiding in Images", Springer Verlag, 1st Int'l Workshop, Cambridge, UK, May 30-Jun. 1, 1996, pp. 207-227.	
	59	L- 059	1997	Kutter, Martin et al., "Digital Signature of Color Images Using Amplitude Modulation", SPIE-E197, vol. 3022, pp. 518-527.	
	60	L- 060	1997	Puate, Joan et al., "Using Fractal Compression Scheme to Embed a Digital Signature into an Image", SPIE-96 Proceedings, vol. 2915, Mar. 1997, pp. 108-118.	
	61	L- 061	1996	Swanson, Mitchell D.,et al., "Transparent Robust Image Watermarking", Proc. of the 1996 IEEE Int'l Conf. on Image Processing, vol. 111, 1996 , pp. 211-214.	
	62	L- 062	1996	Swanson, Mitchell D., et al. "Robust Data Hiding for Images", 7th IEEE Digital Signal Processing Workshop, Leon, Norway. Sep. 1-4, 1996, pp. 37-40.	

DATE:	EXAMINER'S SIGNATURE:

DISH-Blue Spike-842
Exhibit 1004, Page 1292

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	63	L- 063	Unknown	Zhao, Jian et al., "Embedding Robust Labels into Images for Copyright Protection", Proceeding of the Know Right '95 Conference, pp. 242-251.	
	64	L- 064	1995	Koch, E., et al., "Towards Robust and Hidden Image Copyright Labeling", 1995 IEEE Workshop on Nonlinear Signal and Image Processing, Jun. 1995 Neos Marmaras pp. 4.	
	65	L- 065	1995	Van Schyandel, et al., "Towards a Robust Digital Watermark", Second Asain Image Processing Conference, Dec. 6-8, 1995, Singapore, vol. 2, pp. 504-508.	
	66	L- 066	1995	Tirkel,A.Z., "A Two-Dimensional Digital Watermark", DICTA '95, Univ. of Queensland, Brisbane, Dec. 5-8, 1995, pp. 7.	
	67	L- 067	1996	Tirkel,A.Z., "Image Watermarking--A Spread Spectrum Application", ISSSTA '96, Sep. 1996, Mainz, German, pp. 6.	
	68	L- 068	1996	O'Ruanaidh, et al. "Watermarking Digital Images for Copyright Protection", IEEE Proceedings, vol. 143, No. 4, Aug. 1996, pp. 250-256.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	69	L- 069	Unknown	Cox, et al., Secure Spread Spectrum Watermarking for Multimedia, NEC Research Institude, Techinal Report 95-10, pp. 33.	
	70	L- 070	1969	Kahn, D., "The Code Breakers", The MacMillan Company, 1969, pp. xIII, 81-83, 513, 515, 522-526, 863.	
	71	L- 071	1997	Boney, et al., Digital Watermarks for Audio Signals, EVSIPCO, 96, pp. 473-480 (3/14/1997).	
	72	L- 072	1996	Dept. of Electrical Engineering, Del Ft University of Technology, Del ft The Netherlands, Cr.C. Langelaar et al.,"Copy Protection for Multimedia Data based on Labeling Techniques", Jul. 1996 9 pp.	
	73	L- 073	Unknown	F. Hartung, et al., "Digital Watermarking of Raw and Compressed Video", SPIE vol. 2952, pp. 205-213.	
	74	L- 074	1996	Craver, et al., "Can Invisible Watermarks Resolve Rightful Ownerships?", IBM Research Report, RC 20509 (Jul. 25, 1996) 21 pp.	
	75	L- 075	1988	Press, et al., "Numerical Recipes in C", Cambridge Univ. Press, 1988, pp. 398-417.	
	76	L- 076	1995	Pohlmann, Ken C., "Principles of Digital Audio", 3rd Ed., 1995, pp. 32-37, 40-48:138, 147-149, 332, 333, 364, 499-501, 508-509, 564-571.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	77	L- 077	1991	Pohlmann, Ken C., "Principles of Digital Audio", 2nd Ed., 1991, pp. 1-9, 19-25, 30-33, 41-48, 54-57, 86-107, 375-387.	
	78	L- 078	1994	Schneier, Bruce, Applied Cryptography, John Wiley & Sons, Inc., New York, 1994, pp. 68, 69, 387-392, 1-57, 273-275, 321-324.	
	79	L- 079	1996	Boney, et al., Digital Watermarks for Audio Signals, Proceedings of the International Conf. on Multimedia Computing and Systems, Jun. 17-23, 1996 Hiroshima, Japan, 0-8186-7436-9196, pp. 473-480.	
	80	L- 080	1998	Johnson, et al., "Transform Permuted Watermarking for Copyright Protection of Digital Video", IEEE Globecom 1998, Nov. 8-12, 1998, New York New York vol. 2 1998 pp. 684-689 (ISBN 0-7803-4985-7).	
	81	L- 081	1996	Rivest, et al., "Pay Word and Micromint: Two Simple Micropayment Schemes," MIT Laboratory for Computer Science, Cambridge, MA, May 7, 1996 pp. 1-18.	
	82	L- 082	1996	Bender, et al., "Techniques for Data Hiding", IBM Systems Journal, (1996) vol. 35, Nos. 3 & 4,1996, pp. 313-336.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	83	L- 083	2003	Moskowitz, "Bandwith as Currency", IEEE Multimedia, Jan.-Mar. 2003, pp. 14-21.	
	84	L- 084	2006	Moskowitz, Multimedia Security Technologies for Digital Rights Management, 2006, Academic Press, "Introduction--Digital Rights Management" pp. 3-22.	
	85	L- 085	2001	Rivest, et al., "PayWord and Micromint: Two Simple Micropayment Schemes," MIT Laboratory for Computer Science, Cambridge, MA, Apr. 27, 2001, pp. 1-18.	
	86	L- 086	2000	Tomsich, et al., "Towards a secure and de-centralized digital watermarking infrastructure for the protection of Intellectual Property", in Electronic Commerce and Web Technologies, Proceedings (ECWEB)(2000).	
	87	L- 087	2002	Moskowitz, "What is Acceptable Quality in the Application of Digital Watermarking: Trade-offs of Security; Robustness and Quality", IEEE Computer Society Proceedings of ITCC 2002 Apr. 10, 2002 pp. 80-84.	
	88	L- 088	2006	Lemma, et al. "Secure Watermark Embedding through Partial Encryption", International Workshop on Digital Watermarking" ("IWDW" 2006). Springer Lecture Notes in Computer Science 2006 (to appear) 13.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	89	L- 089	2002	Kocher, et al., "Self Protecting Digital Content", Technical Report from the CRI Content Security Research Initiative, Cryptography Research, Inc. 2002-2003 14 pages.	
	90	L- 090	1995	Sirbu, M. et al., "Net Bill: An Internet Commerce System Optimized for Network Delivered Services", Digest of Papers of the Computer Society Computer Conference (Spring) Mar. 5, 1995 pp. 20-25 vol. CONF40.	
	91	L- 091	1998	Schunter, M. et al., "A Status Report on the SEMPER framework for Secure Electronic Commerce", Computer Networks and ISDN Systems, Sep. 30, 1998, pp. 1501-1510 vol. 30 No. 16-18 NL North Holland.	
	92	L- 092	1999	Konrad, K. et al., "Trust and Electronic Commerce--more than a technical problem," Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems Oct. 19-22, 1999, pp. 360-365 Lausanne.	
	93	L- 093	1998	Kini, et al., "Trust in Electronic Commerce: Definition and Theoretical Considerations", Proceedings of the 31st Hawaii Int'l Conf on System Sciences (Cat. No. 98TB100216). Jan. 6-9, 1998. pp. 51-61. Los.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	94	L- 094	1997	Steinauer D. D., et al., "Trust and Traceability in Electronic Commerce", Standard View, Sep. 1997, pp. 118-124, vol. 5 No. 3, ACM, USA.	
	95	L- 095	1999	Hartung, et al. "Multimedia Watermarking Techniques", Proceedings of the IEEE, Special Issue, Identification & Protection of Multimedia Information, pp. 1079-1107 Jul. 1999 vol. 87 No. 7 IEEE.	
	96	L- 096	N/A	European Search Report & European Search Opinion in EP07112420	
	97	L- 097	2006	STAIND (The Singles 1996-2006), Warner Music--Atlantic, Pre-Release CD image, 2006, 1 page.	
	98	L- 098		DUPLICATE OF L-97, DELETED BY 11/16/2010 by RAN.	
	99	L- 099	2003	Radiohead ("Hail To The Thief"), EMI Music Group--Capitol, Pre-Release CD image, 2003, 1 page.	
	100	L- 0100	N/A	DUPLICATE OF L-4, DELETED BY RN UPON REVIEW ON 11/18/2010. RAN	
	101	L- 0101	N/A	U.S. Appl. No. 60/169,274, filed Dec. 7, 1999, entitled "Systems, Methods And Devices For Trusted Transactions".	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	102	L- 0102		DUPLICATE OF L-22, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	103	L- 0103		DUPLICATE OF L-27, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	104	L- 0104	N/A	U.S. Appl. No. 60/234,199, filed Sep. 20, 2000, "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects".	
	105	L- 0105	N/A	U.S. Appl. No. 09/671,739, filed Sep. 29, 2000, entitled "Method And Device For Monitoring And Analyzing Signals", abandoned.	
	106	L- 0106		DUPLICATE OF L-34, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	107	L- 0107		DUPLICATE OF L-24, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	108	L- 0108		DUPLICATE OF L-57, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	109	L- 0109		DUPLICATE OF L-58, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	

DATE:	EXAMINER'S SIGNATURE:

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	110	L- 0110		DUPLICATE OF L-59, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	111	L- 0111		DUPLICATE OF L-61, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	112	L- 0112		DUPLICATE OF L-62, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	113	L- 0113		DUPLICATE OF L-63, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	114	L- 0114		DUPLICATE OF L-65, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	115	L- 0115	Unknown	Tirkel, A.Z., "A Two-Dimensional Digital Watermark", Scientific Technology, 686, 14, date unknown. (citation revised upon review on 11/16/10 by RAN.)	
	116	L- 0116		DUPLICATE OF L-65, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	117	L- 0117		DUPLICATE OF L-68, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	118	L- 0118		DUPLICATE OF L-69, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	119	L- 0119		DUPLICATE OF L-70, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	120	L- 0120		DUPLICATE OF L-71, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	121	L- 0121		DUPLICATE OF L-72, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	122	L- 0122		DUPLICATE OF L-73, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	123	L- 0123		DUPLICATE OF L-74, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	124	L- 0124		DUPLICATE OF L-75, DELETED BY RN UPON REVIEW ON 11/16/2010. RAN	
	125	L- 0125		DUPLICATE OF L-076, REMOVED. RN. 11/16/2010	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	126	L- 0126		DUPLICATE OF L-77, REMOVED. RN. 11/16/2010	
	127	L- 0127		DUPLICATE OF L-78, REMOVED. RN. 11/16/2010	
	128	L- 0128		DUPLICATE OF L-79, REMOVED. RN. 11/16/2010	
	129	L- 0129		EP0581317A2, MOVED TO FOREIGN PATENT PUBS as F-028	
	130	L- 0130		DUPLICATE OF L-52, REMOVED. RN. 11/16/2010	
	131	L- 0131		DUPLICATE OF L-36, REMOVED. RN. 11/16/2010	
	132	L- 0132		DUPLICATE OF L-38, REMOVED. RN. 11/16/2010.	
	133	L- 0133		DUPLICATE OF L-37, REMOVED. RN. 11/16/2010	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	134	L- 0134		DUPLICATE OF L-36, REMOVED. RN. 11/16/2010	
	135	L- 0135		DUPLICATE OF L-37, REMOVED. RN. 11/16/2010	
	136	L- 0136		DUPLICATE OF L-38, REMOVED. RN. 11/16/2010	
	137	L- 0137		DUPLICATE OF L-39, REMOVED. RN. 11/16/2010	
	138	L- 0138		DUPLICATE OF L-40, REMOVED. RN. 11/16/2010	
	139	L- 0139		DUPLICATE OF L-41, REMOVED. RN. 11/16/2010	
	140	L- 0140		DUPLICATE OF L-42, REMOVED. RN. 11/16/2010	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	141	L- 0141		DUPLICATE OF L-43, REMOVED. RN. 11/16/2010	
	142	L- 0142		DUPLICATE OF L-44, REMOVED. RN. 11/16/2010	
	143	L- 0143		DUPLICATE OF L-45, REMOVED. RN. 11/16/2010.	
	144	L- 0144		DUPLICATE OF L-46, REMOVED. RN. 11/16/2010.	
	145	L- 0145		DUPLICATE OF L-47, REMOVED. RN. 11/16/2010	
	146	L- 0146		DUPLICATE OF L-48, REMOVED. RN. 11/16/2010	
	147	L- 0147		DUPLICATE OF L-49, REMOVED. RN. 11/16/2010	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	148	L- 0148		DUPLICATE OF L-50, REMOVED. RN. 11/16/2010	
	149	L- 0149		DUPLICATE OF L-51, REMOVED. RN. 11/16/2010	
	150	L- 0150		DUPLICATE OF L-52, REMOVED. RN. 11/16/2010	
	151	L- 0151		DUPLICATE OF L-63, REMOVED. RN. 11/16/2010	
	152	L- 0152		DUPLICATE OF L-54, REMOVED. RN. 11/16/2010	
	153	L- 0153		DUPLICATE OF L-55, REMOVED. RN. 11/16/2010.	
	154	L- 0154		DUPLICATE OF L-80, REMOVED. RN. 11/16/2010.	
	155	L- 0155	N/A	PCT International Search Report in PCT/US95/08159.	
	156	L- 0156	N/A	PCT International Search Report in PCT/US96/10257	
	157	L- 0157	N/A	Supplementary European Search Report in EP 96919405.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	158	L- 0158	N/A	PCT International Search Report in PCT/US97/00651.	
	159	L- 0159	N/A	PCT International Search Report in PCT/US97/00652	
	160	L- 0160	N/A	PCT International Search Report in PCT/US97/11455.	
	161	L- 0161	N/A	PCT International Search Report in PCT/US99/07262.	
	162	L- 0162	N/A	PCT International Search Report, completed Jun. 30, 2000; authorized officer Paul E. Callahan (PCT/US00/06522) (7 pages).	
	163	L- 0163	N/A	Supplementary European Search Report in EP00919398	
	164	L- 0164	N/A	PCT International Search Report in PCT/US00/18411.	
	165	L- 0165	N/A	PCT International Search Report in PCT/US00/18411.	
	166	L- 0166	N/A	PCT International Search Report in PCT/US00/33126	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	167	L- 0167	N/A	PCT International Search Report in PCT/US00/21189	
	168	L- 0168	1996	Delaigle, J.-F., et al. "Digital Watermarking," Proceedings of the SPIE, vol. 2659, Feb 1, 1996, pp. 99-110.	
	169	L- 0169	1996	Schneider, M., et al. "A Robust Content Based Digital Signature for Image Authentication," Proceedings of the International Conference on Image Processing (IC. Lausanne) Sep. 16-19, 1996, pp. 227-230, IEEE ISBN.	
	170	L- 0170	1997	Cox, I. J., et al. "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6 No. 12, Dec. 1, 1997, pp. 1673-1686.	
	171	L- 0171	1998	Wong, Ping Wah. "A Public Key Watermark for Image Verification and Authentication," IEEE International Conference on Image Processing, vol. 1 Oct. 4-7, 1998, pp. 455-459.	
	172	L- 0172	1998	Fabien A.P. Petitcolas, Ross J. Anderson and Markkus G. Kuhn, "Attacks on Copyright Marking Systems," LNCS, vol. 1525, Apr. 14-17, 1998, pp. 218-238 ISBN: 3-540-65386-4.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	173	L- 0173	1996	Ross Anderson, "Stretching the Limits of Steganography," LNCS, vol. 1174, May/Jun. 1996, 10 pages, ISBN: 3-540-61996-8.	
	174	L- 0174	1997	Joseph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", pre-publication, Summer 1997 4 pages.	
	175	L- 0175	1997	Joseph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", Submitted to Signal Processing Aug. 21, 1997, 19 pages.	
	176	L- 0176	2008	OASIS (Dig Out Your Soul), Big Brother Recordings Ltd, Promotional CD image, 2008, 1 page.	
	177	L- 0177	1998	Rivest, R. "Chaffing and Winnowing: Confidentiality without Encryption", MIT Lab for Computer Science, http://people.csail.mit.edu/rivest/Chaffing.txt Apr. 24, 1998, 9 pp.	
	178	L- 0178	2003	PortalPlayer, PP502 digital media management system-on-chip, May 1, 2003, 4 pp.	
	179	L- 0179	2001	VeriDisc, "The Search for a Rational Solution to Digital Rights Management (DRM)", http://64.244.235.240/news/whitepaper, /docs/veridisc.sub.--white.sub.--paper.pdf, 2001, 15 pp.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	180	L- 0180	2008	Cayre, et al., "Kerckhoff's-Based Embedding Security Classes for WOA Data Hiding", IEEE Transactions on Information Forensics and Security, vol. 3 No. 1, Mar. 2008, 15 pp.	
	181	L- 0181	1999	Wayback Machine, dated Jan. 17, 1999, http://web.archive.org/web/19990117020420/http://www.netzero.com/, accessed on Feb. 19, 2008.	
	182	L- 0182	1997	Namgoong, H., "An Integrated Approach to Legacy Data for Multimedia Applications", Proceedings of the 23rd EUROMICRO Conference, vol., Issue 1-4, Sep. 1997, pp. 387-391.	
	183	L- 0183	2007	Wayback Machine, dated Aug. 26, 2007, http://web.archive,org/web/20070826151732/http://www.screenplaysmag.com/t-abid/96/articleType/ArticleView/articleId/495/Default.aspx/.	
	184	L- 0184	2009	"YouTube Copyright Policy: Video Identification tool--YouTube Help", accessed Jun. 4, 2009, http://www.google.com/support/youtube/bin/answer.py?h1=en&answer=83766, 3 pp.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	185	L- 0185	N/A	U.S. Appl. No. 12/665,002, filed Dec. 22, 2009, entitled "Method for Combining Transfer Function with Predetermined Key Creation", published as 2010-0182570 A1 07-22-2010.	
	186	L- 0186	N/A	U.S. Appl. No. 12/592,331, filed Nov. 23, 2009, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2010-0077220 A1 03-25-2010.	
	187	L- 0187	N/A	U.S. Appl. No. 12/590,553, filed Nov. 10, 2009, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2010-0077219 A1 03-25-2010.	
	188	L- 0188	N/A	U.S. Appl. No. 12/590,681, filed Nov. 12, 2009, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data", published as 2010-0064140 A1 03-11-2010.	
	189	L- 0189	N/A	U.S. Appl. No. 12/655,036, filed Dec. 22, 2009, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems", published as 2010-0153734 A1 06-17-2010 .	
	190	L- 0190	N/A	U.S. Appl. No. 12/655,357, filed Dec. 22, 2009, entitled "Method And Device For Monitoring And Analyzing Signals", published as 2010-0106736 A1 04-29-2010.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	191	L- 0191	N/A	PCT Application No. PCT/US95/08159, filed Jun. 26, 1995, entitled, "Digital Information Commodities Exchange with Virtual Menuing", published as WO/1997/001892; Publication Date: 16.01.1997.	
	192	L- 0192	N/A	PCT Application No. PCT/US96/10257, filed Jun. 7, 1996, entitled "Steganographic Method and Device"--corresponding to--EPO Application No. 96919405.9, entitled "Steganographic Method and Device", published as WO/1996/042151; Publication Date: 27.12.1996.	
	193	L- 0193	N/A	PCT Application No. PCT/US97/00651, filed Jan. 16, 1997, entitled, "Method for Stega-Cipher Protection of Computer Code", published as WO/1997/026732; Publication Date: 24.07.1997.	
	194	L- 0194	N/A	PCT Application No. PCT/US97/00652, filed Jan. 17, 1997, entitled, "Method for an Encrypted Digital Watermark", published as WO/1997/026733; Publication Date: 24.07.1997	
	195	L- 0195	N/A	PCT Application No. PCT/US97/11455, filed Jul. 2, 1997, entitled, "Optimization Methods for the Insertion, Protection and Detection of Digital Watermarks in Digitized Data", published as WO/1998/002864; Publication Date: 22.01.1998	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	196	L- 0196	N/A	PCT Application No. PCT/US99/07262, filed Apr. 2, 1999, entitled, "Multiple Transform Utilization and Applications for Secure Digital Watermarking", published as WO/1999/052271; Publication Date: 14.10.1999.	
	197	L- 0197	N/A	PCT Application No. PCT/US00/06522, filed Mar. 14, 2000, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems", published as WO/2000/057643; Publication Date: 28.09.2000.	
	198	L- 0198	N/A	PCT Application No. PCT/US00/18411, filed Jul. 5, 2000, entitled, "Copy Protection of Digital Data Combining Steganographic and Cryptographic Techniques"--corresponding to AU200060709A5 (not available).	
	199	L- 0199	N/A	PCT Application No. PCT/US00/33126, filed Dec. 7, 2000, entitled "Systems, Methods and Devices for Trusted Transactions", published as WO/2001/043026; Publication Date: 14.06.2001.	
	200	L- 0200	N/A	EPO Divisional Patent Application No. 07112420.0, entitled "Steganographic Method and Device" corresponding to PCT Application No. PCT/US96/10257, cited herein above as L-192.	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	201	L- 0201	N/A	US Provisional Application 60/222,023 filed July 31, 2007 entitled "Method and apparatus for recognizing sound and signals in high noise and distortion"	
	202	L- 0202	N/A	US Application 11/458,639 filed July 19, 2006 entitled "Methods and Systems for Inserting Watermarks in Digital Signals", published as 2006-0251291 A1 11-09-2006.	
	203	L- 0203	1995	"Techniques for Data Hiding in Audio Files," by Morimoto, 1995	
	204	L- 0204	1998	Howe, Dennis July 13, 1998 http://foldoc..org//steganography	
	205	L- 0205	N/A	CSG, Computer Support Group and CSGNetwork.com 1973 http://www.csgnetwork.com/glossarys.html	
	206	L- 0206	2010	QuinStreet Inc. 2010 What is steganography?-A word definition from the Webopedia Computer Dictionary http://www.webopedia.com/terms/steganography.html	
	207	L- 0207	2000	Graham, Robert August 21, 2000 "Hacking Lexicon" http://robertgraham.com/pubs/hacking-dict.html	

