(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 March 2005 (24.03.2005)

PCT

(10) International Publication Number
WO 2005/026960 A1

(51) International Patent Classification[7]: G06F 11/30, H04L 9/00, H04K 1/00, H04N 7/167

(21) International Application Number: PCT/US2004/029137

(22) International Filing Date: 8 September 2004 (08.09.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/657,822 8 September 2003 (08.09.2003) US

(71) Applicant *(for all designated States except US)*: **AIRCRAFT PROTECTIVE SYSTEMS, INC.** [US/US]; 1142 Broadway Plaza, Suite 400, Tacoma, WA 98402 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **HENSON, Robert, Ray** [US/US]; 21111 55th Avenue Court E, Spanaway, WA 98387 (US).

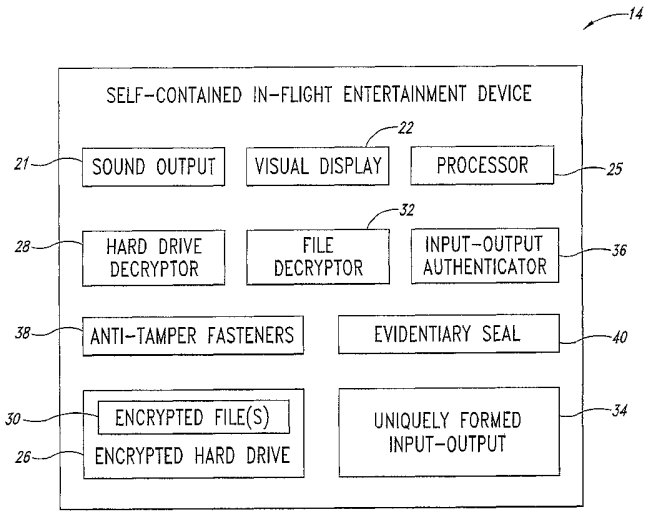
(74) Agents: **RONDEAU, Jr., George, C.** et al.; 2600 Century Square, 1501 Fourth Avenue, Seattle, WA 98101-1688 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH,

[Continued on next page]

(54) Title: SECURITY SYSTEM AND METHOD OF IN-FLIGHT ENTERTAINMENT DEVICE RENTALS HAVING SELF-CONTAINED AUDIOVISUAL PRESENTATIONS



(57) Abstract: The self-contained IFED (14) contains a processor (25), for interaction and control of various other components of the self-contained IFED (14). An encrypted hard drive (26) is included for storing one or more files containing current movies or other audiovisual presentations. The encrypted hard drive (26) is accessible thorough a hard drive decryptor (28) so that both encrypted files (30) containing current movies and other proprietary property and unencrypted files are protected by the encryption mechanisms associated directly with the encrypted hard drive. An input-output (34) of unique physical configuration is used to delete out-dated audiovisual presentations from the encrypted hard drive (26) and to transfer current movie releases and other audiovisual presentations to the encrypted hard drive. Anti-tamper fasteners (38) are used to physically secure the case of the self-contained IFED (14) together, thereby requiring a unique tool for physically accessing internal components of the self-contained IFED (14). An evidentiary seal (40) is used to seal an internal portion of the self-contained IFED (14). Camera artifacts are used to hinder illegal video recording taken of movies being displayed (22). During encryption, a unique key for decryption is generated for each individual file, which is required for subsequent playing of the file and is handled by the file decrypt (32) of the self-contained IFED (14). Also, the input-output (34) uses protocols that require authorization through the input-output authenticator (36) to occur within a limited window of time otherwise physical reconnection to the input-output is necessary for further access attempts.

WO 2005/026960 A1

GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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 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.

SECURITY SYSTEM AND METHOD OF IN-FLIGHT ENTERTAINMENT DEVICE RENTALS HAVING SELF-CONTAINED AUDIOVISUAL PRESENTATIONS

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention is directed generally to security measures for electronic devices and, more particularly, to security measures for entertainment devices having self-contained audiovisual presentations for rent to passengers of conveyances such as commercial airline flights.

