US006633653B1

(12) **United States Patent**
Hobson et al.

(10) **Patent No.: US 6,633,653 B1**
(45) **Date of Patent: Oct. 14, 2003**

(54) **WATERMARKED DIGITAL IMAGES**

(75) Inventors: **Paola Marcella Hobson**, Basingstoke (GB); **Lai Hock Tay**, London (GB)

(73) Assignee: **Motorola, Inc.**, Schaumburg, IL (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/499,048**

(22) Filed: **Feb. 4, 2000**

(30) **Foreign Application Priority Data**

Jun. 21, 1999 (GB) 9914384

(51) **Int. Cl.**[7] **G06K 9/00**
(52) **U.S. Cl.** **382/100**; 382/250
(58) **Field of Search** 382/100, 250

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,930,369 A * 7/1999 Cox et al. 283/113
6,285,775 B1 * 9/2001 Wu et al. 382/100

FOREIGN PATENT DOCUMENTS

EP 0 828 372 A2 3/1998

OTHER PUBLICATIONS

"Secure Spread Spectrum Watermarking for Multimedia" by Ingemar Cox et al. NEC Research Institute Technical Report 95–10 1995.*

"DCT–based Watermark Recovering without Resorting to the Uncorrupted Original Image" by A. Piva et al. IEEE Signal Processing Society 1997 International Conference on Image Processing.*

"Improved robust watermarking through attack characterization" by Deepa Kundur et al. Optics Express 485 1998.*

"Copyright protection of digital images by embedded unperceivable marks" by Mauro Barni et al. 1998.*

Fridrich J: "Robust Bit Extraction from Images"; Proceedings of the International Conference on Multimedia Computing and Systems, Jun. 1999, XP000939253, p. 536, right–hand column, line 35—p. 537, right–hand column, line 42.

Kundur D. et al.: "Attach Characterization for Effective Watermarking"; Kobe, Japan, Oct. 24–28, 1999, Los Alamitos, Ca: IEEE, US, Oct. 1999, pp. 240–244, XP000939230, ISBN: 0–7803–5468–0, p. 242, left–hand column, line 9–line 22.

Ruanaidh JJKO et al.: "Phase Watermarking of Digital Images" Proceedings of the International Conference on Image Processing (ICIP), US, New York, IEEE, Sep. 16, 1996, pp. 239–242, XP000199952, ISBN: 0–7803–3259–8 the whole document.

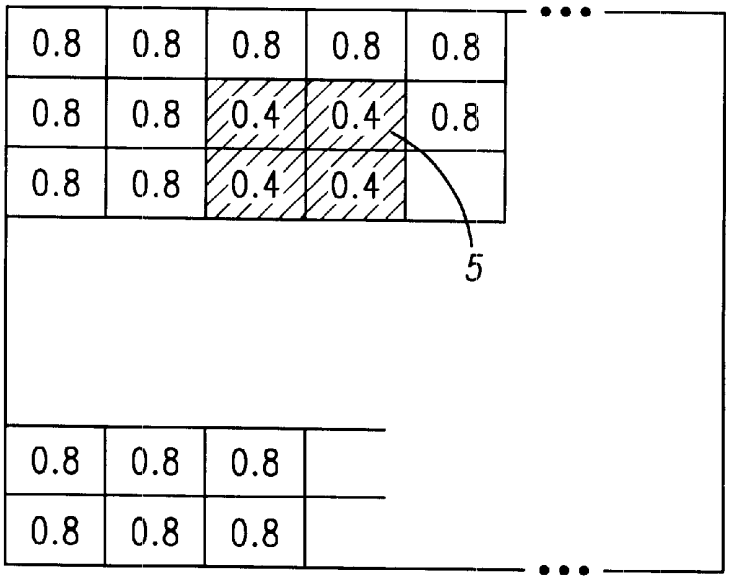
* cited by examiner

Primary Examiner—Jon Chang
Assistant Examiner—Charles Kim
(74) *Attorney, Agent, or Firm*—Steven R. Santema; Valerie M. Davis

(57) **ABSTRACT**

A tamper detection method for digital images includes: providing a digitally watermarked image; digitally processing at least some watermarked parts of the image to obtain confidence values; and using the confidence values to provide an indication as to the likelihood that the image has been tampered with.