DATE:	EXAMINER'S SIGNATURE:

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

EXAMINER INITIALS	REF. NO. (L series)	REFERENCE NUMBER (L Series)	PUB. DATE	INCLUDE IN SEQUENCE: Name of first author (in CAPITAL LETTERS), Title in quotation marks, name of publication, date or publication, page numbers, publisher, city of publication, and country of publication NOTE - For US patent applications listed herein, if a publication of the application is identified, Applicant is citing the listed publication and not submitting a copy of the cited application as filed. The examiner is invited to inspect the IFW as desired to view any application as filed.	ENGLISH LANGUAGE TRANSLATION ATTACHED? (YES OR NO) AND/OR OR IDENTIFICATION OF PRIORITY APPLICATION IN WHICH REFERENCE IS CITED
	208	L- 0208	2010	Farkex, Inc 2010 "Steganography definition of steganography in the Free Online Encyclopedia" http://encyclopedia2.Thefreedictionary.com/steganography	
	209	L- 0209	1989	Horowitz, et al., The Art of Eletronics. 2nd Ed., 1989, pp7	
	210	L- 0210	2004	Jimmy eat world ("futures"), Interscope Records, Pre-Release CD image, 2004, 1 page.	
	211	L- 0211	2001	Aerosmith ("Just Push Play"), Pre-Release CD image, 2001, 1 page.	
	212	L- 0212	2002	Phil Collins(Testify) Atlantic, Pre-Release CD image, 2002, 1 page.	

ran

Date/time code: November 19, 2010 (12:45pm)

Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd

DATE:	EXAMINER'S SIGNATURE:

DISH-Blue Spike-842
Exhibit 1004, Page 1314

Printed: November 19, 2010 (12:45pm)
Path: Y:\Clients\SCOT Scott A Moskowitz and Wistaria Trading, Inc\SCOT0014-4\Drafts\IDS_SCOT00014-4_11-19-2010.wpd
37 CFR 1.98(a)(1)(i) APPLICATION:
37 CFR 1.98(a)(1)(iii): THIS IS AN INFORMATION DISCLOSURE STATEMENT

DATE:	EXAMINER'S SIGNATURE:

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 581 317 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: **93112290.7**

(51) Int. Cl.5: **G07D 7/00**, G07F 7/12

(22) Date of filing: **30.07.93**

(30) Priority: **31.07.92 US 923841**

(43) Date of publication of application:
02.02.94 Bulletin 94/05

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(71) Applicant: **INTERACTIVE HOME SYSTEMS**
17950 N.E. 65th Street
Redmond, Washington 98052(US)

(72) Inventor: **Powell, Robert D.**
13720 - 246th Avenue Southeast
Issaquah, Washington 98027(US)
Inventor: **Nitzberg, Mark J.**
20A Prescott Street No.3B
Cambridge, Massachusetts 02138(US)

(74) Representative: **Patentanwälte Grünecker, Kinkeldey, Stockmair & Partner**
Maximilianstrasse 58
D-80538 München (DE)

(54) Method and system for digital image signatures.

(57) A method and system for embedding signatures within visual images in both digital representation and print or film. A signature is inseparably embedded within the visible image, the signature persisting through image transforms that include resizing as well as conversion to print or film and back to digital form. Signature points are selected from among the pixels of an original image. The pixel values of the signature points and surrounding pixels are adjusted by an amount detectable by a digital scanner. The adjusted signature points form a digital signature which is stored for future identification of subject images derived from the image. In one embodiment, a signature is embedded within an image by locating relative extrema in the continuous space of pixel values and selecting the signature points from among the extrema. Preferably, the signature is redundantly embedded in the image such that any of the redundant representations can be used to identify the signature. Identification of a subject image includes ensuring that the subject image is normalized with respect to the original image or the signed image. Preferably, the normalized subject image is compared with the stored digital signature.

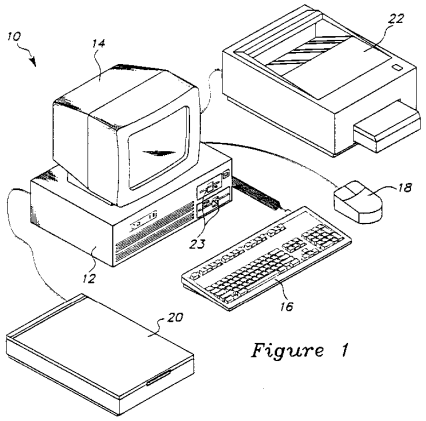


Figure 1

EP 0 581 317 A2

Technical Field

This invention relates to a method of and system for encoding a signature into a digital image and auditing a digital subject image to determine if it was derived from the encoded image.

Background of the Invention

Various images in traditional print or photographic media are commonly distributed to many users. Examples include the distribution of prints of paintings to the general public and photographs and film clips to and among the media. Owners may wish to audit usage of their images in print and electronic media, and so require a method to analyze print, film and digital images to determine if they were obtained directly from the owners or derived from their images. For example, the owner of an image may desire to limit access or use of the image. To monitor and enforce such a limitation, it would be beneficial to have a method of verifying that a subject image is copied or derived from the owner's image. The method of proof should be accurate and incapable of being circumvented. Further, the method should be able to detect unauthorized copies that have been resized, rotated, cropped, or otherwise altered slightly.

In the computer field, digital signatures have been applied to non-image digital data in order to identify the origin of the data. For various reasons these prior art digital signatures have not been applied to digital image data One reason is that these prior art digital signatures are lost if the data to which they are applied are modified. Digital images are often modified each time they are printed, scanned, copied, or photographed due to unintentional "noise" created by the mechanical reproduction equipment used. Further, it is often desired to resize, rotate, crop or otherwise intentionally modify the image. Accordingly, the existing digital signatures are unacceptable for use with digital images.

Summary of the Invention

The invention includes a method and system for embedding image signatures within visual images, applicable in the preferred embodiments described herein to digital representations as well as other media such as print or film. The signatures identify the source or ownership of images and distinguish between different copies of a single image. In preferred embodiments, these signatures persist through image transforms such as resizing and conversion to or from print or film and so provide a method to track subsequent use of digital images including derivative images in print or other form.

In a preferred embodiment described herein, a plurality of signature points are selected that are positioned within an original image having pixels with pixel values. The pixel values of the signature points are adjusted by an amount detectable by a digital scanner. The adjusted signature points form a digital signature that is stored for future identification of subject images derived from the image.

The preferred embodiment of the invention described herein embeds a signature within the original image by locating candidate points such as relative extrema in the pixel values. Signature points are selected from among the candidate points and a data bit is encoded at each signature point by adjusting the pixel value at and surrounding each point. Preferably, the signature is redundantly embedded in the image such that any of the redundant representations can be used to identify the signature. The signature is stored for later use in identifying a subject image.

According to a preferred embodiment, the identification of a subject image includes ensuring that the subject image is normalized, i.e., of the same size. rotation, and brightness level as the original image. If not already normalized, the subject image is normalized by aligning and adjusting the luminance values of subsets of the pixels in the subject image to match corresponding subsets in the original image. The normalized subject image is then subtracted from the original image and the result is compared with the stored digital signature. In an alternate embodiment, the normalized subject image is compared directly with the signed image.

Brief Description of the Drawings

Figure 1 is a diagram of a computer system used in a preferred embodiment of the present invention.

Figure 2 is a sample digital image upon which a preferred embodiment of the present invention is employed.

Figure 3 is a representation of a digital image in the form of an array of pixels with pixel values.

Figure 4 is graphical representation of pixel values showing relative minima and maxima pixel values.

DISH-Blue Spike-842
Exhibit 1004, Page 1317

Figure 5 is a digital subject image that is compared to the image of Figure 2 according to a preferred embodiment of the present invention.

Detailed Description of the Invention

The present invention includes a method and system for embedding a signature into an original image to create a signed image. A preferred embodiment includes selecting a large number of candidate points in the original image and selecting a number of signature points from among the candidate points. The signature points are altered slightly to form the signature. The signature points are stored for later use in auditing a subject image to determine whether the subject image is derived from the signed image.

The signatures are encoded in the visible domain of the image and so become part of the image and cannot be detected or removed without prior knowledge of the signature. A key point is that while the changes manifested by the signature are too slight to be visible to the human eye, they are easily and consistently recognizable by a common digital image scanner, after which the signature is extracted, interpreted and verified by a software algorithm.

In contrast to prior art signature methods used on non-image data, the signatures persist through significant image transformations that preserve the visible image but may completely change the digital data. The specific transforms allowed include resizing the image larger or smaller, rotating the image, uniformly adjusting color, brightness and/or contrast, and limited cropping. Significantly, the signatures persist through the process of printing the image to paper or film and rescanning it into digital form.

Shown in Figure 1 is a computer system 10 that is used to carry out an embodiment of the present invention. The computer system 10 includes a computer 12 having the usual complement of memory and logic circuits, a display monitor 14, a keyboard 16, and a mouse 18 or other pointing device. The computer system also includes a digital scanner 20 that is used to create a digital image representative of an original image such as a photograph or painting. Typically, delicate images, such as paintings, are converted to print or film before being scanned into digital form. In one embodiment a printer 22 is connected to the computer 12 to print digital images output from the processor. In addition, digital images can be output in a data format to a storage medium 23 such as a floppy disk for displaying later at a remote site. Any digital display device may be used, such a common computer printer, X-Y plotter, or a display screen.

An example of the output of the scanner 20 to the computer 12 is a digital image 24 shown in Figure 2. More accurately, the scanner outputs data representative of the digital image and the computer causes the digital image 24 to be displayed on the display monitor 14. As used herein "digital image" refers to the digital data representative of the digital image, the digital image displayed on the monitor or other display screen, and the digital image printed by the printer 22 or a remote printer.

The digital image 24 is depicted using numerous pixels 24 having various pixel values. In the gray-scale image 24 the pixel values are luminance values representing a brightness level varying from black to white. In a color image the pixels have color values and luminance values, both of which being pixel values. The color values can include the values of any components in a representation of the color by a vector. Figure 3 shows digital image 24A in the form of an array of pixels 26. Each pixel is associated with one or more pixel values, which in the example shown in Figure 3 are luminance values from 0 to 15.

The digital image 24 shown in Figure 2 includes thousands of pixels. The digital image 24A represented in Figure 3 includes 225 pixels. The invention preferably is used for images having pixels numbering in the millions. Therefore, the description herein is necessarily a simplistic discussion of the utility of the invention.

According to a preferred embodiment of the invention numerous candidate points are located within the original image. Signature points are selected from among the candidate points and are altered to form a signature. The signature is a pattern of any number of signature points. In a preferred embodiment, the signature is a binary number between 16 and 32 bits in length. The signature points may be anywhere within an image, but are preferably chosen to be as inconspicuous as possible. Preferably, the number of signature points is much greater than the number of bits in a signature. This allows the signature to be redundantly encoded in the image. Using a 16 to 32 bit signature, 50-200 signature points are preferable to obtain multiple signatures for the image.

A preferred embodiment of the invention locates candidate points by finding relative maxima and mituma, collectively referred to as extrema, in the image. The extrema represent local extremes of luminance or color. Figure 4 shows what is meant by relative extrema. Figure 4 is a graphical representation of the pixel values of a small portion of a digital image. The vertical axis of the graph shows pixel values while the horizontal axis shows pixel positions along a single line of the digital image. Small undulations in pixel values, indicated at 32. represent portions of the digital image where only small changes in luminance or color occur between pixels. A relative maximum 34 represents a pixel that has the highest pixel value for

DISH-Blue Spike-842
Exhibit 1004, Page 1318

a given area of the image. Similarly, a relative minimum 36 represents a pixel that has the lowest pixel value for a given area of the image.

Relative extrema are preferred signature points for two major reasons. First, they are easily located by simple, well known processing. Second, they allow signature points to be encoded very inconspicuously.

One of the simplest methods to determine relative extrema is to use a "Difference of Averages" technique. This technique employs predetermined neighborhoods around each pixel 26; a small neighborhood 28 and a large neighborhood 30, as shown in Figures 2 and 3. In the present example the neighborhoods are square for simplicity, but a preferred embodiment employs circular neighborhoods. The technique determines the difference between the average pixel value in the small neighborhood and the average pixel value of the large neighborhood. If the difference is large compared to the difference for surrounding pixels then the first pixel value is a relative maxima or minima.

Using the image of Figure 3 as an example, the Difference of Averages for the pixel 26A is determines as follows. The pixel values within the 3x3 pixel small neighborhood 28A add up to 69; dividing by 9 pixels gives an average of 7.67. The pixel values within the 5x5 pixel large neighborhood 30A add up to 219; dividing by 25 pixels gives an average of 8.76 and a Difference of Averages of -1.09. Similarly, the average in small neighborhood 28G is 10.0; the average in large neighborhood 30G is 9.8; the Difference of Averages for pixel 26G is therefore 0.2. Similar computations on pixels 26B-26F produce the following table:

	26A	26B	26C	26D	26E	26F	26G
Small Neighborhood	7.67	10.56	12.89	14.11	13.11	11.56	10.0
Large Neighborhood	8.76	10.56	12.0	12.52	12.52	11.36	9.8
Difference of Averages	-1.09	0.0	0.89	1.59	0.59	0.2	0.2

Based on pixels 26A-26G. there may be a relative maximum at pixel 26D, whose Difference of Averages of 1.59 is greater than the Difference of Averages for the other examined pixels in the row. To determine whether pixel 26D is a relative maximum rather than merely a small undulation, its Difference of Averages must be compared with the Difference of Averages for the pixels surrounding it in a larger area.

Preferably, extrema within 10% of the image size of any side are not used as signature points. This protects against loss of signature points caused by the practice of cropping the border area of an image. It is also preferable that relative extrema that are randomly and widely spaced are used rather than those that appear in regular patterns.

Using the Difference of Averages technique or other known techniques, a large number of extrema are obtained, the number depending on the pixel density and contrast of the image. Of the total number of extrema found, a preferred embodiment chooses 50 to 200 signature points. This may be done manually by a user choosing with the keyboard 16, mouse 18, or other pointing device each signature point from among the extrema displayed on the display monitor 14. The extrema may be displayed as a digital image with each point chosen by using the mouse or other pointing device to point to a pixel or they may be displayed as a list of coordinates which are chosen by keyboard, mouse, or other pointing device. Alternatively, the computer 12 can be programmed to choose signature points randomly or according to a preprogrammed pattern.

One bit of binary data is encoded in each signature point in the image by adjusting the pixel values at and surrounding the point. The image is modified by making a small, preferably 2%-10% positive or negative adjustment in the pixel value at the exact signature point, to represent a binary zero or one. The pixels surrounding each signature point, in approximately a 5 x 5 to 10 x 10 grid, are preferably adjusted proportionally to ensure a continuous transition to the new value at the signature point. A number of bits are encoded in the signature points to form a pattern which is the signature for the image.