Description of the Related Art

Rental of entertainment devices having self-contained audiovisual presentations to be used by passengers during a commercial airline flight can provide individually tailored current entertainment and other services to the passengers during the commercial flight. Unfortunately, conventional security measures for electronic devices generally afford an insufficient degree of protection from theft of the valuable audiovisual (A/V) properties that would be stored on the self-contained in-flight entertainment device. Without a level of security greater than conventional approaches, adoption of self-contained in-flight entertainment devices having current movies and other audiovisual presentations could suffer due to risks involved with allowing members of the general public to rent such devices. Consequently, prior support for their implementation has not been available.

BRIEF SUMMARY OF THE INVENTION

The present invention resides in a security system and method of in-flight entertainment device rentals having self-contained audiovisual presentations. Aspects include receiving an audiovisual master file from a movie recording studio or other organization containing an audiovisual presentation such as a to-be-released or recently released movie, the audiovisual master file being in a first encoded and compressed format. Aspects further include adding watermark characters to the encoded audiovisual master file, adding camera artifacts to the encoded audiovisual master file, encrypting the encoded audiovisual master file to create an encrypted

encoded audiovisual master file, generating keys associated with the encrypted encoded audiovisual master file for using in decoding the encrypted encoded audiovisual master file, and transmitting the encrypted encoded audiovisual master file and the associated keys to a distribution point host computer. Aspects further include loading the transmitted encrypted encoded audiovisual master file on the distribution point host computer, linking the distribution point host computer with a self-contained entertainment device and establishing bi-directional authentication between the distribution point host computer and the self-contained entertainment device through use, in part, of an input-output of the self-contained entertainment device, and after bi-directional authentication occurs, using the distribution point host computer to delete at least some of the previously loaded encrypted encoded audiovisual master files from the self-contained entertainment device. Aspects further include using the distribution point host computer to transfer the newly loaded encrypted encoded audiovisual master file and keys associated with the newly loaded encrypted encoded audiovisual master file to the self-contained entertainment device to which the distribution point host computer is linked without decryption of the newly loaded encrypted encoded audiovisual master file being transferred to the self-contained entertainment device; and storing the newly loaded encrypted encoded audiovisual master file and the keys associated with the newly loaded encrypted encoded audiovisual master file on an encrypted hard drive of the self-contained entertainment device to which the distribution point host computer is linked.

Other features and advantages of the invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S)

Figure 1 is a side-view of a passenger viewing an audiovisual presentation being presented by a representative self-contained in-flight entertainment device (IFED) rental while traveling during a commercial flight.

Figure 2 is a perspective view of the self-contained IFED of Figure 1.

Figure 3 is a schematic view of various elements of the self-contained IFED of Figure 2 including elements related to security of the one or more audiovisual files stored on the self-contained IFED.

Figure 4 is a schematic view of various levels of security associated with implementations of the IFED of Figure 2.

Figure 5 is a flow-chart of a method associated with security elements of the IFED of Figure 2.

DETAILED DESCRIPTION OF THE INVENTION

A security method and system of in-flight entertainment device (IFED) rentals having self-contained audiovisual presentations is disclosed herein. A self-contained IFED has internal storage configured to contain current releases of movies and other audiovisual presentations. According to implementations of the present system and method, the self-contained IFED can be rented by passengers of commercial airline flights for viewing of such movies and other audiovisual presentations during the flight. Use of the self-contained IFED provides a selection of audiovisual presentations from which the passengers renting the self-contained IFED can choose. This individualizes the selection opportunity provided to each passenger by the self-contained IFED and increases the potential for enjoyment by the passengers compared with conventional systems that display one audiovisual presentation to a large group of passengers with the passengers having no input on the particular audiovisual property being presented.

As shown in Figure 1, a passenger 10 while seated in aircraft seat 12 can view a movie being presented by a self-contained IFED 14 resting on a seat back table 16 that is connected to a forwardly adjacent aircraft seat 18. As is conventional practice, earphones 20 are plugged into a sound output 21 on the self-contained IFED to allow the passenger 10 to listen to the audio portion of the presentation without disturbing fellow passengers. The self-contained IFED 14, further depicted in Figure 2, includes a display 22 for viewing presentations and controls 24 for selection of presentations and adjustment of the self-contained IFED.