4 Claims, 3 Drawing Sheets



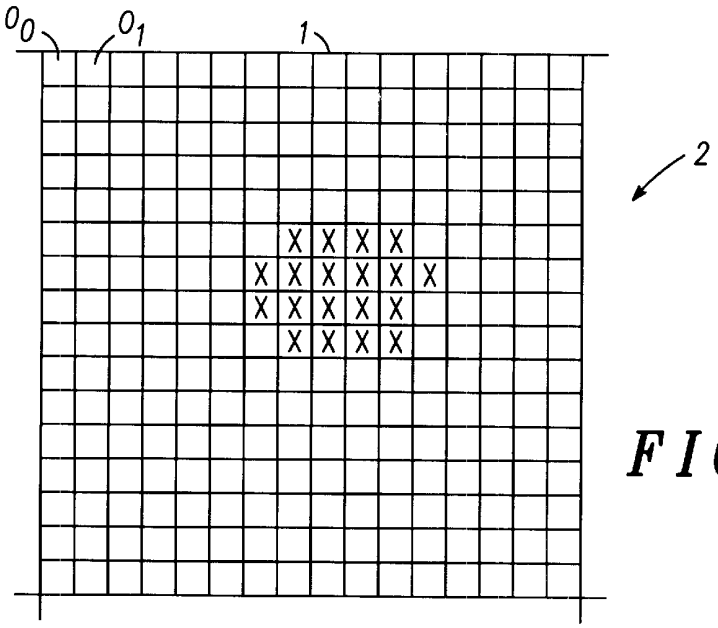


FIG. 1

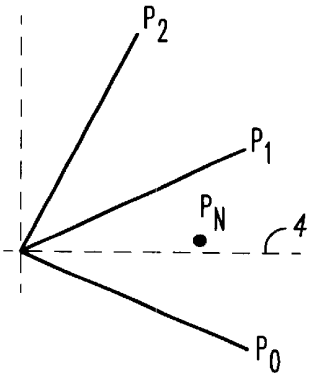


FIG. 3

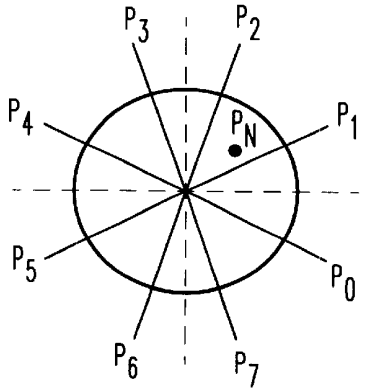


FIG. 2

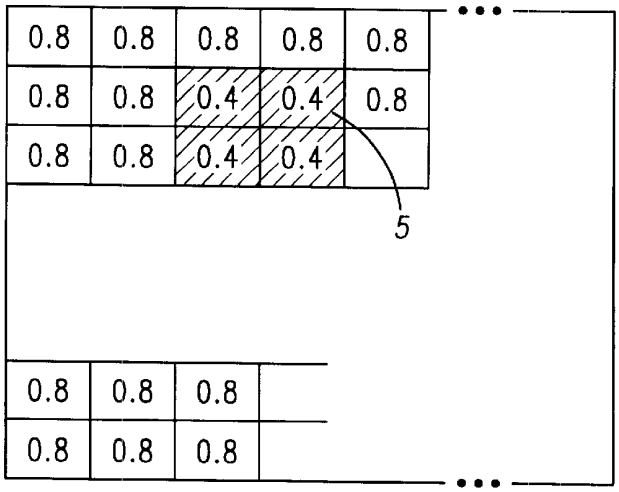


FIG. 4

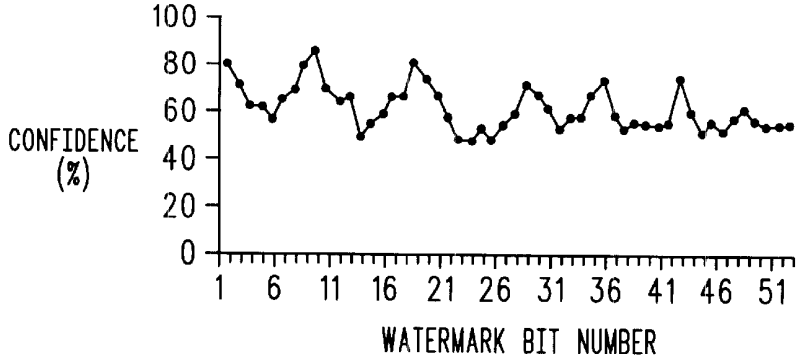


FIG. 5

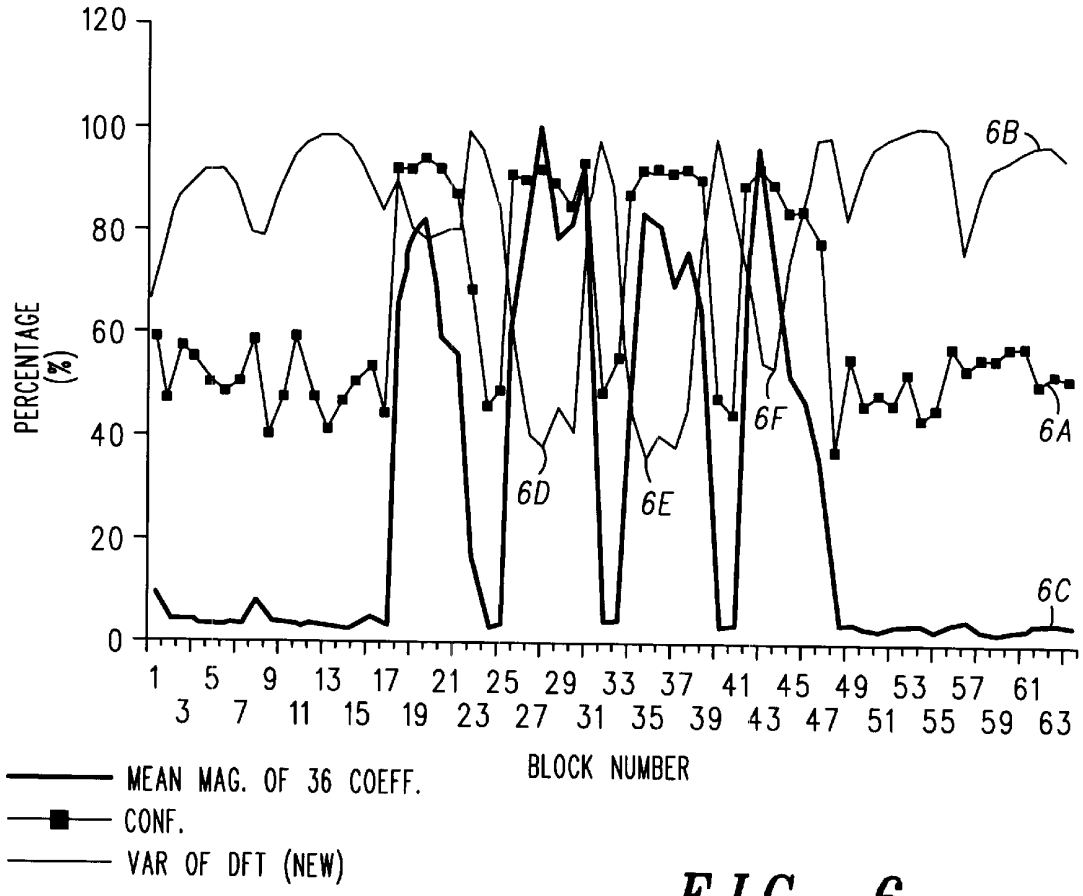


FIG. 6

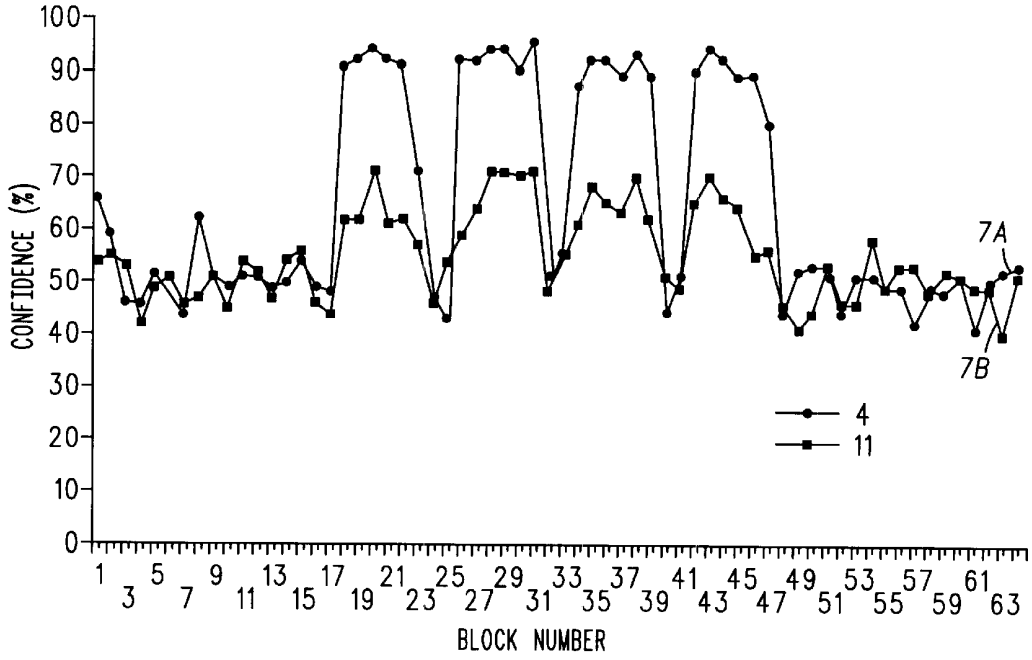


FIG. 7

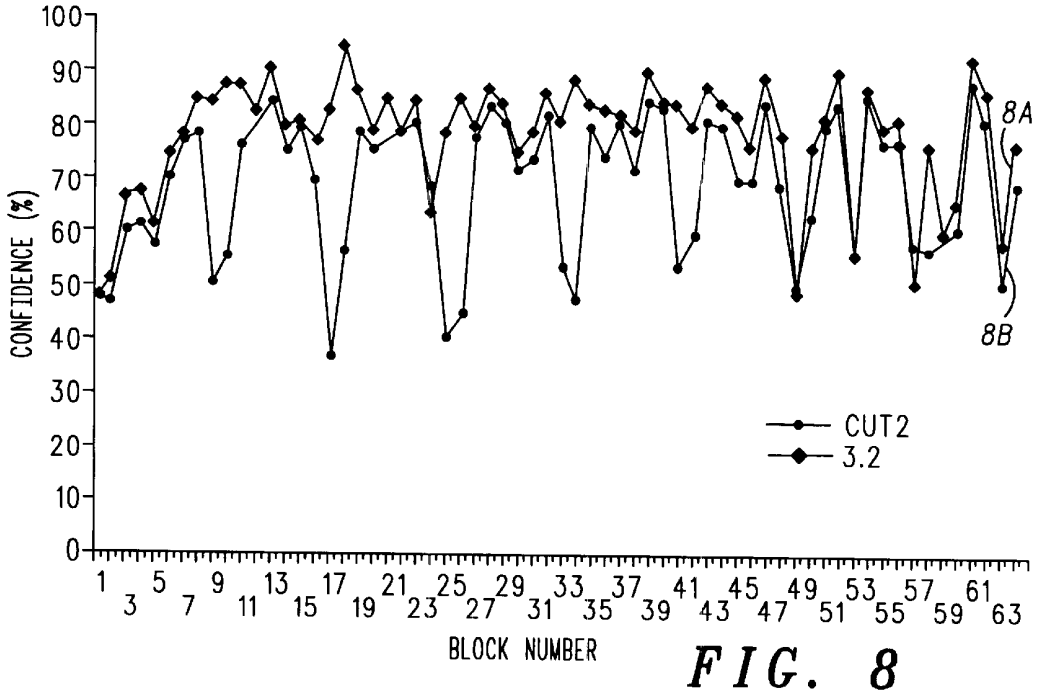


FIG. 8

WATERMARKED DIGITAL IMAGES

FIELD OF THE INVENTION

This invention relates to watermarked digital images. In particular, it relates to methods for improving confidence in and for authentication of watermarked digital images.

In order to increase confidence of use of digital images as evidence, possibly in a court of law, there is a significant need to demonstrate that an image has not been tampered with.

BACKGROUND OF THE INVENTION

It is known to use audit trails, in which information about when an image was processed is appended to the image, but these methods are only applicable once an image has been registered onto a system. Such audit trails therefore cannot detect any unauthorized operations prior to registration on a computer, and may not be able to report on the type of processing done at any one time. Audit trails can also be avoided or corrupted, whether deliberately or accidentally.