In a preferred embodiment, the signature is a pattern of all of the signature points. When auditing a subject image, if a statistically significant number of potential signature points in the subject image match corresponding signature points in the signed image, then the subject image is deemed to be derived from the signed image. A statistically significant number is somewhat less than 100%, but enough to be reasonably confident that the subject image was derived from the signed image.

In an alternate embodiment, the signature is encoded using a redundant pattern that distributes it among the signature points in a manner that can be reliably retrieved using only a subset of the points. One embodiment simply encodes a predetermined number of exact duplicates of the signature. Other redundant representation methods, such as an error-correcting code, may also be used.

In order to allow future auditing of images to determine whether they match the signed image, the signature is stored in a database in which it is associated with the original image. The signature can be

DISH-Blue Spike-842
Exhibit 1004, Page 1319

stored by associating the bit value of each signature point together with x-y coordinates of the signature point. The signature may be stored separately or as part of the signed image. The signed image is then distributed in digital form.

As discussed above, the signed image may be transformed and manipulated to form a derived image. The derived image is derived from the signed image by various transformations, such as resizing, rotating, adjusting color, brightness and/or contrast, cropping and converting to print or film. The derivation may take place in multiple steps or processes or may simply be the copying of the signed image directly.

It is assumed that derivations of these images that an owner wishes to track include only applications which substantially preserve the resolution and general quality of the image. While a size reduction by 90%, a significant color alteration or distinct-pixel-value reduction may destroy the signature, they also reduce the images significance and value such that no auditing is desired.

In order to audit a subject image according to a preferred embodiment, a user identifies the original image of which the subject image is suspected of being a duplicate. For a print or film image, the subject image is scanned to create a digital image file. For a digital image, no scanning is necessary. The subject digital image is normalized using techniques as described below to the same size, and same overall brightness, contrast and color profile as the unmodified original image. The subject image is analyzed by the method described below to extract the signature, if present, and compare it to any signatures stored for that image.

The normalization process involves a sequence of steps to undo transformations previously made to the subject image, to return it as close as possible to the resolution and appearance of the original image. It is assumed that the subject image has been manipulated and transformed as described above. To align the subject image with the original image, a preferred embodiment chooses three or more points from the subject image which correspond to points in the original image. The three or more points of the subject image are aligned with the corresponding points in the original image. The points of the subject image not selected are rotated and resized as necessary to accommodate the alignment of the points selected.

For example, Figure 5 shows a digital subject image 38 that is smaller than the original image 24 shown in Figure 2. To resize the subject image, a user points to three points such as the mouth 40B, ear 42B and eye 44B of the subject image using the mouse 18 or other pointer. Since it is usually difficult to accurately point to a single pixel, the computer selects the nearest extrema to the pixel pointed to by the user. The user points to the mouth 40A, ear 42A, and eye 44A of the original image. The computer 12 resizes and rotates the subject image as necessary to ensure that points 40B, 42B, and 44B are positioned with respect to each other in the same way that points 40A, 42A, and 44A are positioned with respect to each other in the original image. The remaining pixels are repositioned in proportion to the repositioning of points 40B, 42B and 44B. By aligning three points the entire subject image is aligned with the original image without having to align each pixel independently.

After the subject image is aligned, the next step is to normalize the brightness, contrast and/or color of the subject image. Normalizing involves adjusting pixel values of the subject image to match the value-distribution profile of the original image. This is accomplished by a technique analogous to that used to align the subject image. A subset of the pixels in the subject image are adjusted to equal corresponding pixels in the original image. The pixels not in the subset are adjusted in proportion to the adjustments made to the pixels in the subset. The pixels of the subject image corresponding to the signature points should not be among the pixels in the subset. Otherwise any signature points in the subject image will be hidden from detection when they are adjusted to equal corresponding pixels in the original image.

In a preferred embodiment, the subset includes the brightest and darkest pixels of the subject image. These pixels are adjusted to have luminance values equal to the luminance values of corresponding pixels in the original image. To ensure that any signature points can be detected, no signature points should be selected during the signature embedding process described above that are among the brightest and darkest pixels of the original image. For example, one could use pixels among the brightest and darkest 3% for the adjusting subset, after selecting signature points among less than the brightest and darkest 5% to ensure that there is no overlap.

When the subject image is fully normalized, it is preferably compared to the original image. One way to compare images is to subtract one image from the other. The result of the subtraction is a digital image that includes any signature points that were present in the subject image. These signature points, if any, are compared to the stored signature points for the signed image. If the signature points do not match, then the subject image is not an image derived from the signed image, unless the subject image was changed substantially from the signed image.

In an alternative embodiment, the normalized subject image is compared directly with the signed image instead of subtracting the subject image from the original image. This comparison involves subtracting the

DISH-Blue Spike-842
Exhibit 1004, Page 1320

subject image from the signed image. If there is little or no image resulting from the subtraction then the subject image equals to the signed image, and therefore has been derived from the signed image.

In another alternate embodiment instead of normalizing the entire subject image, only a section of the subject image surrounding each potential signature point is normalized to be of the same general resolution and appearance as a corresponding section of the original image. This is accomplished by selecting each potential signature point of the subject image and selecting sections surrounding each potential signature point. The normalization of each selected section proceeds according to methods similar to those disclosed above for normalizing the entire subject image.

Normalizing each selected section individually allows each potential signature point of the subject image to be compared directly with a corresponding signature point of the signed image. Preferably, an average is computed for each potential signature point by averaging the pixel value of the potential signature point with the pixel values of a plurality of pixels surrounding the potential signature point. The average computed for each signature is compared directly with a corresponding signature point of the signed image.

While the methods of normalizing and extracting a signature from a subject image as described above are directed to luminance values, similar methods may be used for color values. Instead of or in addition to normalizing by altering luminance values, the color values of the subject image can also be adjusted to equal corresponding color values in an original color image. However, it is not necessary to adjust color values in order to encode a signature in or extract a signature from a color image. Color images use pixels having pixel values that include luminance values and color values. A digital signature can be encoded in any pixel values regardless of whether the pixel values are luminance values, color values, or any other type of pixel values. Luminance values are preferred because alterations may be made more easily to luminance values without the alterations being visible to the human eye.

From the foregoing it will be appreciated that, although specific embodiments of the invention have been described herein for purposes of illustration, various modifications may be made without deviating from the spirit and scope of the invention. Accordingly, the invention is not limited except as by the appended claims.

Claims

1. A method of image signature processing of an original image having pixels with luminance values, comprising:
   locating a plurality of candidate points from among the pixels of the original image;
   selecting a first plurality of signature points from among the candidate points;
   adjusting the pixel values of the signature points to form a signed image, the adjusted signature point pixel values forming a signature for the signed image; and
   storing the signature for future identification.

2. The method according to claim 1 wherein the candidate points are located by locating relative extrema in the original image and wherein the selecting step includes selecting the signature points from among the extrema.

3. The method according to claim 2 wherein the extrema are relative minima or maxima of luminance values of the pixels of the original image.

4. The method according to claim 1, further comprising adjusting a plurality of pixel values surrounding the signature points to provide smooth transitions to the adjusted pixel values at the signature points.

5. The method according to claim 1, further comprising:
   selecting a second plurality of signature points from among the candidate points; and
   adjusting the pixel values of the second plurality of signature points to form a redundant signature for the signed image.

6. A method of image signature processing of an original image having pixels with pixel values, comprising:
   selecting a first plurality of signature points from among the pixels of the original image;
   adjusting the pixel values of the signature points, the adjusted signature point pixel values forming a signature for the image; and

DISH-Blue Spike-842
Exhibit 1004, Page 1321

storing the signature for future identification.

7. The method according to claim 6, further comprising locating relative extrema in the original image and wherein the selecting step includes selecting the signature points from among the extrema.

8. The method according to claim 7 wherein the extrema are relative minima or maxima of luminance values of the pixels of the original image.

9. The method according to claim 6 further comprising:
selecting a second plurality of signature points from among the candidate points; and
adjusting the pixel values of the second plurality of signature points to form a redundant signature for the signed image.

10. The method according to claim 6 wherein the digital image has a border surrounding the image and the pixel values adjusted are selected so as not to be within a predetermined distance from the border.

11. The method according to claim 6, further comprising adjusting a plurality of pixel values surrounding the signature points to provide smooth transitions to the adjusted pixel values at the signature points.

12. The method according to claim 6 wherein the pixel values adjusted are luminance values.

13. The method according to claim 6 wherein the pixel values adjusted are color values.

14. The method according to claim 6, further comprising analyzing whether a digital subject image constitutes or is derived from a signed image having pixel values that were adjusted to form a signature according to claim 6.

15. The method according to claim 14 wherein the analyzing step includes normalizing the subject image.

16. The method according to claim 15 wherein the normalizing step includes aligning the subject image with the signed image or the original image.

17. The method according to claim 16 wherein the aligning step includes selecting three or more pixels in the subject image and aligning the three or more peels with corresponding pixels in the original or the signed image.

18. The method according to claim 15 wherein the pixel values of the subject image and the original image include luminance values and the normalizing step includes adjusting the luminance values of a subset of the pixels in the subject image to equal the luminance values of a corresponding subset of pixels in the original image.

19. The method according to claim 14 wherein the analyzing step includes subtracting the subject image from the original image to obtain a resulting image and comparing the resulting image with the stored signature.

20. The method according to claim 14 wherein the analyzing step includes comparing the subject image with the signed image.

21. The method according to claim 14 wherein the analyzing step includes selecting a potential signature point in the subject image corresponding to a signature point of the signed image and comparing the pixel value of the selected point to the pixel value of the corresponding signature point of the signed image.

22. The method according to claim 14 wherein the analyzing step includes selecting a potential signature point in the subject image corresponding to a signature point of the signed image, computing an average of pixel values of the potential signature point and a plurality of pixels surrounding the potential signature point, and comparing the average to the pixel value of the corresponding signature point of the signed image.

DISH-Blue Spike-842
Exhibit 1004, Page 1322

23. A method of determining whether a subject image having pixels with pixel values constitutes or is derived from a signed image having pixels with pixel values that have been adjusted to collectively form a signature, comprising:

ensuring that the subject image is normalized with respect to an original image or the signal image;

comparing the signature of the signed image with potential signature points of the subject image corresponding to the pixels of the signature.

24. The method according to claim 23 wherein the ensuring step includes normalizing the subject image with respect to the original image or the signed image.

25. The method according to claim 24 wherein the normalizing step includes aligning the subject image with the signal image or the original image.

26. The method according to claim 25 wherein the aligning step includes selecting three or more pixels in the subject image and aligning the three or more pixels with a like number of pixels in the original or signed image.

27. The method according to claim 24 wherein the pixel values of the subject image and the original image include luminance values and the normalizing step includes adjusting the luminance values of a subset of the pixels in the subject image to equal the luminance value of a corresponding subset of pixels in the original image.

28. The method according to claim 23 wherein the comparing step includes subtracting the subject image from the original image to obtain a resulting image and comparing the resulting image with the stored digital signature.

29. The method according to claim 23 wherein the comparing step includes comparing the subject image with the signed image.

30. The method according to claim 23 wherein the comparing step includes selecting the potential signature points corresponding to pixels of the signature, computing an average of the pixel values of each potential signature point and a plurality of pixels surrounding each signature point, and comparing each average to the pixel value of the corresponding signature point of the signed image.

31. A system for image signature processing of an original image having pixels with pixel values, comprising:

a display device for displaying digital images to a user;

selection means for selecting a plurality of signature points from among the pixels of the original image;

a computing device in communication with the display device and the selection means, the computing device adjusting the pixel values of the signature points to form a signed image, the adjusted signature point pixel values forming a signature associated with the signed image: and

memory in communication with the computing device, the memory receiving the signature from the computing device and storing the signature for future identification.

32. The system according to claim 31 wherein the computing device includes location means for locating candidate points from among the pixels in the original image and the selecting means selects signature points from among the candidate points.

33. The system according to claim 32 wherein the selection means includes a pointer operatively connected to the display device and the computing device such that a user can select signature points from among the candidate points displayed on the display device and the computing device alters the signature points selected to form a signature associated with the signed image.

34. The system according to claim 32 wherein the location means includes means for locating pixel value extrema in the original image, the extrema being the candidate points.

DISH-Blue Spike-842
Exhibit 1004, Page 1323

35. The system according to claim 31 wherein the computing device includes means for identifying a subject image derived from the signed image.

36. The system according to claim 35, further comprising normalizing means for normalizing the subject image with the original image or the signed image.

37. The system according to claim 36 wherein the normalizing means includes a pointer operatively connected to the display device and the computing device such that a user can select alignment points from among the pixels of the subject image displayed on the display device and the computing device receives the alignment points selected and aligns the subject image with the original image or the signed image in response thereto.

38. The system according to claim 36 wherein the computing device includes comparing means for comparing the normalized subject image with the original image or the signed image.

39. The system according to claim 36 wherein the computing device includes:

subject selection means for selecting a potential signature point on the subject image corresponding to a signature point of the signed image;

averaging means for computing an average of the pixel values of the potential signature point and a plurality of pixels surrounding the potential signature point; and

comparing means for comparing the average to a pixel value of the corresponding signature point of the signed image.