The self-contained IFED 14 contains a processor 25, as shown in Figure 3, for interaction and control of various other components of the self-contained IFED. An encrypted hard drive 26 is included for storing one or more files containing current movies or other audiovisual presentations. The encrypted hard drive 26 is accessible through a hard drive decryptor 28 so that both encrypted files 30 containing current movies and other proprietary property and unencrypted files (not shown) are protected

by the encryption mechanisms associated directly with the encrypted hard drive. The encrypted files 30 are further protected by their own encryption mechanisms and are only accessible through a file decryptor 32 containing one or more decryption keys for reading of the encrypted files.

An input-output 34 of unique physical configuration is used to delete out-dated audiovisual presentations from the encrypted hard drive 26 and to transfer current movie releases and other audiovisual presentations to the encrypted hard drive. The input-output 34 is formed such that a specially formed connector of a unique shape complementary to the input-output is used to connect a workstation to the self-contained IFED 14 for the file deletion and loading activities. An input-output authenticator 36 is used to verify that the workstation connected to the self-contained IFED 14 through the input-output 34 has authorized access privileges. Although the input-output 34 has a unique physical configuration, it can still use standard protocols such as USB 2.0 or IEEE 1394, which can be utilized for the authorization process. Even when access privileges are granted, in some implementations, no read access to obtain files from the encrypted hard drive is allowed.

Anti-tamper fasteners 38 are used to physically secure the case of the self-contained IFED 14 together, thereby requiring a unique tool for physically accessing internal components of the self-contained IFED. An evidentiary seal 40 is used to seal an internal portion of the self-contained IFED 14 in such a way that if physical access is achieved to the internal components of the self-contained IFED, then the evidentiary seal is broken and easily visible upon inspection.

The various layers of security 42 associated with the self-contained IFED 14 are summarized in Figure 4 as including one or more encoded files of one or more original master recordings received from a movie recording studio or other organization. Typically each original master recording will be processed to generate a separate encoded file in a compressed format such as MPEG-4 Advanced Simple Profile with DVD playback quality approximately 1 Mbps. Other implementations have other modes of compression and display quality. The encoded files are encoded with a unique bit stream encoding format (layer 44) such that the processor 25 of the IFED 14 is specially configured to render the encoded file for display. Consequently, in the event other security layers discussed herein are breached, the special configuration of the processor 25 will still be needed for viewing, which will help to prevent piracy. During

encoding, a digital process is used to add additional characters to the encoded file as a watermark (layer 46) to identify details such as time and place of the encoding to assist in forensic tracking if needed through watermark detection software.

Some implementations further include the addition of camera artifacts to the encoded files (layer 48) during the encoding process. Camera artifacts are used to hinder illegal video recording taken of movies being displayed on the self-contained IFED 14. The camera artifacts are displayed on the display 22 of the self-contained IFED 14 when the encoded file is played on the self-contained IFED, but are not visible to the passenger 10. Instead, if video recordings are taken of the display 22 during play of the encoded file, the camera artifacts are visible when these video recordings are viewed. Thus, attempts at recording video content from the self-contained IFED 14 for later viewing on equipment other than the self-contained IFED can be hindered.

After the encoding process is completed, the encoded files are encrypted, thereby producing encrypted encoded audiovisual files (layer 50). During encryption, a unique key for decryption is generated for each individual file, which is required for subsequent playing of the file and is handled by the file decryptor 32 of the self-contained IFED 14. The encrypted encoded audiovisual files are stored on the encrypted hard drive 26 (layer 52) such that the hard drive decryptor 28, having decryption methods separate from those used to decrypt the individual encrypted files, is necessary for accessing the encrypted files.

In some implementations only the input-output 34 is available for external access to the encrypted hard drive 26. As explained above the input-output 34 has a unique physical configuration. Also, the input-output 34 uses protocols that require authorization through the input-output authenticator 36 to occur within a limited window of time otherwise physical reconnection to the input-output is necessary for further access attempts (layer 54). In some implementations, the operation of the encrypted hard drive 26 together with the input-output 34 only allows for writes and delete functions without allowing read functions, which can also add to the security provided under layer 54. As discussed, the self-contained IFED 14 also has anti-tamper fasteners 38 and an evidentiary seal 40 (layer 56) for an additional layer of security.