Image watermarking is a known technique. In this technique, a known binary pattern or signature is embedded into an image at the moment of image acquisition. Such watermarks are called "robust" because they are designed to remain intact regardless of any post-processing of the image such as filtering, cropping etc. While such watermarks do provide a useful degree of protection, they can at present not be wholly relied on and they cannot always possess the required degree of surety that an image has not been tampered with in order for the image to be used as evidence under the strict rules of courts of law, etc.

Ruanaidh, Dowling and Boland "Phase Watermarking of Digital Images", IEEE INTCONF Image Processing, Vol. 3, Lausanne, Switzerland, September 1996, pp 239 to 241, describes a technique for watermarking digital images in which an image is divided into blocks of a selected size (e.g. 16×16 pixels). A discrete Fourier transform (DFT) is applied to the luminance component of the image on a block by block basis. The DFT is a complex value and thereby generates a modulus and a phase. The resulting watermark comprises a binary string of 1's and 0's which may represent, for example, a company logo, a user authentication code, date/time/location information and so on. The watermark is embedded in the image by altering the phase of selected DFT coefficients.

The present invention arose in an attempt to provide an improved method of authenticating, and thereby improve confidence in, a watermarked image.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

FIG. **1** shows the DFT of a block forming part of an image;

FIG. **2** shows phase quantization levels for forming a watermark;

FIG. **3** shows a phase diagram on subsequent stage of verifying the watermark;

FIG. **4** shows confidence values across part of an image;

FIG. **5** shows variations in confidence value depending upon the bit position;

FIG. **6** is a plot of confidence values and DFT magnitude variance values;

FIG. **7** is a plot of confidence values for different JPEG compression regimes; and

FIG. **8** shows the effect on confidence of cutting and pasting part of an image.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

According to the present invention there is provided a tamper detection method for digital images, comprising providing a digitally watermarked image; digitally processing at least some watermarked parts of the image to obtain confidence values, and using the confidence values to provide an indication as to the likelihood that the image has been tampered with.

Preferably, a discrete Fourier transform is applied to the image on a block by block basis, and the watermark is applied to each one of a selected number of DFT coefficients within a block by selecting the phase of that DFT coefficient to be equal to the phase of one or other of a plurality of phase values, of a set of quantized phase values, which are closest to the actual phase dependent upon the value with which the watermarked bit is to be embedded, and wherein during recovery of the watermark, a discrete Fourier transform is again taken of each block and the watermark is recovered by determining which of the quantized set of levels the recovered bit phase data is closest to.

A confidence measure for each bit n of recovered phase P_n may be defined as

$$C_n = 1 - (2^* |P_x - P_n| / |P_x - P_y|)$$

where P_n is the recovered phase for bit n of the watermark, $\|$ denotes modulus, and P_x, P_y are the nearest reference phase levels, where P_x was chosen as the closest phase level.

Alternatively, the digital watermarking is done on blocks of the image of a predetermined size; wherein an amplitude value is added to, or from, an amplitude relating to each one of a number of selected pixels of the block, depending upon whether the value with which the watermarked bit is to be embedded, and wherein during recovery of the watermark, an estimate of the actual value is made, and wherein each confidence value is related to how close the recovered amplitude is to one or more of a quantized set of reference amplitude levels. The confidence measure C_n of each bit n may then be defined as

$$C_n = 1 - (2^* |A_x - A_n| / |A_x - A_y|)$$

wherein An is the recovered amplitude for bit n of the watermark, $\|$ denotes modulus, and A_x, A_y are the nearest reference amplitude levels, where A_x was chosen as the closest.

The watermark is preferably a binary code (i.e., the value can be 0 or 1) or may be other codes, in which each bit could be embedded with any of three, four or more values for example. This coding may be useful in the spatial domain but can also be used in the transform domain.

Embodiments of the invention will be described which use phase modulation types of image watermarking. However, it should be appreciated that the concepts of the present invention may be equally applied with other types of image processing, and particularly in the spatial domain in addition to the frequency or phase domain.

In a method in line with that used by Ruanaidh et al, an image is divided into blocks of desired size. These may be, for example, 16×16 pixels. A discrete Fourier transform (DFT) is applied to the luminance component of the image

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.