DISH-Blue Spike-842
Exhibit 1004, Page 1324

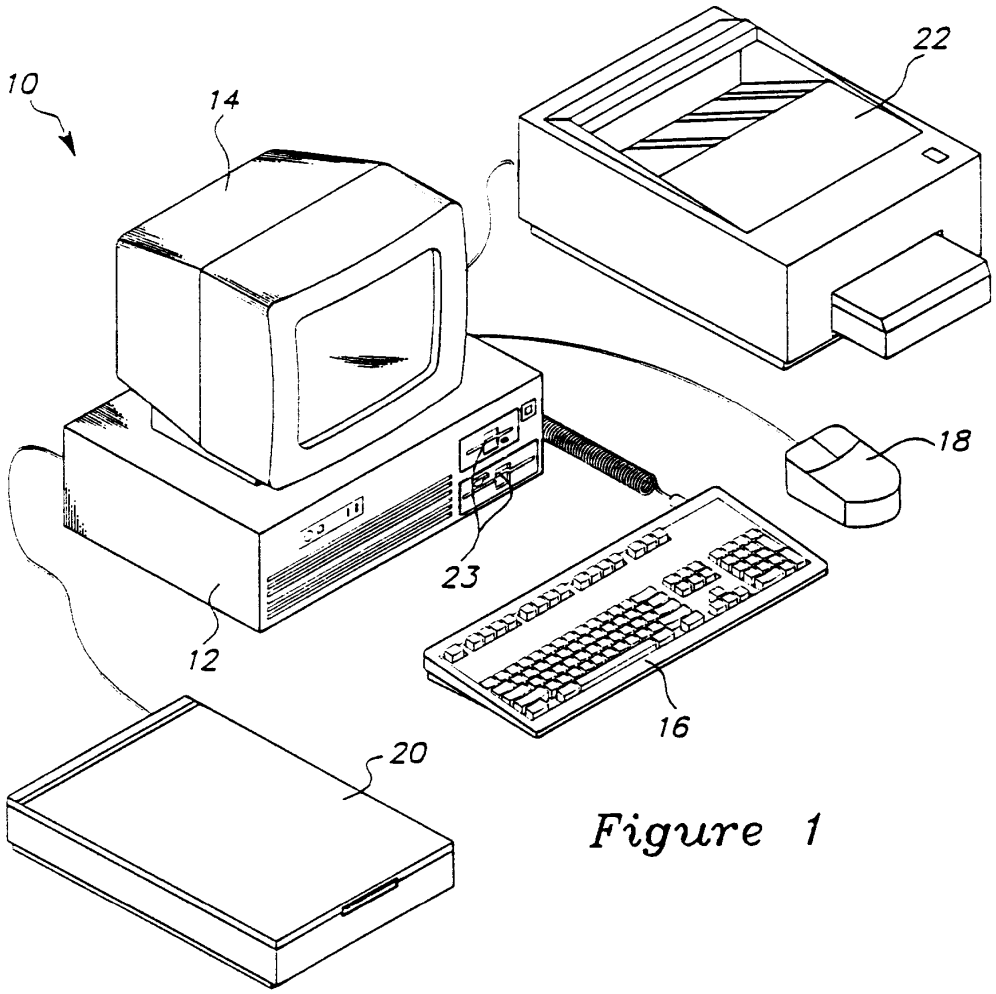


Figure 1

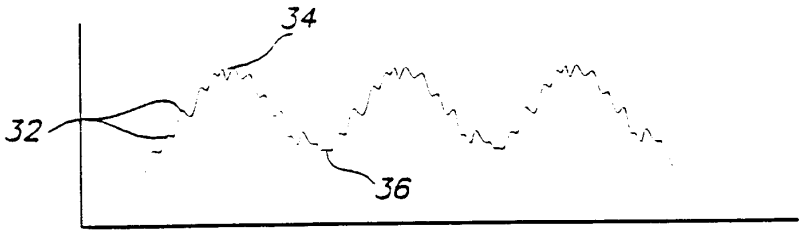


Figure 4

DISH-Blue Spike-842
Exhibit 1004, Page 1325

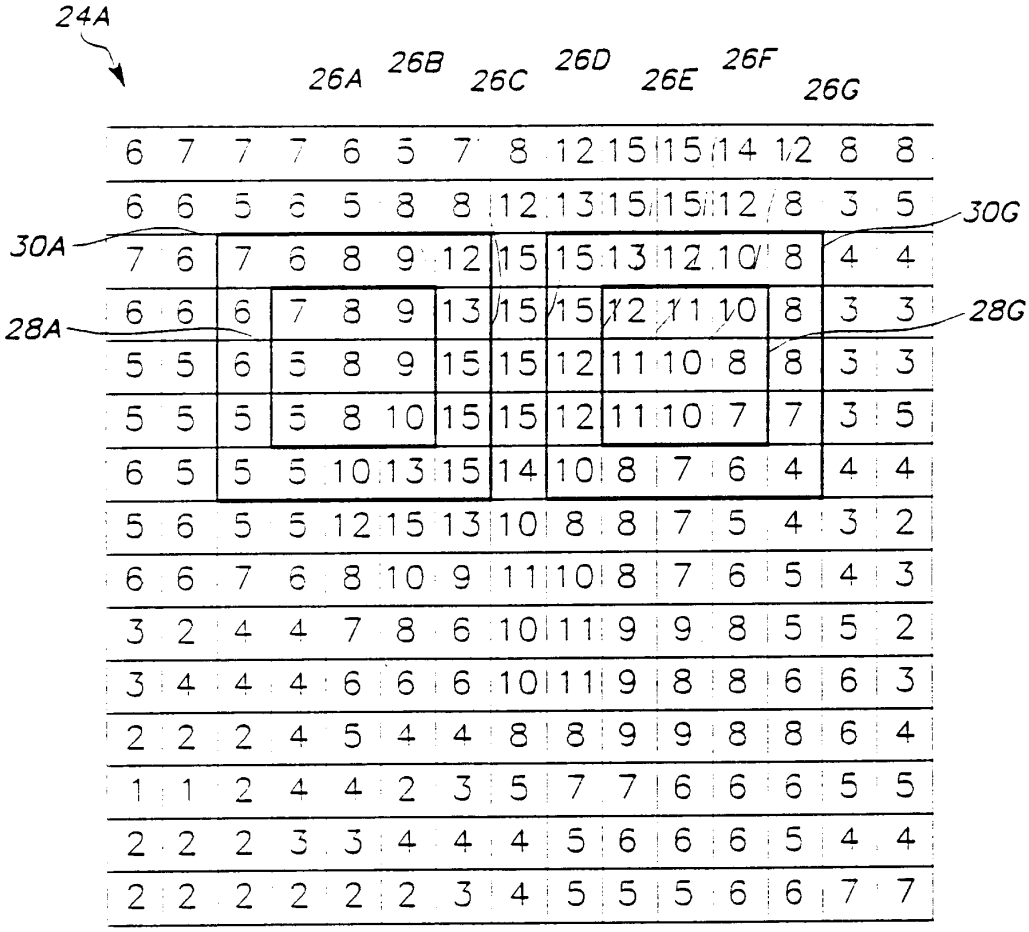


Figure 3

DISH-Blue Spike-842
Exhibit 1004, Page 1326

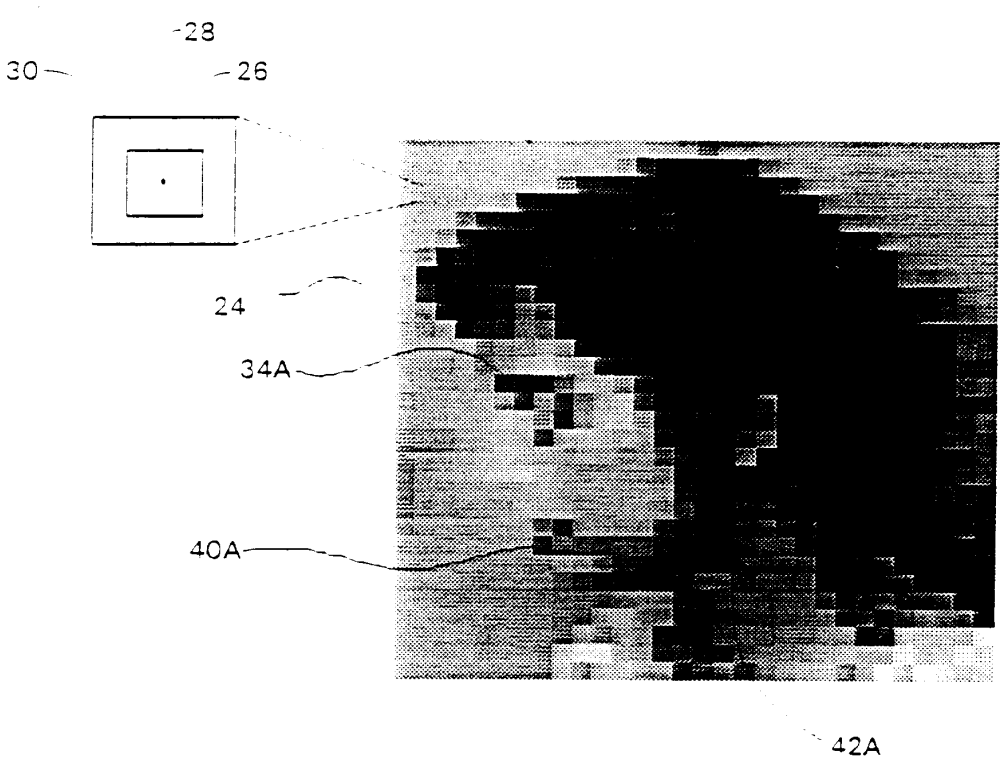


Figure 2

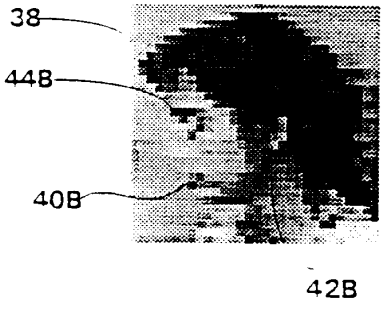


Figure 5

DISH-Blue Spike-842
Exhibit 1004, Page 1327

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 581 317 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
01.05.1996 Bulletin 1996/18

(43) Date of publication A2:
02.02.1994 Bulletin 1994/05

(21) Application number: **93112290.7**

(22) Date of filing: **30.07.1993**

(51) Int. Cl.[6]: **G07D 7/00**, G07F 7/12

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **31.07.1992 US 923841**

(71) Applicant: **CORBIS CORPORATION**
Bellevue, Washington 98007-6537 (US)

(72) Inventors:
- **Powell, Robert D.**
  Issaquah, Washington 98027 (US)
- **Nitzberg, Mark J.**
  D-50677 Köln (DE)

(74) Representative: **Grünecker, Kinkeldey,**
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
D-80538 München (DE)

(54) Method and system for digital image signatures

(57) A method and system for embedding signatures within visual images in both digital representation and print or film. A signature is inseparably embedded within the visible image, the signature persisting through image transforms that include resizing as well as conversion to print or film and back to digital form. Signature points are selected from among the pixels of an original image. The pixel values of the signature points and surrounding pixels are adjusted by an amount detectable by a digital scanner. The adjusted signature points form a digital signature which is stored for future identification of subject images derived from the image. In one embodiment, a signature is embedded within an image by locating relative extrema in the continuous space of pixel values and selecting the signature points from among the extrema. Preferably, the signature is redundantly embedded in the image such that any of the redundant representations can be used to identify the signature. Identification of a subject image includes ensuring that the subject image is normalized with respect to the original image or the signed image. Preferably, the normalized subject image is compared with the stored digital signature.

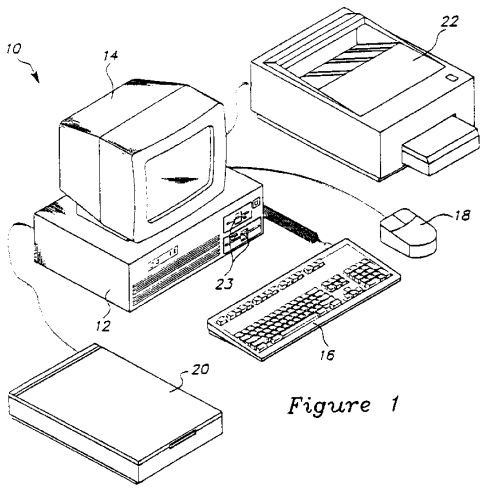


Figure 1

EP 0 581 317 A3

DISH-Blue Spike-842
Exhibit 1004, Page 1328

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 93 11 2290

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
X	1979 CARNAHAN CONFERENCE ON CRIME COUNTERMEASURES, 16 - 18 May 1979 UNIVERSITY OF KENTUCKY, LEXINGTON, KENTUCKY USA, pages 101-109, SZEPANSKI, WOLFRAM 'A Signal Theoretic method for creating Forgery-proof Documents for Automatic Verification.' * page 103 - page 104; figures 3.4 , 4 * ---	1-39	G07D7/00 G07F7/12
X	DE-A-29 43 436 (SZEPANSKI WOLFRAM DR ING) 7 May 1981 * page 8, paragraph 3; figure 3 * ---	1-39	
A	US-A-3 914 877 (HINES MARION E) 28 October 1975 * claim 1; figure 2 * ---	1-39	
A	US-A-4 488 245 (DALKE GEORGE W ET AL) 11 December 1984 * claim 1; figure 6 * ---	1-39	TECHNICAL FIELDS SEARCHED (Int.Cl.5)
A	US-A-4 310 180 (MOWRY JR WILLIAM H ET AL) 12 January 1982 * claim 1; figure 1 * -----	1-39	G07D G07F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	7 March 1996	Kirsten, K

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

DISH-Blue Spike-842
Exhibit 1004, Page 1329

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00	A1	(11) International Publication Number: WO 97/26733
		(43) International Publication Date: 24 July 1997 (24.07.97)

(21) International Application Number: PCT/US97/00652

(22) International Filing Date: 17 January 1997 (17.01.97)

(30) Priority Data:
08/587,944 17 January 1996 (17.01.96) US

(71) Applicant: THE DICE COMPANY [US/US]; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US).

(72) Inventors: COOPERMAN, Marc; 2929 Ramona, Palo Alto, CA 94306 (US). MOSKOWITZ, Scott, A.; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US).

(74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).

(81) Designated States: AL, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GE, HU, IL, IS, JP, KP, KR, LC, LK, LR, LT, LV, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD FOR AN ENCRYPTED DIGITAL WATERMARK

(57) Abstract

A method for the human-assisted generation and application of pseudo-random keys for the purpose of encoding and decoding digital watermarks to and from a digitized data stream. A pseudo-random key and key application "envelope" are generated and stored using guideline parameters input by a human engineer interacting with a graphical representation of the digitized data stream. Key "envelope" information is permanently associated with the pseudo-random binary string comprising the key. Key and "envelope" information are then applied in a digital watermark system to the encoding and decoding of digital watermarks.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic			SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

METHOD FOR AN ENCRYPTED DIGITAL WATERMARK

FIELD OF INVENTION

With the advent of computer networks and digital multimedia, protection of intellectual property has become a prime concern for creators and publishers of digitized copies of copyrightable works, such as musical recordings, movies, and video games. One method of protecting copyrights in the digital domain is to use "digital watermarks". Digital watermarks can be used to mark each individual copy of a digitized work with information identifying the title, copyright holder, and even the licensed owner of a particular copy. The watermarks can also serve to allow for secured metering and support of other distribution systems of given media content and relevant information associated with them, including addresses, protocols, billing, pricing or distribution path parameters, among the many things that could constitute a "watermark." For further discussion of systems that are oriented around content-based addresses and directories, see U.S. Patent No. 5,428,606 Moskowitz. When marked with licensing and ownership information, responsibility is created for individual copies where before there was none. More information on digital watermarks is set forth in "Steganographic Method and Device" - The DICE Company, U.S. application Serial No. 08/489,172, the disclosure of which is hereby incorporated by reference. Also, "Technology: Digital

Commerce", Denise Caruso, New York Times, August 7, 1995 "Copyrighting in the Information Age", Harley Ungar, ONLINE MARKETPLACE, September 1995, Jupiter Communications further describe digital watermarks.

Additional information on other methods for hiding information signals in content signals, is disclosed in U.S. Patent No. 5,319,735 - Preuss et al. and U.S. Patent No. 5,379,345 - Greenberg.

Digital watermarks can be encoded with random or pseudo random keys, which act as secret maps for locating the watermarks. These keys make it impossible for a party without the key to find the watermark - in addition, the encoding method can be enhanced to force a party to cause damage to a watermarked data stream when trying to erase a random-key watermark.

It is desirable to be able to specify limitations on the application of such random or pseudo random keys in encoding a watermark to minimize artifacts in the content signal while maximizing encoding level. This preserves the quality of the content, while maximizing the security of the watermark. Security is maximized because erasing a watermark without a key results in the greatest amount of perceptible artifacts in the digital content. It is also desirable to separate the functionality of the decoder side of the process to provide fuller recognition and substantiation of the protection of goods that are essentially digitized bits, while ensuring the security of the encoder and the encoded content. It is also desirable that the separate decoder be incorporated into an agent, virus, search engine, or other autonomously operating or search function software. This would make it possible for parties possessing a decoder to verify the presence of valid watermarks in a data stream, without accessing the contents of the watermark. It would also be possible to scan or search archives for files containing watermarked

content, and to verify the validity of the presence of such files in an archive, by means of the information contained in the watermarks. This scenario has particular application in screening large archives of files kept by on-line services and internet archives. It is further a goal of such processes to bring as much control of copyrights and content, including its pricing, billing, and distribution, to the parties that are responsible for creating and administering that content. It is another goal of the invention to provide a method for encoding multiple watermarks into a digital work, where each watermark can be accessed by use of a separate key. This ability can be used to provide access to watermark information to various parties with different levels of access. It is another goal of the invention to provide a mechanism which allows for accommodation of alternative methods encoding and decoding watermarks from within the same software or hardware infrastructure. This ability can be used to provide upgrades to the watermark system, without breaking support for decoding watermarks created by previous versions of the system. It is another goal of the invention to provide a mechanism for the certification and authentication, via a trusted third party, and public forums, of the information placed in a digital watermark. This provides additional corroboration of the information contained in a decoded digital watermark for the purpose of its use in prosecution of copyright infringement cases. It also has use in any situation in which a trusted third party verification is useful. It is another goal of this invention to provide an additional method for the synchronization of watermark decoding software to an embedded watermark signal that is more robust than previously disclosed methods.

SUMMARY OF THE INVENTION

The invention described herein is a human-assisted random key generation and application system for use in a digital watermark system. The invention allows an engineer or other individual, with specialized knowledge regarding processing and perception of a particular content type, such as digital audio or video, to observe a graphical representation of a subject digital recording or data stream, in conjunction with its presentation (listening or viewing) and to provide input to the key generation system that establishes a key generation "envelope", which determines how the key is used to apply a digital watermark to the digital data stream. The envelope limits the parameters of either or both the key generation system and the watermark application system, providing a rough guide within which a random or pseudo random key may be automatically generated and applied. This can provide a good fit to the content, such that the key may be used to encode a digital watermark into the content in such a manner as to minimize or limit the perceptible artifacts produced in the watermarked copy, while maximizing the signal encoding level. The invention further provides for variations in creating, retrieving, monitoring and manipulating watermarks to create better and more flexible approaches to working with copyrights in the digital domain.

Such a system is described herein and provides the user with a graphical representation of the content signal over time. In addition, it provides a way for the user to input constraints on the application of the digital watermark key, and provides a way to store this information with a random or pseudo random key sequence which is also generated to apply to a content signal. Such a system would also be more readily adaptable by current techniques to master content with personal

computers and authoring/editing software. It would also enable individuals to monitor their copyrights with decoders to authenticate individual purchases, filter possible problematic and unpaid copyrightable materials in archives, and provide for a more generally distributed approach to the monitoring and protection of copyrights in the digital domain.

DETAILED DESCRIPTION

Digital watermarks are created by encoding an information signal into a larger content signal. The information stream is integral with the content stream, creating a composite stream. The effectiveness and value of such watermarks are highest when the informational signal is difficult to remove, in the absence of the key, without causing perceptible artifacts in the content signal. The watermarked content signal itself should contain minimal or no perceptible artifacts of the information signal. To make a watermark virtually impossible to find without permissive use of the key, its encoding is dependent upon a randomly generated sequence of binary 1s and 0s, which act as the authorization key. Whoever possesses this key can access the watermark. In effect, the key is a map describing where in the content signal the information signal is hidden. This represents an improvement over existing efforts to protect copyrightable material through hardware-based solutions always existing outside the actual content.

"Antipiracy" devices are used in present applications like VCRs, cable television boxes, and digital audio tape (DAT) recorders, but are quite often disabled by those who have some knowledge of the location of the device or choose not to purchase hardware with these "additional security features." With digital watermarks, the "protection," or more accurately, the

DISH-Blue Spike-842
Exhibit 1004, Page 1336

deterrent, is hidden entirely in the signal, rather than a particular chip in the hardware.

Given a completely random key, which is uniformly applied over a content signal, resulting artifacts in the watermarked content signal are unpredictable, and depend on the interaction of the key and the content signal itself. One way to ensure minimization of artifacts is to use a low information signal level. However, this makes the watermark easier to erase, without causing audible artifacts in the content signal. This is a weakness. If the information signal level is boosted, there is the risk of generating audible artifacts.

The nature of the content signal generally varies significantly over time. During some segments, the signal may lend itself to masking artifacts that would otherwise be caused by high level encoding. At other times, any encoding is likely to cause artifacts. In addition, it might be worthwhile to encode low signal level information in a particular frequency range which corresponds to important frequency components of the content signal in a given segment of the content signal. This would make it difficult to perform bandpass filtering on the content signal to remove watermarks.

Given the benefits of such modifications to the application of the random key sequence in encoding a digital watermark, what is needed is a system which allows human-assisted key generation and application for digital watermarks. The term "human-assisted key generation" is used because in practice, the information describing how the random or pseudo random sequence key is to be applied must be stored with the key sequence. It is, in essence, part of the key itself, since the random or pseudo random sequence alone is not enough to encode, or possibly decode the watermark.

DISH-Blue Spike-842
Exhibit 1004, Page 1337

Encoding of digital watermarks into a content signal can be done in the time domain, by modifying content samples on a sample by sample basis, or in the frequency domain, by first performing a mathematical transform on a series of content samples in order to convert them into frequency domain information, subsequently modifying the frequency domain information with the watermark, and reverse transforming it back into time-based samples. The conversion between time and frequency domains can be accomplished by means of any of a class of mathematical transforms, known in general as "Fourier Transforms." There are various algorithmic implementations and optimizations in computer source code to enable computers to perform such transform calculations. The frequency domain method can be used to perform "spread spectrum" encoding implementations. Spread spectrum techniques are described in the prior art patents disclosed. Some of the shortcomings evident in these techniques relate to the fixed parameters for signal insertion in a sub audible level of the frequency-based domain, e.g., U.S. Patent No. 5,319,735 Preuss et al. A straightforward randomization attack may be engaged to remove the signal by simply over-encoding random information continuously in all sub-bands of the spread spectrum signal band, which is fixed and well defined. Since the Preuss patent relies on masking effects to render the watermark signal, which is encoded at -15 dB relative to the carrier signal, inaudible, such a randomization attack will not result in audible artifacts in the carrier signal, or degradation of the content. More worrisome, the signal is not the original but a composite of an actual frequency in a known domain combined with another signal to create a "facsimile" or approximation, said to be imperceptible to a human observer, of the original copy. What results is the forced maintenance of one

original to compare against subsequent "suspect" copies for examination. Human-assisted watermarking would provide an improvement over the art by providing flexibility as to where information signals would be inserted into content while giving the content creator the ability to check all subsequent copies without the requirement of a single original or master copy for comparison. Thus the present invention provides for a system where all necessary information is contained within the watermark itself.