A flow-chart of a method 60 associated with security elements of the self-contained IFED 14 is shown in Figure 5. The method 60 begins with receiving an audiovisual master from a movie recording studio or other organization containing an

audiovisual presentation such as a to-be-released or recently released movie (step 62). The audiovisual master is encoded with the special format discussed above and watermark characters are added to the encoded audiovisual file (step 64). In some implementations, camera artifacts are also added during the encoding process (step 66). The encoded audiovisual file is next encrypted (step 68) and then sent (as well as associated keys) to a distribution point host computer (step 70). The encrypted encoded audiovisual files are loaded on to the distribution host computer. The distribution host computer then links with one of the pluralities of the self-contained IFED 14 in which bi-directional authentication occurs between the distribution host computer and the self-contained IFED through use in part of the input-output 34 of the self-contained IFED (step 72).

Once the bi-directional authentication occurs, the distribution host computer can be used to delete out-of-date audiovisual files from the self-contained IFED 14 (step 74). The distribution host computer can then transfer the encrypted encoded files along with the associated keys to the self-contained IFED 14 without need of decryption of the files occurring (step 76). Consequently, the encrypted audiovisual files are stored on the encrypted hard drive 26 of the self-contained IFED 14 (step 78). Also, the keys associated with the encrypted audiovisual files are stored on the self-contained IFED 14 to be used for subsequent decryption of the encrypted audiovisual files for display of the associated audiovisual presentations (e.g. current release movies), such as during an airline flight (step 80) to an airline passenger who rented the self-contained IFED.

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

The invention claimed is

1. A method comprising:

receiving an audiovisual master file from a movie recording studio or other organization containing an audiovisual presentation such as a to-be-released or recently released movie, the audiovisual master file being in a first encoded and compressed format;

adding watermark characters to the encoded audiovisual master file;

adding camera artifacts to the encoded audiovisual master file;

encrypting the encoded audiovisual master file to create an encrypted encoded audiovisual master file;

generating keys associated with the encrypted encoded audiovisual master file for using in decoding the encrypted encoded audiovisual master file;

transmitting the encrypted encoded audiovisual master file and the associated keys to a distribution point host computer;

loading the transmitted encrypted encoded audiovisual master file on the distribution point host computer;

linking the distribution point host computer with a self-contained entertainment device and establishing bi-directional authentication between the distribution point host computer and the self-contained entertainment device through use, in part, of an input-output of the self-contained entertainment device;

after bi-directional authentication occurs, using the distribution point host computer to delete at least some of the previously loaded encrypted encoded audiovisual master files from the self-contained entertainment device;

using the distribution point host computer to transfer the newly loaded encrypted encoded audiovisual master file and keys associated with the newly loaded encrypted encoded audiovisual master file to the self-contained entertainment device to which the distribution point host computer is linked without decryption of the newly loaded encrypted encoded audiovisual master file being transferred to the self-contained entertainment device; and

storing the newly loaded encrypted encoded audiovisual master file and the keys associated with the newly loaded encrypted encoded audiovisual master file on an encrypted hard drive of the self-contained entertainment device to which the distribution point host computer is linked.

2. The method of claim 1 further including using the self-contained entertainment device to subsequently decrypt the newly loaded encrypted encoded audiovisual master file stored on an encrypted hard drive of the self-contained entertainment device using the keys associated with the newly loaded encrypted encoded audiovisual master file stored on an encrypted hard drive of the self-contained entertainment device to display audiovisual presentation of the newly loaded encrypted encoded audiovisual master file stored on an encrypted hard drive of the self-contained entertainment device to a person who rented the self-contained entertainment device.

3. A system comprising:

a sound output;

a visual display;

a processor;

encrypted audiovisual files;

an encrypted hard drive containing the encrypted audiovisual files;

a hard drive decryptor configured for decrypting the encrypted hard drive;

a file decryptor for decrypting the encrypted files;

an input-output with unique physical configuration;

an input-output authenticator configured to authenticate a device attempting to communicatively link to the input-output;

a case being secured with anti-tamper fasteners; and

an evidentiary seal positioned to rupture when a portion of the case is dissembled.

