Docket No.: PMC-003C180

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: John C. Harvey *et al.*	
Application No.: 08/485,507	Confirmation No.: 5691
Filed: May 24, 1995	Art Unit: 2600
For: SIGNAL PROCESSING APPARATUS AND METHODS	Examiner: Groody, James J.

AMENDMENT AFTER FINAL REJECTION AND REQUEST FOR RECONSIDERATION

MS AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Office Action mailed August 2, 2011, ("Office Action" or "the Action") from the Patent and Trademark Office ("the Office") rejecting Claims 33-63, please amend the above-identified U.S. patent application as follows:

Amendment to the Claims are reflected in the listing of the claims that begins on page 2 of this paper.

Remarks begin on page 7.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

AMENDMENT TO THE CLAIMS

33. (Previously Presented) A method of inhibiting piracy of information or enabling a presentation of programming at a subscriber station, said method comprising the steps of:

receiving an information transmission from a first remote station;

detecting instruct-to-samp1e instructions in the information transmission;

processing, under control of said instruct-to-samp1e instructions, a datum at said subscriber station;

comparing, under control of said instruct-to-samp1e instructions, selected comparison information of said instruct-to-samp1e instructions to a selected sample of preprogrammed operating information at said subscriber station, said selected comparison information and said selected sample of preprogrammed operating information being selected based on said step of processing, whereby a successful match indicates that said subscriber station is properly programmed and a failed match suggests that said preprogrammed operating information at said subscriber station has been tampered with; and

performing, under control of said instruct-to-samp1e instructions, at said subscriber station at least one of the steps of:

(1) disabling the functionality of some portion of said subscriber station (i) when said step of comparing results in a determination that said subscriber station has been tampered with or (ii) when an instruction is executed based on said step of comparing and said subscriber station fails to respond in a predetermined fashion or within a predetermined period of time;

(2) communicating appearance-of-tampering information to a second remote station when said step of comparing results in a determination that said subscriber station has been tampered with; and

(3) enabling at least some of a programming presentation when said step of comparing results in a determination that said subscriber station is properly programmed.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

34. (Previously Presented) The method of claim 33, wherein said comparing step is performed under control of a selected subroutine of said instruct-to-sample instructions.

35. (Previously Presented) The method of claim 34, wherein said subscriber station selects said selected subroutine based on said step of processing.

36. (Previously Presented) The method of claim 35, wherein said datum comprises a station specific identifier.

37. (Previously Presented) The method of claim 36, wherein said subscriber station selects said station specific identifier.

38. (Previously Presented) The method of claim 33, wherein said step of performing includes said step of disabling and wherein said step of disabling includes erasing information from memory.

39. (Previously Presented) The method of claim 38, wherein a read only memory is disabled.

40. (Previously Presented) The method of claim 33, wherein said step of performing includes said step of disabling and wherein said step of disabling includes disabling a decryptor.

41. (Previously Presented) The method of claim 33, wherein said step of performing includes said step of communicating and wherein said step of communicating includes establishing telephone communications.

42. (Previously Presented) The method of claim 33, wherein said step of performing includes said step of communicating and wherein said step of communicating includes transmitting an identifier of said subscriber station to said second remote station.

43. (Previously Presented) The method of claim 33, wherein said step of comparing results in a determination that said subscriber station may have been tampered with and said subscriber station performs both of said steps of disabling and communicating.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

44. (Previously Presented) The method of claim 33, wherein said step of performing includes said step of enabling and wherein said step of enabling includes controlling a decryptor.

45. (**Currently Amended**) A method of decrypting programming at a receiver station, said method comprising the steps of:

receiving an information transmission including encrypted information;

detecting in said information transmission the presence of an instruct-to-enable signal;

passing said instruct-to-enable signal to a processor;

determining a fashion in which said receiver station locates a first decryption key by processing said instruct-to-enable signal;

locating said first decryption key based on said step of determining;

decrypting said encrypted information using said first decryption key; and

outputting said programming based on said step of decrypting.

46. (Previously Presented) The method of claim 45, further comprising the step of computing a second decryption key, and wherein said step of decrypting comprises decrypting said encrypted information using said first and second decryption keys.

47. (Previously Presented) The method of claim 46, wherein said first and second decryption keys are used to decrypt a video portion of said programming.

48. (Previously Presented) The method of claim 45, further comprising the step of storing information evidencing said step of decrypting.

49. (Previously Presented) The method of claim 45, further comprising the step of determining if said receiver station is decrypting said encrypted information correctly, and if not, communicating appearance-of-tampering information to a remote station.

50. (Previously Presented) The method of claim 45, wherein said encrypted information includes television programming.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

51. (Previously Presented) The method of claim 47, wherein a third decryption key is used to decrypt an audio portion of said programming, and said first decryption key is located based on decrypting said audio portion using said third decryption key.

52. (**Currently Amended**) A method of decrypting programming at a receiver station, said method comprising the steps of:

receiving an information transmission including encrypted information;

detecting in said information transmission the presence of a first instruct-to-enable signal including first processor instructions;

executing said first processor instructions of said first instruct-to-enable signal to provide a first decryption key;

detecting in said information transmission the presence of a second instruct-to-enable signal including second processor instructions;

executing said second processor instructions to provide a second decryption key;

decrypting said encrypted information using said first and second decryption keys; and

outputting said programming based on said step of decrypting.

53. (Previously Presented) The method as in claim 52, further comprising the step of storing information evidencing said step of decrypting.

54. (Previously Presented) The method as in claim 52, further comprising the step of determining if said receiver station is decrypting said encrypted information correctly, and if not, communicating appearance-of-tampering information to a remote station.

55. (Previously Presented) The method of claim 52, wherein said first and second decryption keys are used to decrypt a video portion of said programming.

56. (Previously Presented) The method of claim 52, wherein said encrypted information includes television programming.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

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.