Among other improvements over the art, generation of keys and encoding with human assistance would allow for a better match of a given informational signal (be it an ISRC code, an audio or voice file, serial number, or other "file" format) to the underlying content given differences in the make-up of the multitudes of forms of content (classical music, CD-ROM versions of the popular game DOOM, personal HTML Web pages, virtual reality simulations, etc.) and the ultimate wishes of the content creator or his agents. This translates into a better ability to maximize the watermark signal level, so as to force maximal damage to the content signal when there is an attempt to erase a watermark without the key. For instance, an engineer could select only the sections of a digital audio recording where there were high levels of distortion present in the original recording, while omitting those sections with relatively "pure" components from the watermark process. This then allows the engineer to encode the watermark at a relatively higher signal level in the selected sections without causing audible artifacts in the signal, since the changes to the signal caused by the watermark encoding will be masked by the distortion. A party wanting to erase the watermark has no idea, however, where or at what level a watermark is encoded, and so must choose to "erase" at the maximum level across the

DISH-Blue Spike-842
Exhibit 1004, Page 1339

entire data stream, to be sure they have obliterated every instance of a watermark.

In the present invention, the input provided by the engineer is directly and immediately reflected in a graphical representation of content of that input, in a manner such that it is overlaid on a representation of the recorded signal. The key generation "envelope" described by the engineer can be dictated to vary dynamically over time, as the engineer chooses. The graphical representation of the content is typically rendered on a two dimensional computer screen, with a segment of the signal over time proceeding horizontally across the screen. The vertical axis is used to distinguish various frequency bands in the signal, while the cells described by the intersection of vertical and horizontal unit lines can signify relative amplitude values by either a brightness or a color value on the display.

Another possible configuration and operation of the system would use a display mapping time on the horizontal axis versus signal amplitude on the vertical axis. This is particularly useful for digital audio signals. In this case, an engineer could indicate certain time segments, perhaps those containing a highly distorted signal, to be used for watermark encoding, while other segments, which contain relatively pure signals, concentrated in a few bandwidths, may be exempt from watermarking. The engineer using a time vs. amplitude assisted key generation configuration would generally not input frequency limiting information.

In practice, the system might be used by an engineer or other user as follows:

The engineer loads a file containing the digitized content stream to be watermarked onto a computer. The engineer runs the key generation application and opens the file to be watermarked. The application opens a

DISH-Blue Spike-842
Exhibit 1004, Page 1340

window which contains a graphical representation of the digitized samples. Typically, for digital audio, the engineer would see a rectangular area with time on the horizontal axis, frequency bands on the vertical axis, and varying color or brightness signifying signal power at a particular time and frequency band. Each vertical slice of the rectangle represents the frequency components, and their respective amplitude, at a particular instant ("small increment") of time. Typically, the display also provides means for scrolling from one end of the stream to the other if it is too long to fit on the screen, and for zooming in or out magnification in time or frequency. For the engineer, this rectangular area acts as a canvas. Using a mouse and/or keyboard, the engineer can scroll through the signal slowly marking out time segments or frequency band minima and maxima which dictate where, at what frequencies, and at what encoding signal level a watermark signal is to be encoded into the content, given a random or pseudo random key sequence. The engineer may limit these marks to all, none or any of the types of information discussed above. When the engineer is finished annotating the content signal, he or she selects a key generation function. At this point, all the annotated information is saved in a record and a random or pseudo random key sequence is generated associated with other information. At some later point, this combined key record can be used to encode and/or decode a watermark into this signal, or additional instances of it.

A suitable pseudo-random binary sequence for use as a key may be generated by: collecting some random timing information based on user keystrokes input to a keyboard device attached to the computer, performing a secure one way hash operation on this random timing data, using the results of the hash to seed a block cipher algorithm

DISH-Blue Spike-842
Exhibit 1004, Page 1341

loop, and then cycling the block cipher and collecting a sequence of 1s and 0s from the cipher's output, until a pseudo-random sequence of 1s and 0s of desired length is obtained.

The key and its application information can then be saved together in a single database record within a database established for the purpose of archiving such information, and sorting and accessing it by particular criteria. This database should be encrypted with a passphrase to prevent the theft of its contents from the storage medium.

Another improvement in the invention is support for alternate encoding algorithm support. This can be accomplished for any function which relates to the encoding of the digital watermark by associating with the pseudo-random string of 1s and 0s comprising the pseudo-random key, a list of references to the appropriate functions for accomplishing the encoding. For a given function, these references can indicate a particular version of the function to use, or an entirely new one. The references can take the form of integer indexes which reference chunks of computer code, of alphanumeric strings which name such "code resources," or the memory address of the entry point of a piece of code already resident in computer memory. Such references are not, however, limited to the above examples. In the implementation of software, based on this and previous filings, each key contains associated references to functions identified as CODEC - basic encode/decode algorithm which encodes and decodes bits of information directly to and from the content signal, MAP - a function which relates the bits of the key to the content stream, FILTER - a function which describes how to pre-filter the content signal, prior to encoding or decoding, CIPHER - a function which provides encryption and decryption services for information

DISH-Blue Spike-842
Exhibit 1004, Page 1342

contained in the watermark, and ERRCODE - a function which further encodes/decodes watermark information so that errors introduced into a watermark may be corrected after extraction from the content signal.

Additionally, a new method of synchronizing decoder software to an embedded watermark is described. In a previous disclosure, a method whereby a marker sequence of N random bits was generated, and used to signal the start of an encoded watermark was described. When the decoder recognizes the N bit sequence, it knows it is synchronized. In that system the chance of a false positive synchronization was estimated at 1/(N^2) ("one over (N to the power of 2)"). While that method is fairly reliable, it depends on the marker being encoded as part of the steganographic process, into the content stream. While errors in the encoded bits may be partially offset by error coding techniques, error coding the marker will require more computation and complexity in the system. It also does not completely eliminate the possibility that a randomization attack can succeed in destroying the marker. A new method is implemented in which the encoder pre-processes the digital sample stream, calculating where watermark information will be encoded. As it is doing this, it notes the starting position of each complete watermark, and records to a file, a sequence of N-bits representing sample information corresponding to the start of the watermark, for instance, the 3rd most significant bit of the 256 samples immediately preceding the start of a watermark. This would be a 256 bit marker. The order in which these markers are encountered is preserved, as it is important. The decoder then searches for matches to these markers. It processes the markers from first to last, discarding each as it is found, or possibly not found within a certain scanning distance, and proceeding with the remaining markers. This method does not modify

the original signal with marker information and has the added benefit that high-significance sequences can be used, requiring that an attack based on randomizing markers do very obvious damage to the content stream.

With multichannel encoding, both private and public keys, similar in use to those from public-key cryptosystems, could be provided for authentication by concerned third party vendors and consumers, as well as contribute to better management and protection of copyrights for the digital world that already exist in the physical world. For more information on public-key cryptosystems see US Pat No 4,200,770 Diffie-Hellman, 4,218,582 Hellman, 4,405,829 RSA, 4,424,414 Hellman Pohlig. In addition, any number of key "designations" between "public" and "private" could be established, to provide various access privileges to different groups. Multi-channel watermarks are effected by encoding separate watermark certificates with separate keys by either interleaving windows in the time domain or by using separate frequency bands in the frequency domain. For instance, 3 separate watermarks could be encoded by using every third sample window processed to encode a corresponding certificate. Alternatively, complete watermarks could be interleaved. Similarly, the frequency range of an audio recording might be partitioned into 3 sub-ranges for such a purpose. Use of multi-channel watermarks would allow groups with varying access privileges to access watermark information in a given content signal. The methods of multichannel encoding would further provide for more holographic and inexpensive maintenance of copyrights by parties that have differing levels of access priority as decided by the ultimate owner or publisher of the underlying content. Some watermarks could even play significant roles in adhering to given filtering (for example, content that is not intended for all

DISH-Blue Spike-842
Exhibit 1004, Page 1344

observers), distribution, and even pricing schemes for given pieces of content. Further, on-the-fly watermarking could enhance identification of pieces of content that are traded between a number of parties or in a number of levels of distribution. Previously discussed patents by Preuss et al. and Greenberg and other similar systems lack this feature.

Further improvements over the prior art include the general capacity and robustness of the given piece of information that can be inserted into media content with digital watermarks, described in **Steganographic Method and Device** and further modified here, versus "spread spectrum-only" methods. First, the spread spectrum technique described in US. Patent No. 5,319,735 Preuss et al. is limited to an encoding rate of 4.3 8-bit symbols per second within a digital audio signal. This is because of the nature of reliability requirements for spread spectrum systems. The methods described in this invention and those of the previous application, "Steganographic Method and Device," do not particularly adhere to the use of such spread spectrum techniques, thus removing such limitation. In the steganographic derived implementation the inventors have developed based on these filings, watermarks of approximately 1,000 bytes (or 1000x 8 bits) were encoded at a rate of more than 2 complete watermarks per second into the carrier signal. The carrier signal was a two channel (stereo) 16-bit, 44.1 Khz recording. The cited encoding rate is per channel. This has been successfully tested in a number of audio signals. While this capacity is likely to decrease by 50% or more as a result of future improvements to the security of the system, it should still far exceed the 4.3 symbols per second envisioned by Preuss et al. Second, the ability exists to recover the watermarked information with a sample of the overall piece of digitized content (that is, for instance, being

DISH-Blue Spike-842
Exhibit 1004, Page 1345

able to recover a watermark from just 10 seconds of a 3 minute song, depending on the robustness or size of the data in a given watermark) instead of a full original. Third, the encoding process described in **Steganographic Method and Device** and further modified in this invention explicitly seeks to encode the information signal in such a way with the underlying content signal as to make destruction of the watermark cause destruction of the underlying signal. The prior art describes methods that confuse the outright destruction of the underlying content with "the level of difficulty" of removing or altering information signals that *may* destroy underlying content. This invention anticipates efforts that can be undertaken with software, such as Digidesign's Sound Designer II or Passport Design's Alchemy, which gives audio engineers (similar authoring software for video also exists, for instance, that sold by Avid Technology, and others as well as the large library of picture authoring tools) very precise control of digital signals, "embedded" or otherwise, that can be purely manipulated in the frequency domain. Such software provides for bandpass filtering and noise elimination options that may be directed at specific ranges of the frequency domain, a ripe method for attack in order to hamper recovery of watermark information encoded in specific frequency ranges.

Separating the decoder from the encoder can limit the ability to reverse the encoding process while providing a reliable method for third parties to be able to make attempts to screen their archives for watermarked content without being able to tamper with all of the actual watermarks. This can be further facilitated by placing separate signals in the content using the encoder, which signal the presence of a valid watermark, e.g. by providing a "public key accessible" watermark channel which contains information comprised

of a digitally signed digital notary registration of the watermark in the private channel, along with a checksum verifying the content stream. The checksum reflects the unique nature of the actual samples which contain the watermark in question, and therefore would provide a means to detect an attempt to graft a watermark lifted from one recording and placed into another recording in an attempt to deceive decoding software of the nature of the recording in question. During encoding, the encoder can leave room within the watermark for the checksum, and analyze the portion of the content stream which will contain the watermark in order to generate the checksum before the watermark is encoded. Once the checksum is computed, the complete watermark certificate, which now contains the checksum, is signed and/or encrypted, which prevents modification of any portion of the certificate, including the checksum, and finally encoded into the stream. Thus, if it is somehow moved at a later time, that fact can be detected by decoders. Once the decoder functions are separate from the encoder, watermark decoding functionality could be embedded in several types of software including search agents, viruses, and automated archive scanners. Such software could then be used to screen files or search out files from archive which contain specific watermark information, types of watermarks, or lack watermarks. For instance, an online service could, as policy, refuse to archive any digital audio file which does not contain a valid watermark notarized by a trusted digital notary. It could then run automated software to continuously scan its archive for digital audio files which lack such watermarks, and erase them.

Watermarks can be generated to contain information to be used in effecting software or content metering services. In order to accomplish this, the watermark

would include various fields selected from the following information:

title identification;

unit measure;

unit price;

percentage transfer threshold at which liability is incurred to purchaser;

percent of content transferred;

authorized purchaser identification;

seller account identification;

payment means identification;

digitally signed information from sender indicating percent of content transferred; and

digitally signed information from receiver indicating percent of content received.

These "metering" watermarks could be dependent on a near continuous exchange of information between the transmitter and receiver of the metered information in question. The idea is that both sides must agree to what the watermark says, by digitally signing it. The sender agrees they have sent a certain amount of a certain title, for instance, and the receiver agrees they have received it, possibly incurring a liability to pay for the information once a certain threshold is passed. If the parties disagree, the transaction can be discontinued before such time. In addition, metering watermarks could contain account information or other payment information which would facilitate the transaction.

Watermarks can also be made to contain information pertaining to geographical or electronic distribution restrictions, or which contain information on where to locate other copies of this content, or similar content. For instance, a watermark might stipulate that a recording is for sale only in the United States, or that it is to be sold only to persons connecting to an online

DISH-Blue Spike-842
Exhibit 1004, Page 1348

distribution site from a certain set of internet domain names, like ".us" for United States, or ".ny" for New York. Further a watermark might contain one or more URLs describing online sites where similar content that the buyer of a piece of content might be interested in can be found.

A digital notary could also be used in a more general way to register, time stamp and authenticate the information inside a watermark, which is referred to as the certificate. A digital notary processes a document which contains information and assigns to it a unique identification number which is a mathematical function of the contents of the document. The notary also generally includes a time stamp in the document along with the notary's own digital signature to verify the date and time it received and "notarized" the document. After being so notarized, the document cannot be altered in any way without voiding its mathematically computed signature. To further enhance trust in such a system, the notary may publish in a public forum, such as a newspaper, which bears a verifiable date, the notarization signatures of all documents notarized on a given date. This process would significantly enhance the trust placed in a digital watermark extracted for the purpose of use in settling legal disputes over copyright ownership and infringement.

Other "spread spectrum" techniques described in the art have predefined time stamps to serve the purpose of verifying the actual time a particular piece of content is being played by a broadcaster, e.g., U.S. Patent No. 5,379,345 Greenberg, not the insertion and control of a copyright or similar information (such as distribution path, billing, metering) by the owner or publisher of the content. The Greenberg patent focuses almost exclusively on concerns of broadcasters, not content creators who deal with digitized media content when

DISH-Blue Spike-842
Exhibit 1004, Page 1349

distributing their copyrightable materials to unknown parties. The methods described are specific to spread spectrum insertion of signals as "segment timing marks" to make comparisons against a specific master of the underlying broadcast material-- again with the intention of specifying if the broadcast was made according to agreed terms with the advertisers. No provisions are made for stamping given audio signals or other digital signals with "purchaser" or publisher information to stamp the individual piece of content in a manner similar to the sales of physical media products (CDs, CD-ROMs, etc.) or other products in general (pizza delivery, direct mail purchases, etc.). In other words, "interval-defining signals," as described in the Greenberg patent, are important for verification of broadcasts of a time-based commodity like time and date-specific, reserved broadcast time, but have little use for individuals trying to specify distribution paths, pricing, or protect copyrights relating to given content which may be used repeatedly by consumers for many years. It would also lack any provisions for the "serialization" and identification of individual copies of media content as it can be distributed or exchanged on the Internet or in other on-line systems (via telephones, cables, or any other electronic transmission media). Finally, the Greenberg patent ties itself specifically to broadcast infrastructure, with the described encoding occurring just before transmission of the content signal via analog or digital broadcast, and decoding occurring upon reception.

While the discussion above has described the invention and its use within specific embodiments, it should be clear to those skilled in the art that numerous modifications may be made to the above without departing from the spirit of the invention, and that the

DISH-Blue Spike-842
Exhibit 1004, Page 1350

scope of the above invention is to be limited only by the claims appended hereto.

DISH-Blue Spike-842
Exhibit 1004, Page 1351

What is Claimed:

1. A method for using a computer to generate a random or pseudo random key for a digital watermark system wherein said random key includes:

a random or pseudo random sequence of binary 1s and 0s

information describing the application of the random sequence to a stream of digitized samples wherein said information includes:

at least one list of time delimiters describing segments of the stream;

at least one list of frequency delimiters describing frequency bands to be included in watermark computations; and

a signal encoding level;

wherein the method comprises the step of receiving human interactive input information used to describe limits on where, at what level, and at what frequencies the random binary information of the random key is to be applied to the stream of digitized samples in encoding the digital watermark;

wherein said human interactive input information comprises at least one of the following datum:

a list of time delimiters;

a list of frequency delimiters; and

a signal encoding level.

2. The method of claim 1 further comprising the step of selecting said stream of digitized samples from a list provided by a computer system.

3. The method of claim 2 further comprising the step of creating and displaying a graphical representation on the display device of the computer

DISH-Blue Spike-842
Exhibit 1004, Page 1352

system, wherein said graphical representation includes a time axis and a signal frequency axis.

4. The method of claim 2 further comprising the step of creating and displaying a graphical representation on the display device of the computer system, wherein said graphical representation includes a time axis and a signal amplitude axis.

5. The method of claim 3 or 4, further comprising the step of updating the graphical display to reflect receipt of new human interactive input information.

6. The method of claim 5 further comprising the step of generating a random or pseudo random sequence of 1s and 0s.

7. The method of claim 6 further comprising the step of storing input information in association with the random sequence of 1s and 0s as a single record in a database of such records.

8. The method of claim 7 wherein the record is encrypted using a pass phrase.

9. The method of claim 1 where the stream of digitized samples contains a digital audio recording.

10. The method of claim 1 where the stream of digitized samples to be watermarked contains a digital video recording.

11. The method of claim 6 wherein the process of generating the random sequence comprises the steps of:

DISH-Blue Spike-842
Exhibit 1004, Page 1353

(a) collecting a series of random bits derived from keyboard latency intervals in random typing;

(b) processing the initial series of random bits through a secure one-way hash function;

(c) using the results of one-way hash function to seed a block encryption cipher loop;

(d) cycling through the block encryption loop, and extracting the least significant bit of each result after cycle; and

(e) concatenating the block encryption output bits into the random key sequence

12. A method of encoding and decoding a digital watermark where the encoder and decoder are separate software applications or hardware devices.

13. The method of claim 12 wherein the decoder functionality is embedded in a software search engine, word-wide web-crawler file scanning engine, intelligent agent, or a virus.

14. The method of claim 12 wherein the decoder can access only a limited number of watermark channels, corresponding to public watermark keys, or any keys otherwise made available to said decoder.

15. The method of claim 12 wherein the decoder is capable of detecting the presence of a valid watermark but not of accessing the information in the watermark.

16. The method of claim 12 wherein the encoder places a separate signal, which does not interfere with the watermark, into a content stream, where said separate signal can indicate

DISH-Blue Spike-842
Exhibit 1004, Page 1354

watermark synchronization information, which helps locate watermarks in the content; and

the presence of a valid watermark in the content.

17. A method of using digital watermarks to convey information which is to be used for a content metering service, wherein said watermarks contain at least one of the following pieces of information:

title identification;

unit measure;

unit price;

percentage transfer threshold at which liability is incurred to purchaser;

percent of content transferred;

authorized purchaser identification;

seller account identification;

payment means identification;

digitally signed information from sender indicating percent of content transferred; and

digitally signed information from receiver indicating percent of content received.