4. A method comprising:

receiving an audiovisual master file from a movie recording studio or other organization containing an audiovisual presentation such as a to-be-released or

recently released movie, the audiovisual master file being in a first encoded and compressed format;

encrypting the encoded audiovisual master file to create an encrypted encoded audiovisual master file;

generating keys associated with the encrypted encoded audiovisual master file for using in decoding the encrypted encoded audiovisual master file;

transmitting the encrypted encoded audiovisual master file and the associated keys to a distribution point host computer;

loading the transmitted encrypted encoded audiovisual master file on the distribution point host computer;

linking the distribution point host computer with a self-contained entertainment device and establishing bi-directional authentication between the distribution point host computer and the self-contained entertainment device through use, in part, of an input-output of the self-contained entertainment device;

after bi-directional authentication occurs, using the distribution point host computer to delete at least some of the previously loaded encrypted encoded audiovisual master files from the self-contained entertainment device;

using the distribution point host computer to transfer the newly loaded encrypted encoded audiovisual master file and keys associated with the newly loaded encrypted encoded audiovisual master file to the self-contained entertainment device to which the distribution point host computer is linked without decryption of the newly loaded encrypted encoded audiovisual master file being transferred to the self-contained entertainment device; and

storing the newly loaded encrypted encoded audiovisual master file and the keys associated with the newly loaded encrypted encoded audiovisual master file on an encrypted hard drive of the self-contained entertainment device to which the distribution point host computer is linked.

5. A system comprising:

a sound output;

a visual display;

a processor;

encrypted audiovisual files;

an encrypted hard drive containing the encrypted audiovisual files;

a hard drive decryptor configured for decrypting the encrypted hard drive;

a file decryptor for decrypting the encrypted files; and

an input-output authenticator configured to authenticate a device attempting to communicatively link to the input-output.