18. A method of encoding digital watermarks which contain information pertaining to distribution restrictions and a location of an addressable directory containing related content, where said watermarks contain at least one of the following pieces of information:

geographical constraints on distribution (state, country, etc);

logical constraints on distribution;

Universal Resource Locator (URL);

telephone number;

Internet Protocol address;

Internet domain name;

email address; and

DISH-Blue Spike-842
Exhibit 1004, Page 1355

file name.

19. A method of encoding multiple digital watermarks into a single content stream wherein each watermark is encoded with a separate key.

20. The method of claim 18 wherein watermark information from each watermark is interleaved in the time domain.

21. A method of claim 18 wherein watermark information from each watermark is placed into specific frequency bands, or interleaved in the frequency domain.

22. A method of associating with a pseudo-random key, a list of component function references, which dictate what component functions are applied to the encoding and decoding of a digital watermark using the key in question.

23. A method of providing synchronization of a decoder to watermark which consists of the following steps:

a) recording a feature of sample stream, or a marker extracted from the sample stream immediately preceding the start of an encoded watermark;

b) recording the order in which a list of markers was encountered in the sample stream;

c) storing a list of such markers and the order of their appearance in a file for use by the decoder;

d) optionally, associating the stored information of step c) with a watermark key or watermark receipt or content title;

e) in the decoder, selecting a marker from the file in step c) such that the selected marker is not previous

in order to any other marker previously selected in decoding the sample stream in question;

f) attempting to find a feature or marker in the portion of the sample stream currently under processing;

g) at such time as the currently selected marker is deemed unlikely to be found, discarding it and proceeding to step e);

h) at such time as marker is found, decoding the watermark, then proceeding to step e) unless the sample stream is exhausted.

DISH-Blue Spike-842
Exhibit 1004, Page 1357

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00652

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL :380/20
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/20, 54

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US, A, 5,530,759 (BRAUDAWAY ET AL) 25 June 1996, see Figs. 1-2.	1-11, 22

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 06 MAY 1997	Date of mailing of the international search report 09 JUN 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer SALVATORE CANGIALOSI Telephone No. (703) 305-1837

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00652

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-11 and 22

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

DISH-Blue Spike-842
Exhibit 1004, Page 1359

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00652

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

Group I, Claims 1-11, 22, drawn to an method of generating an encrypted digital watermark.

Group II, Claims 12-21 and 23 method of making and using a digital watermark.

The inventions listed as Groups I-II do not relate to a single inventive concept under PCT Rule 13.1 because under PCT Rule 13.2, they lack the same or corresponding technical features for the following Reasons: The invention of Group I lack the separate software, hardware devices or content monitoring. The invention of Group II lack the pseudo-Random key.

DISH-Blue Spike-842
Exhibit 1004, Page 1360

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G09C 5/00, H04L 9/00	A1	(11) International Publication Number: WO 98/02864
		(43) International Publication Date: 22 January 1998 (22.01.98)

(21) International Application Number: PCT/US97/11455

(22) International Filing Date: 2 July 1997 (02.07.97)

(30) Priority Data:
08/677,435 2 July 1996 (02.07.96) US

(71) Applicant: THE DICE COMPANY [US/US]; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US).

(72) Inventors: MOSKOWITZ, Scott, A.; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US). COOPERMAN, Marc, S.; 2929 Ramona, Palo Alto, CA 94306 (US).

(74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).

(81) Designated States: AU, BR, CN, JP, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: OPTIMIZATION METHODS FOR THE INSERTION, PROTECTION AND DETECTION OF DIGITAL WATERMARKS IN DIGITIZED DATA

(57) Abstract

The implementations of digital watermarks can be optimally suited to particular transmission, distribution and storage mediums given the nature of digitally-sampled audio, video and other multimedia works. Watermark application parameters can be adapted to the individual characteristics of a given digital sample stream. Watermark information can be either carried in individual samples or in relationships between multiple samples, such as in a waveform shape. More optimal models may be obtained to design watermark systems that are tamper-resistant given the number and breadth of existent digitized sample options with different frequency and time components. The highest quality of a given content signal may be maintained as it is mastered, with the watermark suitably hidden, taking into account usage of digital filters and error correction. The quality of the underlying content signals can be used to identify and highlight advantageous locations for the insertion of digital watermarks. The watermark is integrated as closely as possible to the content signal, at a maximum level to force degradation of the content signal when attempts are made to remove the watermarks.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

OPTIMIZATION METHODS FOR THE INSERTION, PROTECTION AND DETECTION OF DIGITAL WATERMARKS IN DIGITIZED DATA

RELATED APPLICATIONS

This application is related to patent applications entitled "Steganographic Method and Device", Serial No. 08/489,172 filed on June 7, 1995; "Method for Human-Assisted Random Key Generation and Application for Digital Watermark System", Serial No. 08/587,944 filed on January 17, 1996; "Method for Stega-Cipher Protection of Computer Code", Serial No. 08/587,943 filed on January 17, 1996; "Digital Information Commodities Exchange", Serial No. 08/365,454 filed on December 28, 1994, which is a continuation of Serial No. 08/083,593 filed on June 30, 1993; and "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management", Serial No. 08/674,726 filed on July 2, 1996. These related applications are all incorporated herein by reference.

This application is also related to U.S. Patent No. 5,428,606, "Digital Information Commodities Exchange", issued on June 27, 1995, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

The present invention relates to digital watermarks.

Digital watermarks exist at a convergence point where creators and publishers of digitized multimedia content demand localized, secured

identification and authentication of that content. Because existence of piracy is clearly a disincentive to the digital distribution of copyrighted works, establishment of responsibility for copies and derivative copies of such works is invaluable. In considering the various forms of multimedia content, whether "master," stereo, NTSC video, audio tape or compact disc, tolerance of quality degradation will vary with individuals and affect the underlying commercial and aesthetic value of the content. It is desirable to tie copyrights, ownership rights, purchaser information or some combination of these and related data to the content in such a manner that the content must undergo damage, and therefore a reduction in value, with subsequent, unauthorized distribution of the content, whether it be commercial or otherwise.

Legal recognition and attitude shifts, which recognize the importance of digital watermarks as a necessary component of commercially distributed content (audio, video, game, etc.), will further the development of acceptable parameters for the exchange of such content by the various parties engaged in the commercial distribution of digital content. These parties may include artists, engineers, studios, INTERNET access providers, publishers, agents, on-line service providers, aggregators of content for various forms of delivery, on-line retailers, individuals and parties that participate in the transfer of funds to arbitrate the actual delivery of content to intended parties.

Since the characteristics of digital recordings vary widely, it is a worthwhile goal to provide tools to describe an optimized envelope of parameters for inserting, protecting and detecting digital watermarks in a given digitized sample (audio, video, virtual reality, etc.) stream. The optimization techniques described hereinafter make unauthorized removal of digital watermarks containing these parameters a significantly costly operation in terms of the absolute given projected economic gain from undetected commercial distribution. The optimization techniques, at the least, require significant damage to the content signal, as to make the

unauthorized copy commercially worthless, if the digital watermark is removed, absent the use of extremely expensive tools.

Presumably, the commercial value of some works will dictate some level of piracy not detectable in practice and deemed "reasonable" by rights holders given the overall economic return. For example, there will always be fake $100 bills, LEVI jeans, and GUCCI bags, given the sizes of the overall markets and potential economic returns for pirates in these markets--as there also will be unauthorized copies of works of music, operating systems (Windows95, etc.), video and future multimedia goods.

However, what differentiates the "digital marketplace" from the physical marketplace is the absence of any scheme that establishes responsibility and trust in the authenticity of goods. For physical products, corporations and governments mark the goods and monitor manufacturing capacity and sales to estimate loss from piracy. There also exist reinforcing mechanisms, including legal, electronic, and informational campaigns to better educate consumers.

SUMMARY OF THE INVENTION

The present invention relates to implementations of digital watermarks that are optimally suited to particular transmission, distribution and storage mediums given the nature of digitally-sampled audio, video, and other multimedia works.

The present invention also relates to adapting watermark application parameters to the individual characteristics of a given digital sample stream.

The present invention additionally relates to the implementation of digital watermarks that are feature-based. That is, a system where watermark information is not carried in individual samples, but is carried in the relationships between multiple samples, such as in a waveform shape. The present invention envisions natural extensions for digital watermarks that may also separate frequencies (color or audio), channels in 3D while utilizing discreteness in feature-based encoding only known to those with

pseudo-random keys (i.e., cryptographic keys) or possibly tools to access such information, which may one day exist on a quantum level.

The present invention additionally relates to a method for obtaining more optimal models to design watermark systems that are tamper-resistant given the number and breadth of existent digitized-sample options with differing frequency and time components (audio, video, pictures, multimedia, virtual reality, etc.).

To accomplish these goals, the present invention maintains the highest quality of a given content signal as it was mastered, with its watermarks suitably hidden, taking into account usage of digital filters and error correction presently concerned solely with the quality of content signals.

The present invention additionally preserves quality of underlying content signals, while using methods for quantifying this quality to identify and highlight advantageous locations for the insertion of digital watermarks.

The present invention integrates the watermark, an information signal, as closely as possible to the content signal, at a maximal level, to force degradation of the content signal when attempts are made to remove the watermarks.

The present invention relates to a method for amplitude independent encoding of digital watermark information in a signal including steps of determining in the signal a sample window having a minimum and a maximum, determining a quantization interval of the sample window, normalizing the sample window, normalizing the sample window to provide normalized samples, analyzing the normalized samples, comparing the normalized samples to message bits, adjusting the quantization level of the sample window to correspond to the message bit when a bit conflicts with the quantization level and de-normalizing the analyzed samples.

The present invention also relates to a method for amplitude independent decoding of digital watermark information in a signal including steps of determining in the signal a sample window having a minimum and a

maximum, determining a quantization interval of the sample window, normalizing the sample window to provide samples, and analyzing the quantization level of the samples to determine a message bit value.

The present invention additionally relates to a method of encoding and decoding watermarks in a signal where, rather than individual samples, insertion and detection of abstract signal features to carry watermark information in the signal is done.

The present invention also relates to a method for pre-analyzing a digital signal for encoding digital watermarks using an optimal digital filter in which it is determined what noise elements in the digital signal will be removed by the optimal digital filter based on response characteristics of the filter.

The present invention also relates to a method of error coding watermark message certificates using cross-interleaved codes which use error codes of high redundancy, including codes with Hamming distances of greater than or equal to "n", wherein "n" is a number of bits in a message block.

The present invention additionally relates to a method of pre-processing a watermark message certificate including a step of determining an absolute bit length of the watermark message as it will be encoded.

The present invention additionally relates to a method of generating watermark pseudo-random key bits using a non-linear (chaotic) generator or to a method of mapping pseudo-random key and processing state information to affect an encode/decode map using a non-linear (chaotic) generator.

The present invention additionally relates to a method of guaranteeing watermark certificate uniqueness including a step of attaching a time stamp or user identification dependent hash or message digest of watermark certificate data to the certificate.

The present invention also relates to a method of generating and quantizing a local noise signal to contain watermark information where the

noise signal is a function of at least one variable which depends on key and processing state information.

The present invention also relates to a method of dithering watermark quantizations such that the dither changes an absolute quantization value, but does not change a quantization level or information carried in the quantization.

The present invention further relates to a method of encoding watermarks including inverting at least one watermark bit stream and encoding a watermark including the inverted watermark bit stream.

The present invention also relates to a method of decoding watermarks by considering an original watermark synchronization marker, an inverted watermark synchronization marker, and inverted watermarks, and decoding based on those considerations.

The present invention also relates to a method of encoding and decoding watermarks in a signal using a spread spectrum technique to encode or decode where information is encoded or decoded at audible levels and randomized over both frequency and time.

The present invention additionally relates to a method of analyzing composite digitized signals for watermarks including obtaining a composite signal, obtaining an unwatermarked sample signal, time aligning the unwatermarked sample signal to the composite signal, gain adjusting the time aligned unwatermarked sample signal to the composite signal, estimating a pre-composite signal using the composite signal and the gain adjusted unwatermarked sample signal, estimating a watermarked sample signal by subtracting the estimated pre-composite signal for the composite signal, and scanning the estimated watermark sample signal for watermarks.

The present invention additionally relates to a method for varying watermark encode/decode algorithms automatically during the encoding or decoding of a watermark including steps of (a) assigning a list of desired CODECs to a list of corresponding signal characteristics which indicate use

of particular CODECs, (b) during encoding/decoding, analyzing characteristics of the current sample frame in the signal stream, prior to delivering the frame to CODEC, (c) looking up the corresponding CODEC from the list of CODECs in step (a) which matches the observed signal characteristics from step (b), (d) loading and/or preparing the desired CODEC, (e) passing the sample frame to the CODEC selected in step (c), and f) receiving the output samples from step (e).

The present invention also relates to a method for varying watermark encode/decode algorithms automatically during the encoding or decoding of a watermark, including steps of (a) assigning a list of desired CODECs to a list of index values which correspond to values computed to values computed as a function of the pseudo-random watermark key and the state of the processing framework, (b) during encoding/decoding, computing the pseudo-random key index value for the current sample frame in the signal stream, prior to delivering the frame to a CODEC, (c) looking up the corresponding CODEC from the list of CODECs in step (a) which matches the index value from step (b), (d) loading and/or preparing the desired CODEC, (e) passing the sample frame to the CODEC selected in step (c), and (f) receiving the output samples from step (e).

DETAILED DESCRIPTION

The present invention relates to implementations of digital watermarks that are optimally suited to particular transmission, distribution and storage mediums given the nature of digitally sampled audio, video, and other multimedia works.

The present invention also relates to adapting watermark application parameters to the individual characteristics of a given digital sample stream.

The present invention additionally relates to the implementation of digital watermarks that are feature-based. That is, a system where watermark information is not carried in individual samples, but is carried in the relationships between multiple samples, such as in a waveform shape.

For example, in the same manner a US $100 bill has copy protection features including ink type, paper stock, fiber, angles of artwork that distort in photocopier machines, inserted magnetic strips, and composite art, the present invention envisions natural extensions for digital watermarks that may also separate frequencies (color or audio), channels in 3D while utilizing discreteness in feature-based encoding only known to those with pseudo-random keys (i.e., cryptographic keys) or possibly tools to access such information, which may one day exist on a quantum level.

There are a number of hardware and software approaches in the prior art that attempt to provide protection of multimedia content, including encryption, cryptographic containers, cryptographic envelopes or "cryptolopes", and trusted systems in general. None of these systems places control of copy protection in the hands of the content creator as the content is created, nor provides an economically feasible model for exchanging the content to be exchanged with identification data embedded within the content.

Yet, given the existence of over 100 million personal computers and many more non-copy-protected consumer electronic goods, copy protection seems to belong within the signals. After all, the playing (i.e., using) of the content establishes its commercial value.

Generally, encryption and cryptographic containers serve copyright holders as a means to protect data in transit between a publisher or distributor and the purchaser of the data (i.e., a means of securing the delivery of copyrighted material from one location to another by using variations of public key cryptography or other more centralized cryptosystems).

Cryptolopes are suited specifically for copyrighted text that is time-sensitive, such as newspapers, where intellectual property rights and origin data are made a permanent part of the file. For information on public-key cryptosystems see U.S. Patent No. 4,200,770 to Hellman et al., U.S. Patent No. 4,218,582 to Hellman et al., U.S. Patent No. 4,405,829 to Rivest et al.,

and U.S. Patent No. 4,424,414 to Hellman et al. Systems are proposed by IBM and Electronic Publishing Resources to accomplish cryptographic container security.

Digitally-sampled copyrighted material, that is binary data on a fundamental level, is a special case because of its long term value coupled with the ease and perfectness of copying and transmission by general purpose computing and telecommunications devices. In particular, in digitally-sampled material, there is no loss of quality in copies and no identifiable differences between one copy and any other subsequent copy. For creators of content, distribution costs may be minimized with electronic transmission of copyrighted works. Unfortunately, seeking some form of informational or commercial return via electronic exchange is ill-advised absent the use of digital watermarks to establish responsibility for specific copies and unauthorized copying. Absent digital watermarks, the unlikely instance of a market of trusted parties who report any distribution or exchange of unauthorized copies of the protected work must be relied upon for enforcement. Simply, content creators still cannot independently verify watermarks should they choose to do so.

For a discussion of systems that are oriented around content-based addresses and directories, see U.S. Patent No. 5,428,606 to Moskowitz.

In combining steganographic methods for insertion of information identifying the title, copyright holder, pricing, distribution path, licensed owner of a particular copy, or a myriad of other related information, with pseudo-random keys (which map insertion location of the information) similar to those used in cryptographic applications, randomly placed signals (digital watermarks) can be encoded as random noise in a content signal. Optimal planning of digital watermark insertion can be based on the inversion of optimal digital filters to establish or map areas comprising a given content signal insertion envelope. Taken further, planning operations will vary for different digitized content: audio, video, multimedia, virtual reality, etc. Optimization techniques for processes are described in the

copending related applications entitled "Steganographic Method and Device" and "Method for Human Assisted Random Key Generation and Application for Digital Watermark System".

Optimization processes must take into consideration the general art of digitization systems where sampling and quantizing are fundamental physical parameters. For instance, discrete time sampling has a natural limit if packets of time are used, estimated at $1x10^{-42}$ second. This provides a natural limit to the sampling operation. Also, since noise is preferable to distortion, quantizing will vary given different storage mediums (magnetic, optical, etc.) or transmission mediums (copper, fiber optic, satellite, etc.) for given digitized samples (audio, video, etc.). Reducing random bit error, quantization error, burst error, and the like is done for the singular goal of preserving quality in a given digitized sample. Theoretical perfect error correction is not efficient, given the requirement of a huge allocation of redundant data to detect and correct errors. In the absence of such overhead, all error correction is still based on data redundancy and requires the following operations: error detection to check data validity, error correction to replace erroneous data, and error concealment to hide large errors or substitute data for insufficient data correction. Even with perfect error correction, the goal of a workable digital watermark system for the protection of copyrights would be to distribute copies that are less than perfect but not perceivably different from the original. Ironically, in the present distribution of multimedia, this is the approach taken by content creators when faced with such distribution mechanisms as the INTERNET. As an example, for audio clips commercially exchanged on the World Wide Web (WWW), a part of the INTERNET, 8 bit sampled audio or audio downsampled from 44.1 kHz (CD-quality), to 22 kHz and lower. Digital filters, however, are not ideal because of trade-offs between attenuation and time-domain response, but provide the engineer or similarly-trained individual with a set of decisions to make about maximizing content quality with minimum data overhead and consideration of the ultimate delivery

mechanism for the content (CDs, cable television, satellite, audio tape, stereo amplifier, etc.).

For audio signals and more generally for other frequency-based content, such as video, one method of using digital filters is to include the use of an input filter to prevent frequency aliasing higher than the so-called Nyquist frequencies. The Nyquist theorem specifies that the sampling frequency must be at least twice the highest signal frequency of the sampled information (e.g., for the case of audio, human perception of audio frequencies is in a range between 20 Hz and 20 kHz). Without an input filter, aliases can still occur leaving an aliased signal in the original bandwidth that cannot be removed.

Even with anti-aliasing filters, quantization error can still cause low level aliasing which may be removed with a dither technique. Dither is a method of adding random noise to the signal, and is used to de-correlate quantization error from the signal while reducing the audibility of the remaining noise. Distortion may be removed, but at the cost of adding more noise to the filtered output signal. An important effect is the subsequent randomization of the quantization error while still leaving an envelope of an unremovable signaling band of noise. Thus, dither is done at low signal levels, effecting only the least significant bits of the samples. Conversely, digital watermarks, which are essentially randomly-mapped noise, are intended to be inserted into samples of digitized content in a manner such as to maximize encoding levels while minimizing any perceivable artifacts that would indicate their presence or allow for removal by filters, and without destroying the content signal. Further, digital watermarks should be inserted with processes that necessitate random searching in the content signal for watermarks if an attacker lacks the keys. Attempts to over-encode noise into known watermarked signal locations to eliminate the information signal can be made difficult or impossible without damaging the content signal by relying on temporal encoding and randomization in the generation of keys during digital watermark insertion. As a result, although the

watermark occupies only a small percentage of the signal, an attacker is forced to over-encode the entire signal at the highest encoding level, which creates audible artifacts.

The present invention relates to methods for obtaining more optimal models to design watermark systems that are tamper-resistant given the number and breadth of existent digitized sample options with differing frequency and time components (audio, video, pictures, multimedia, virtual reality, etc.).

To accomplish these goals, the present invention maintains the highest quality of a given content signal as it was mastered, with its watermarks suitably hidden, taking into account usage of digital filters and error correction presently concerned solely with the quality of content signals.

Additionally, where a watermark location is determined in a random or pseudo-random operation dependent on the creation of a pseudo-random key, as described in copending related application entitled "Steganographic Method and Device" assigned to the present assignee, and unlike other forms of manipulating digitized sample streams to improve quality or encode known frequency ranges, an engineer seeking to provide high levels of protection of copyrights, ownership, etc. is concerned with the size of a given key, the size of the watermark message and the most suitable area and method of insertion. Robustness is improved through highly redundant error correction codes and interleaving, including codes known generally as q-ary Bose-Chaudhuri-Hocquenghem (BCH) codes, a subset of Hamming coding operations, and codes combining error correction and interleaving, such as the Cross-Interleave Reed-Solomon Code. Using such codes to store watermark information in the signal increases the number of changes required to obliterate a given watermark. Preprocessing the certificate by considering error correction and the introduction of random data to make watermark discovery more difficult, prior to watermarking, will help determine sufficient key size. More generally, absolute key size can be

DISH-Blue Spike-842
Exhibit 1004, Page 1374

determined through preprocessing the message and the actual digital watermark (a file including information regarding the copyright owner, publisher, or some other party in the chain of exchange of the content) to compute the absolute encoded bit stream and limiting or adjusting the key size parameter to optimize the usage of key bits. The number of bits in the primary key should match or exceed the number of bits in the watermark message, to prevent redundant usage of key bits. Optimally, the number of bits in the primary key should exactly match the watermark size, since any extra bits are wasted computation.

Insertion of informational signals into content signals and ranges from applications that originate in spread spectrum techniques have been contemplated. More detailed discussions are included in copending related applications entitled "Steganographic Method and Device" and entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System".

The following discussion illustrates some previously disclosed systems and their weaknesses.

Typically, previously disclosed systems lack emphasis or implementation of any pseudo-random operations to determine the insertion location, or map, of information signals relating to the watermarks. Instead, previous implementations provide "copy protect" flags in obvious, apparent and easily removable locations. Further, previous implementations do not emphasize the alteration of the content signal upon removal of the copy protection.

Standards for digital audio tape (DAT) prescribe insertion of data such as ISRC (Industry Standard Recording Codes) codes, title, and time in sub-code according to the Serial Copy Management System (SCMS) to prevent multiple copying of the content. One time copying is permitted, however, and systems with AES3 connectors, which essentially override copy protection in the sub-code as implemented by SCMS, actually have no copy limitations. The present invention provides improvement over this

implementation with regard to the ability of unscrupulous users to load digital data into unprotected systems, such general computing devices, that may store the audio clip in a generalized file format to be distributed over an on-line system for further duplication. The security of SCMS (Serial Copy Management System) can only exist as far as the support of similarly-oriented hardware and the lack of attempts by those skilled in the art to simply remove the subcode data in question.

Previous methods seek to protect content, but shortcomings are apparent. U.S. Patent No. 5,319,735 to Preuss et al. discusses a spread spectrum method that would allow for over-encoding of the described, thus known, frequency range and is severely limited in the amount of data that can be encoded-- 4.3 8-bit symbols per second. However, with the Preuss et al. method, randomization attacks will not result in audible artifacts in the carrier signal, or degradation of the content as the information signal is in the subaudible range. It is important to note the difference in application between spread spectrum in military field use for protection of real-time radio signals, and encoding information into static audio files. In the protection of real-time communications, spread spectrum has anti-jam features, since information is sent over several channels at once. Therefore, in order to jam the signal, one has to jam all channels, including their own. In a static audio file, however, an attacker has practically unlimited time and processing power to randomize each sub-channel in the signaling band without penalty to themselves, so the anti-jam advantages of spread spectrum do not extend to this domain.

In a completely different implementation, U.S. Patent No. 5,379,345 to Greenberg seeks enforcement of broadcast contracts using a spread spectrum modulator to insert signals that are then confirmed by a spread spectrum-capable receiver to establish the timing and length that a given, marked advertisement is played. This information is measured against a specific master of the underlying broadcast material. The Greenberg patent does not ensure that real-time downloads of copyrighted content can be

marked with identification information unless all download access points (PCs, modems, etc.), and upload points for that matter, have spread spectrum devices for monitoring.

Other methods include techniques similar to those disclosed in related copending patent applications mentioned above by the present assignee, but lack the pseudo-random dimension of those patent applications for securing the location of the signals inserted into the content. One implementation conducted by Michael Gerzon and Peter Craven, and described by Ken Pohlmann in the 3rd edition of Principles of Digital Audio, illustrates a technology called "buried data technique," but does not address the importance of randomness in establishing the insertion locations of the informational signals in a given content signal, as no pseudo-random methods are used as a basis for insertion. The overriding concern of the "buried data techniques" appears to be to provide for a "known channel" to be inserted in such a manner as to leave little or no perceivable artifacts in the content signal while prescribing the exact location of the information (i.e., replacing the least significant bits (LSB) in a given information signal). In Gerzon and Craven's example, a 20-bit signal gives way to 4-bits of LSBs for adding about 27 dB of noise to the music. Per channel data insertion reached 176.4 kilobits per second per channel, or 352.8 kbps with stereo channels. Similarly attempted data insertion by the present inventors using random data insertion yielded similar rates. The described techniques may be invaluable to manufacturers seeking to support improvements in audio, video and multimedia quality improvements. These include multiple audio channel support, surround sound, compressed information on dynamic range, or any combination of these and similar data to improve quality. Unfortunately, this does little or nothing to protect the interests of copyright holders from unscrupulous pirates, as they attempt to create unmarked, perfect copies of copyrighted works.

The present invention also relates to copending patent applications

entitled "Staganographicc Method and Device"; "Method for Human-Assisted Random Key Generation and Application for Digital Watermark System"; and "Method for Stega-Cipher Protection of Computer Code" as mentioned above, specifically addressing the weakness of inserting informational signals or digital watermarks into known locations or known frequency ranges, which are sub-audible. The present invention seeks to improve on the methods disclosed in these patent applications and other methods by describing specific optimization techniques at the disposal of those skilled in the art. These techniques provide an a la carte method for rethinking error correction, interleaving, digital and analog filters, noise shaping, nonlinear random location mapping in digitized samples, hashing, or making unique individual watermarks, localized noise signal mimic encoding to defeat noise filtering over the entire sample stream, super audible spread spectrum techniques, watermark inversion, preanalyzing watermark key noise signatures, and derivative analysis of suspect samples against original masters to evaluate the existence of watermarks with statistical techniques.

The goal of a digital watermark system is to insert a given information signal or signals in such a manner as to leave few or no artifacts in the underlying content signal, while maximizing its encoding level and location sensitivity in the signal to force damage to the content signal when removal is attempted. The present invention establishes methods for estimating and utilizing parameters, given principles of the digitization of multimedia content (audio, video, virtual reality, etc.), to create an optimized "envelope" for insertion of watermarks, and thus establish secured responsibility for digitally sampled content. The pseudo-random key that is generated is the only map to access the information signal while not compromising the quality of the content. A digital watermark naturally resists attempts at removal because it exists as purely random or pseudo-random noise in a given digitized sample. At the same time, inversion techniques and mimicking operations, as well as encoding signal features instead of given

samples, can make the removal of each and every unique encoded watermark in a given content signal economically infeasible (given the potential commercial returns of the life of a given copyright) or impossible without significantly degrading the quality of the underlying, "protected" signal. Lacking this aesthetic quality, the marketability or commercial value of the copy is correspondingly reduced.

The present invention preserves quality of underlying content signals, while using methods for quantifying this quality to identify and highlight advantageous locations for the insertion of digital watermarks.

The present invention integrates the watermark, an information signal, as closely as possible to the content signal, at a maximal level, to force degradation of the content signal when attempts are made to remove the watermarks.

General methods for watermarking digitized content, as well as computer code, are described in copending related patent applications entitled "Steganographic Method and Device" and entitled "Method for Stega-Cipher Protection of Computer Code", both assigned to the present assignee. Recognizing the importance of perceptual encoding of watermarks by the authors and engineers who actually create content is addressed in copending related application entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System".

The present invention describes methods of random noise creation given the necessary consequence of improving signal quality with digitization techniques. Additionally, methods are described for optimizing projections of data redundancy and overhead in error correction methods to better define and generate parameters by which a watermarking system can successfully create random keys and watermark messages that subsequently cannot be located and erased without possession of the key that acts as the map for finding each encoded watermark. This description will provide the backdrop for establishing truly optimized watermark

insertion including: use of nonlinear (chaotic) generators; error correction and data redundancy analysis to establish a system for optimizing key and watermark message length; and more general issues regarding desired quality relating to the importance of subjecting watermarked content to different models when the content may be distributed or sold in a number of prerecorded media formats or transmitted via different electronic transmission systems; this includes the use of perceptual coding; particularized methods such as noise shaping; evaluating watermark noise signatures for predictability; localized noise function mimic encoding; encoding signal features; randomizing time to sample encoding of watermarks; and, finally, a statistical method for analyzing composite watermarked content against a master sample content to allow watermark recovery. All of these features can be incorporated into specialized digital signal processing microprocessors to apply watermarks to nongeneralized computing devices, such as set-top boxes, video recorders that require time stamping or authentication, digital video disc (DVD) machines and a multitude of other mechanisms that play or record copyrighted content.

The sampling theorem, known specifically as the Nyquist Theorem, proves that bandlimited signals can be sampled, stored, processed, transmitted, reconstructed, desampled or processed as discrete values. In order for the theorem to hold true, the sampling must be done at a frequency that is at least twice the frequency of the highest signal frequency to be captured and reproduced. Aliasing will occur as a form of signal fold over, if the signal contains components above the Nyquist frequency. To establish the highest possible quality in a digital signal, aliasing is prevented by low-pass filtering the input signal to a given digitization system by a low-pass or anti-aliasing filter. Any residue aliasing which may result in signal distortion, relates to another area of signal quality control, namely, quantization error removal.

Quantization is required in a digitization system. Because of the continuous nature of an analog signal (amplitude vs. time), a quantized

sample of the signal is an imperfect estimate of the signal sample used to encode it as a series of discrete integers. These numbers are merely estimates of the true value of the signal amplitude. The difference between the true analog value at a discrete time and the quantization value is the quantization error. The more bits allowed per sample, the greater the accuracy of estimation; however, errors still always will occur. It is the recurrent nature of quantization errors that provides an analogy with the location of digital watermarks.

Thus, methods for removal of quantization errors have relevance in methods for determining the most secure locations for placement of watermarks to prevent the removal of such watermarks.

The highest fidelity in digital reproduction of a signal occurs at points where the analog signal converges with a given quantization interval. Where there is no such convergence, in varying degrees, the quantization error will be represented by the following range:

+Q /2 and -Q/2, where Q is the quantization interval.

Indeed, describing maximization of the quantization error and its ratio with the maximum signal amplitude, as measured, will yield a signal-to-error ratio (S/E) which is closely related to the analog signal-to-noise ratio (S/N). To establish more precise boundaries for determining the S/E, with root mean square (rms) quantization error E_{rms}, and assuming a uniform probability density function 1/Q (amplitude), the following describes the error:

$E_{rms}=Q/(12)^{½}$

Signal to quantization error is expressed as:

$S/E=[S_{rms}/E_{rms}]^2=3/2(2^{2n})$

Finally, in decibels (dB) and comparing 16-bit and 15-bit quantization:

$S/E(dB)=10\log[3/2(2^{2n})]=10\log 3/2+2^n\log 2$

(or "$= 20\log [(3/2)^{½} (2^n)]$")

$=6.02n+1.76$

This explains the S/E ratio of 98 dB for 16-bit and 92 dB for 15-bit quantization. The 1.76 factor is established statistically as a result of peak-to-rms ratio of a sinusoidal waveform, but the factor will differ if the signal waveform differs. In complex audio signals, any distortion will exist as white noise across the audible range. Low amplitude signals may alternatively suffer from distortion.

Quantization distortion is directly related with the original signal and is thus contained in the output signal, it is not simply an error. This being the case, implementation of so-called quality control of the signal must use dither. As discussed above, dither is a method of adding random noise to the signal to de-correlate quantization error from the signal while reducing the audibility of the remaining noise. Distortion may be removed at the cost of adding more noise to the filtered output signal. An important effect is the subsequent randomization of the quantization error while still leaving an envelope of an unremovable signaling band of noise. Dither, done at low signal levels, effects only the least significant bits of the samples.

Use of linear and nonlinear quantization can effect the trade-off in the output signal and must be considered for a system of watermarks designed to determine acceptable quantization distortion to contain the digital watermark. For audio systems, block linear quantization implementations have been chosen. However, block floating point and floating point systems, nonuniform companding, adaptive delta modulation, adaptive differential pulse-code modulation, and perceptual coding schemes (which are oriented around the design of filters that closely match the actual perception of humans) appear to provide alternative method implementations that would cause higher perceptible noise artifacts if filtering for watermarks was undertaken by pirates. The choice of method is related to the information overhead desired.

According to one aspect of the present invention, the envelope described in the quantization equations above is suitable for preanalysis of a digitized sample to evaluate optimal locations for watermarks. The

present example is for audio, but corresponding applications for digitization of video would be apparent in the quantization of color frequencies.

The matter of dither complicates preanalysis of a sample evaluated for digital watermarks. Therefore, the present invention also defines the optimal envelope more closely given the three types of dither (this example is for audio, others exist for video): triangular probability density function (pdf), Gaussian pdf, and rectangular pdf. Again, to establish better boundaries for the random or pseudo-random insertion of a watermark to exist in a region of a content signal that would represent an area for hiding watermarks in a manner most likely to cause damage to the content signal if unauthorized searches or removal are undertaken. Dither makes removal of quantization error more economical through lower data overhead in a system by shifting the signal range to decorrelate errors from the underlying signal. When dither is used, the dither noise and signal are quantized together to randomize the error. Dither which is subtractive requires removing the dither signal after requantization and creates total error statistical independence. It would also provide further parameters for digital watermark insertion given the ultimate removal of the dither signal before finalizing the production of the content signal. With nonsubtractive dither, the dither signal is permanently left in the content signal. Errors would not be independent between samples. For this reason, further analysis with the three types of dither should reveal an acceptable dither signal without materially affecting the signal quality.

Some proposed systems for implementing copyright protection into digitally-sampled content, such as that proposed by Digimarc Corporation, predicate the natural occurrence of artifacts that cannot be removed. Methods for creating a digital signature in the minimized error that is evident, as demonstrated by explanations of dither, point out another significant improvement over the art in the system described in the present invention and its antecedents. Every attempt is made to raise the error level of error from LSBs to a level at which erasure necessarily leads to the

degradation of the "protected" content signal. Furthermore, with such a system, pirates are forced to make guesses, and then changes, at a high enough encoding level over a maximum amount of the content signal so as to cause signal degradation, because guessing naturally introduces error. Thus, dither affects the present invention's envelope by establishing a minimum encoding level. Any encoding done below the dither level might be erased by the dither.

One embodiment of the present invention may be viewed as the provision of a random-super-level non-subtractive dither which contains information (the digital watermark).

To facilitate understanding of how this does not cause audible artifacts, consider the meaning of such encoding in terms of the S/E ratio. In a normal 16-bit signal, there is a 98 dB S/E according to the equation S/E = 6.02n + 1.76. Consider that the encoding of watermark information looks like any other error, except it moves beyond the quantization level, out of the LSBs. If the error is of a magnitude expressed in, say, 8 bits, then at that moment, the signal effectively drops to 8 bits (16-8). This corresponds to a momentary drop in S/E, referred to herein as the momentary S/E. Yet, these errors are relatively few and far between and therefore, since the signal is otherwise comprised of higher-bit samples, a "Perceived S/E" may be derived which is simply the weighted average of the samples using the "Pure S/E" (the samples without watermark information) and those with the Momentary S/E. As a direct consequence, it may be observed that the more sparse the watermark map, the fewer errors introduced in a given range, and the higher the perceived S/E. It also helps that the error is random, and so over time, appears as white noise, which is relatively unobtrusive. In general, it is observed that as long as introduced errors leave resulting samples within an envelope in the sample window described by minimum and maximum values, before error introduction, and the map is sufficiently sparse, the effects are not perceived.

In addition, it is possible to obtain an even higher Perceived S/E by allowing the range of introduced errors to vary between a minimum and maximum amount. This makes the weighted average S/E higher by reducing the average introduced error level. Yet, someone trying to erase a watermark, assuming they knew the maximum level, would have to erase at that level throughout the data, since they would not know how the introduced level varies randomly, and would want to erase all watermarks.

A watermarking cipher could perform this operation and may also introduce the further step of local dither (or other noise) significantly above the quantization amplitude on a window by window basis randomly, to restrict total correlation between the watermark signal and the probability that it remains independent between samples, as with subtractive dither implementations that are mostly concerned with the ultimate removal of the dither signal with requantization. This ability could be used to accomplish signal doping, which adds a degree of random errors that do not contain watermark information so as to prevent differential analysis of multiple watermarked copies. Alternatively, it could be used to mimic a specific noise function in a segment of the signal in order to defeat attempts to filter a particular type of noise over the entire signal. By varying this function between watermarks, it may be guaranteed that any particular filter is of no use over the whole signal. By applying several filters in series, it seems intuitive that the net results would be significantly different from the original signal.

The discussion may be more appropriately introduced with perceptual coding techniques, but a watermarking system could also defeat some detection and correction with dither by inserting watermarks into signal features, instead of signal samples. This would be equivalent to looking for signal characteristics, independent of the overall sample as it exists as a composite of a number of signals. Basically, instead of encoding on a bit per sample basis, one might spread bits over several samples. The point of doing this is that filtering and convolution operations, like "flanging", which

definitely change individual samples on a large scale, might leave intact enough of a recognizable overall signal structure (the relationship between multiple samples) to preserve the watermark information. This may be done by measuring, generalizing, and altering features determined by the relationships between samples or frequency bands. Because quantization is strictly an art of approximation, signal-to-error ratios, and thus the dynamic range of a given system are determined.

The choice of eliminating quantization distortion at the expense of leaving artifacts (not perceptible) is a permanent trade-off evident in all digitization systems which are necessarily based on approximation (the design goal of the present invention in preanalyzing a signal to mask the digital watermarks make imperceptibility possible). The high fidelity of duplication and thus subsequent ability to digitally or electronically transmit the finished content (signal) is favored by consumers and artists alike. Moreover, where there continues to be a question of approximating in quantization-- digital watermark systems will have a natural partner in seeking optimized envelopes in the multitude and variety of created digitized content.

Another aspect of optimizing the insertion of digital watermarks regards error correction. Highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks. A detailed description follows from the nature of a digitization system-- binary data can be corrected or concealed when errors exist. Random bit errors and burst errors differ in their occurrence:

Random bit errors are error bits occurring in a random manner, whereas burst errors may exist over large sequences of the binary data comprising a digitized signal. Outside the scope of the present invention are errors caused by physical objects, such as dust and fingerprints, that contribute to the creation of dropouts are different from the errors addressed herein.

Measuring error with bit-error ratio (BER), block error ratio (BLER) and burst-error length (BERL), however, provides the basis of error correction. Redundancy of data is a focus of the present invention. This data necessarily relies on existing data, the underlying content. To efficiently describe optimal parameters for generating a cryptographic key and the digital watermark message discussion of error correction and error concealment techniques is important.

Forms of error detection include one-bit parity, relying on the mathematical ability to cast out numbers, for binary systems including digitization systems, such as 2. Remainders given odd or even results (parity) that are probablistically determined to be errors in the data. For more appropriate error detection algorithms, such as Cyclic Redundancy Check Code (CRCC), which are suited for the detection of commonly occurring burst error. Pohlmann (Principles of Digital Audio) notes the high accuracy of CRCC (99.99%) and the truth of the following statements given a k-bit data word with m bits of CRCC, a code word of n bits is formed (m=n-k):

- burst errors less than or equal to m bits are always predictable.
- the detection probability of burst errors of m+1 bits = $1-2^{-m+1}$.
- the detection probability of burst errors longer than m+1 bits = $1-2^{-m}$
- random errors up to 3 consecutive bits long can be detected.

The medium of content delivery, however, provides the ultimate floor for CRCC design and the remainder of the error correction system.

Error correction techniques can be broken into three categories: methods for algebraic block codes, probablistic methods for convolutional codes, and cross-interleave code where block codes are used in a convolution structure. As previously discussed, the general class of codes that assist in pointing out the location of error are known generally as Hamming codes, versus CRCC which is a linear block code.

What is important for establishing parameters for determining optimized error coding in systems such as digital audio are more specifically known as Reed-Solomon Codes which are effective methods for correcting burst errors. Certain embodiments of the present invention presuppose the necessity of highly redundant error codes and interleaving, such as that done in Cross Interleave Reed-Solomon Code, to counter burst errors typically resulting from randomization attacks. More generally, certain embodiments of the present invention include the use of Hamming Codes of (n,n) to provide n-1 bit error detection and n-2 bit error correction. Further, a Hamming distance of n (or greater than n) is significant because of the nature of randomization attacks. Such an attack seeks to randomize the bits of the watermark message. A bit can be either 0 or 1, so any random change has a 50% chance of actually changing a bit from what it was (50% is indicative of perfect randomness). Therefore, one must assume that a good attack will change approximately half the bits (50%). A Hamming distance of n or greater, affords redundancy on a close par with such randomization. In other words, even if half the bits are changed, it would still be possible to recover the message.

Because interleaving and parity makes data robust for error avoidance, certain embodiments of the present invention seek to perform time interleaving to randomly boost momentary S/E ratio and give a better estimate of not removing keys and watermarks that may be subsequently determined to be "errors."

Given a particular digital content signal, parity, interleaving, delay, and cross-interleaving, used for error correction, should be taken into account when preprocessing information to compute absolute size requirements of the encoded bit stream and limiting or adjusting key size parameters to optimize and perhaps further randomize usage of key bits. In addition, these techniques minimize the impact of errors and are thus valuable in creating robust watermarks.

Uncorrected errors can be concealed in digital systems. Concealment offers a different dynamic to establish insertion parameters for the present invention. Error concealment techniques exist because it is generally more economical to hide some errors instead of requiring overly expensive encoders and decoders and huge information overheads in digitization systems. Muting, interpolation, and methods for signal restoration (removal of noise) relate to methods suggested by the present invention to invert some percentage or number of watermarks so as to ensure that at least some or as many as half of the watermarks must still remain in the content signal to effectively eliminate the other half. Given that a recording contains noise, whether due to watermarks or not, a restoration which "removes" such noise is likely to result in the changing of some bit of the watermark message. Therefore, by inverting every other watermark, it is possible to insure that the very act of such corrections inverts enough watermark bits to create an inverse watermark. This inversion presupposes that the optimized watermark insertion is not truly optimal, given the will of a determined pirate to remove watermarks from particularly valuable content. Ultimately, the inability to resell or openly trade unwatermarked content will help enforce, as well as dictate, the necessity of watermarked content for legal transactions.

The mechanisms discussed above reach physical limits as the intent of signal filtering and error correction are ultimately determined to be effective by humans-- decidedly analog creatures. All output devices are thus also analog for playback.

The present invention allows for a preprocessed and preanalyzed signal stream and watermark data to be computed to describe an optimized envelope for the insertion of digital watermarks and creation of a pseudo-random key, for a given digitized sample stream. Randomizing the time variable in evaluating discrete sample frames of the content signal to introduce another aspect of randomization could further the successful insertion of a watermark. More importantly, aspects of perceptual coding

are suitable for methods of digital watermarks or super-audible spread spectrum techniques that improve on the art described by the Preuss et al. patent described above.

The basis for a perceptual coding system, for audio, is psychoacoustics and the analysis of only what the human ear is able to perceive. Similar analysis is conducted for video systems, and some may argue abused, with such approaches as "subliminal seduction" in advertising campaigns. Using the human for design goals is vastly different than describing mathematical or theoretical parameters for watermarks. On some level of digital watermark technology, the two approaches may actually complement each other and provide for a truly optimized model.

The following example applies to audio applications. However, this example and other examples provided herein are relevant to video systems as well as audio systems. Where a human ear can discern between energy inside and outside the "critical band," (described by Harvey Fletcher) masking can be achieved. This is particularly important as quantization noise can be made imperceptible with perceptual coders given the maintenance of a sampling frequency, decreased word length (data) based on signaling conditions. This is contrasted with the necessary decrease of 6 dB/bit with decreases in the sampling frequency as described above in the explanation of the Nyquist Theorem. Indeed, data quantity can be reduced by 75%. This is an extremely important variable to feed into the preprocessor that evaluates the signal in advance of "imprinting" the digital watermark.

In multichannel systems, such as MPEG-1, AC-3 and other compression schemes, the data requirement (bits) is proportional to the square root of the number of channels. What is accomplished is masking that is nonexistent perceptually, only acoustically.

Taken to another level for digital watermarking, which is necessary for content that may be compressed and decompressed, forward adaptive

allocation of bits and backward adaptive allocation provide for encoding signals into content signals in a manner such that information can be conveyed in the transmission of a given content signal that is subsequently decoded to convey the relatively same audible signal to a signal that carries all of its bits-- e.g., no perceptual differences between two signals that differ in bit size. This coding technique must also be preanalyzed to determine the most likely sample bits, or signal components, that will exist in the smaller sized signal. This is also clearly a means to remove digital watermarks placed into LSBs, especially when they do not contribute theoretically perceptible value to the analyzed signal. Further methods for data reduction coding are similarly important for preanalyzing a given content signal prior to watermarking. Frequency domain coders such as subband and transform bands can achieve data reduction of ratios between 4:1 and 12:1. The coders adaptively quantize samples in each subband based on the masking threshold in that subband (See Pohlmann, Principles of Digital Audio). Transform coders, however, convert time domain samples into the frequency domain for accomplishing lossless compression. Hybrid coders combine both subband and transform coding, again with the ultimate goal of reducing the overall amount of data in a given content signal without loss of perceptible quality.

With digital watermarks, descriptive analysis of an information signal is important to preanalyze a given watermark's noise signature. Analysis of this signature versus the preanalysis of the target content signal for optimized insertion location and key/message length, are potentially important components to the overall implementation of a secure watermark. It is important that the noise signature of a digital watermark be unpredictable without the pseudo-random key used to encode it. Noise shaping, thus, has important applications in the implementation of the present invention. In fact, adaptive dither signals can be designed to correlate with a signal so as to mask the additional noise-- in this case a digital watermark. This relates to the above discussion of buried data

techniques and becomes independently important for digital watermark systems. Each instance of a watermark, where many are added to a given content signal given the size of the content and the size of the watermark message, can be "noise shaped" and the binary description of the watermark signature may be made unique by "hashing" the data that comprises the watermark. Generally, hashing the watermark certificate prior to insertion is recommended to establish differences between the data in each and every watermark "file."

Additionally, the present invention provides a framework in which to analyze a composite content signal that is suspected to contain a watermarked sample of a copyrighted work, against an unwatermarked original master of the same sample to determine if the composite content actually contains a copy of a previously watermarked content signal. Such an analysis may be accomplished in the following scenario:

- Assume the composite signal contains a watermark from the sample.

- Assume the provision of the suspect composite signal $C_w(t)$ (w subscript denotes a possible watermark) and the unwatermarked original sample $S_{uw}(t)$. These are the only two recordings the analyzer is likely to have access to.

Now, it is necessary to recover a watermarked sample $S_w(t)$.

The methods of digital signal processing allow for the computation of an optimal estimate of a signal. The signal to be estimated is the composite minus the watermarked sample, or $C''_w(t) = C_w(t) - S_w(t)$. The analyzer, however, cannot determine a value of $S_w(t)$, since it does not know which of the many possible $S_w(t)$ signals was used in the composite. However, a close estimate may be obtained by using $S_{uw}(t)$, since watermarking makes relatively minor changes to a signal.

So, $C''_w(t)$ (an estimate of $C'_w(t)$ given $C_w(t)$ and $S_{uw}(t)$) may be obtained. Once $C''_w(t)$ is calculated, it is simply subtracted from $C_w(t)$. This yields $S'_w(t) = C_w(t) - C''_w(t)$. If the watermark is robust enough, and the estimate good enough,

then $S'_w(t)$, which is approximately equal to $S_w(t)$, can be processed to extract the watermark. It is simply a matter of attempting watermark decoding against a set of likely encoding key candidates.

Note that although a watermark is initially suspected to be present in the composite, and the process as if it is, the specifics of the watermark are not known, and a watermark is never introduced into the calculations, so a watermark is extracted, it is valid, since it was not introduced by the signal processing operations.

The usefulness of this type of operation is demonstrated in the following scenario:

People are interested in simply proving that their copyrighted sample was dubbed into another recording, not the specifics of ownership of the sample used in the dubbing. So, this implies that only a single, or limited number of watermark keys would be used to mark samples, and hence, the decode key candidates are limited, since the same key would be used to encode simple copyright information which never varies from copy to copy.

There are some problems to solve to accomplish this sort of processing. The sample in question is generally of shorter duration than the composite, and its amplitude may be different from the original. Analysis techniques could use a combination of human-assisted alignment in the time domain, where graphical frequency analysis can indicate the temporal location of a signal which closely matches that of the original sample. In addition, automatic time warping algorithms which time align separate signals, on the assumption they are similar could also be used to solve temporal problems. Finally, once temporal alignment is accomplished, automatic amplitude adjustment could be performed on the original sample to provide an optimal match between the composite section containing the sample and the original sample.

It may be desirable to dynamically vary the encoding/decoding algorithm during the course of encoding/decoding a signal stream with a given watermark. There are two reasons for dynamically varying the encoding/decoding algorithm.

The first reason for dynamically varying the encoding/decoding algorithm is that the characteristics of the signal stream may change between one locality in the stream and another locality in the stream in a way that significantly changes the effects that a given encoding algorithm may have on the perception of that section of the stream on playback. In other words, one may want the encoding algorithm, and by implication, the decoding algorithm, to adapt to changes in the signal stream characteristics that cause relative changes in the effects of the encoding algorithm, so that the encoding process as a whole causes fewer artifacts, while maintaining a certain level of security or encoding a given amount of information.

The second reason for dynamically varying the encoding/decoding algorithm is simply to make more difficult attempts at decoding watermarks without keys. It is obviously a more difficult job to attempt such attacks if the encoding algorithm has been varied. This would require the attacker to guess the correct order in which to use various decoding algorithms.

In addition, other reasons for varying the encoding/decoding algorithms may arise in the future.

Two methods for varying of the encoding/decoding algorithms according to embodiments of the present invention are described herein. The first method corresponded to adaptation to changing signal characteristics. This method requires a continuous analysis of the sample windows comprising the signal stream as passed to the framework. Based on these characteristics, which are mathematically well-defined functions of the sample stream (such as RMS energy, RMS/peak ratio, RMS difference between samples - which could reflect a measure of distortion), a new CODEC module, from among a list of pre-defined CODECs, and the algorithms implemented in them, can be applied to the window in question. For the purpose of this discussion, windows are assumed to be equivalent to frames. And, in a frame-based system, this is a straightforward application of the architecture to provide automated variance of algorithms to encode and decode a single watermark.

The second method for varying of the encoding/decoding algorithms corresponds to increased security. This method is easier, since it does not require the relatively computationally-expensive process of further analyzing the samples in a frame passed to the Framework. In this method, the Framework selects a new CODEC, from among a list of pre-defined CODECs, to which to pass the sample frame as a function of the pseudo-random key employed to encode/decode the watermark. Again, this is a straightforward application of framework architecture which provides automated variance of algorithms to encode and decode a single watermark versus limitations evident in the analysis of a single random noise signal inserted over the entire content signal as proposed by Digimarc, NEC, Thorn EMI and IBM under the general guise of spread spectrum, embedded signalling schemes.

It is important to note that the modular framework architecture, in which various modules including CODECs are linked to keys, provides a basic method by which the user can manually accomplish such algorithmic variations for independent watermarks. The main difference detailed above is that an automated method to accomplish this can be used within single watermarks.

Automated analysis of composited copyrighted material offers obvious advantages over subjective "human listening" and "human viewing" methods currently used in copyright infringement cases pursued in the courts.

DISH-Blue Spike-842
Exhibit 1004, Page 1395

What Is Claimed Is:

1. A method for amplitude independent encoding of digital watermark information in a signal, comprising steps of:

determining in said signal a sample window having a minimum and a maximum;

determining a quantization interval of said sample window, where said quantitization interval can be used to quantize normalized window samples;

normalizing the sample window to provide normalized samples, where normalized samples conform to a limited range of values, proportional to real sample values, and comprise a representation of the real sample values with a resolution higher than the real range of values, and where the normalized values can be divided by the quantization interval into distinct quantization levels;

analyzing the normalized samples to determine quantization levels;

comparing the message bits to the corresponding quantization level information from the analyzing step;

when a bit conflicts with the quantization level, adjusting the quantization level of said sample window to correspond to the message bit; and

de-normalizing the analyzed normalized samples.

2. The method according to claim 1, wherein watermark signal characteristics or a watermark certificate can be compressed.

3. A method for amplitude independent decoding of digital watermark information in a signal comprising steps of:

determining in said signal a sample window having a minimum and a maximum;

determining a quantization interval of said sample window, where said quantitization interval can be used to quantize normalized window samples;

normalizing the sample window to provide samples, where normalized samples conform to a limited range of values, proportional to real sample values, and comprise a representation of the real sample values with a resolution higher than the real range of values, and where the normalized values can be divided by the quantization interval into distinct quantization levels; and

analyzing the quantization level of said samples to determine a message bit value.

4. The method according to claim 3, wherein watermark signal characteristics or a watermark certificate can be compressed.

5. A method of encoding and decoding watermarks in a signal, comprising insertion and detection of abstract signal features in said signal to carry watermark information, wherein said abstract signal features are mathematical functions of the input sample window, and by extension, adjacent sample windows.

6. A method of pre-analyzing a digital signal for encoding digital watermarks using a digital filter comprising determining what changes in the digital signal will be affected by the digital filter.

7. The method according to claim 6, further comprising a step of encoding watermarks so as to either avoid frequency or time delimited areas of the signal which will be changed by the digital filter, or ensure that the watermark will survive the changes instroduced by the digital filter.

8. A method of error coding watermark message certificates using cross interleaved codes which use error codes of high redundancy, including codes with Hamming distances of greater than or equal to n, wherein is a number of bits in a message block.

DISH-Blue Spike-842
Exhibit 1004, Page 1397

9. A method of pre-processing a watermark message certificate comprising determining an exact length of the watermark message as it will be encoded.

10. The method according to claim 9, further comprising a step of generating a watermark key which will provide at least one unique bit for each bit comprising the watermark message.

11. A method of generating watermark pseudo-random key bits using a non-linear generator.

12. A method of generating watermark pseudo-random key bits using a chaotic generator.

13. A method of mapping pseudo-random key and processing state information to effect an encode / decode map using a non-linear generator.

14. A method of mapping pseudo-random key and processing state information to effect an encode / decode map using a chaotic generator.

15. A method of guaranteeing watermark certificate uniqueness comprising attaching a timestamp or user identification dependent hash or message digest of watermark certificate data to the certificate.

16. A method of generating and modulating a local noise signal to contain watermark information, wherein the noise signal is a function of at least one variable which depends on key and processing state information.

DISH-Blue Spike-842
Exhibit 1004, Page 1398