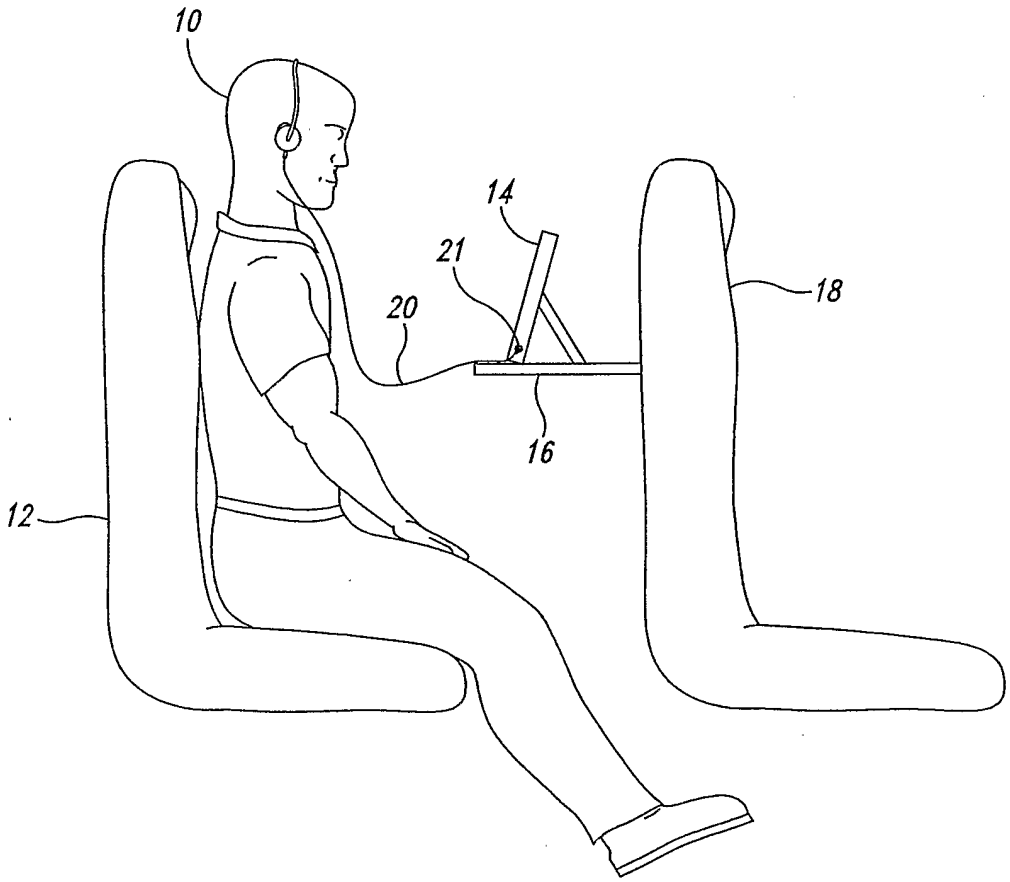


Fig. 1

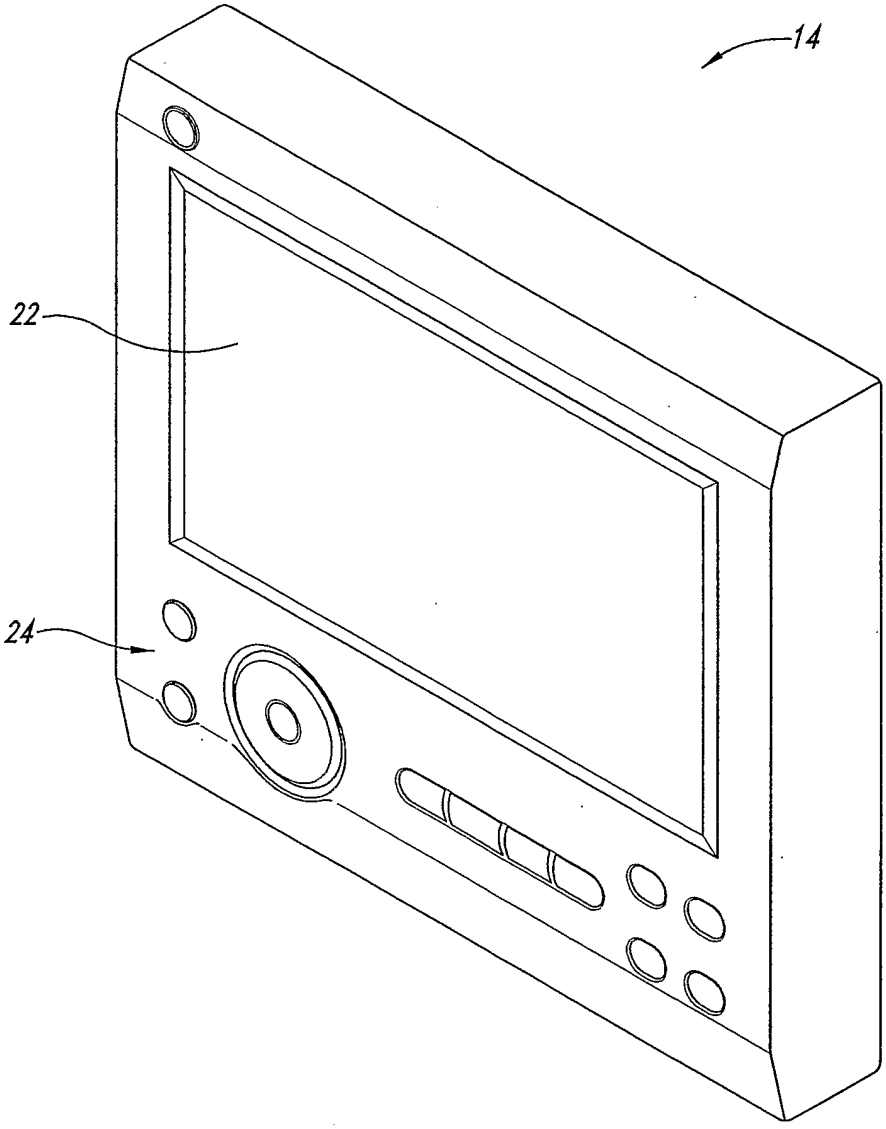


Fig. 2

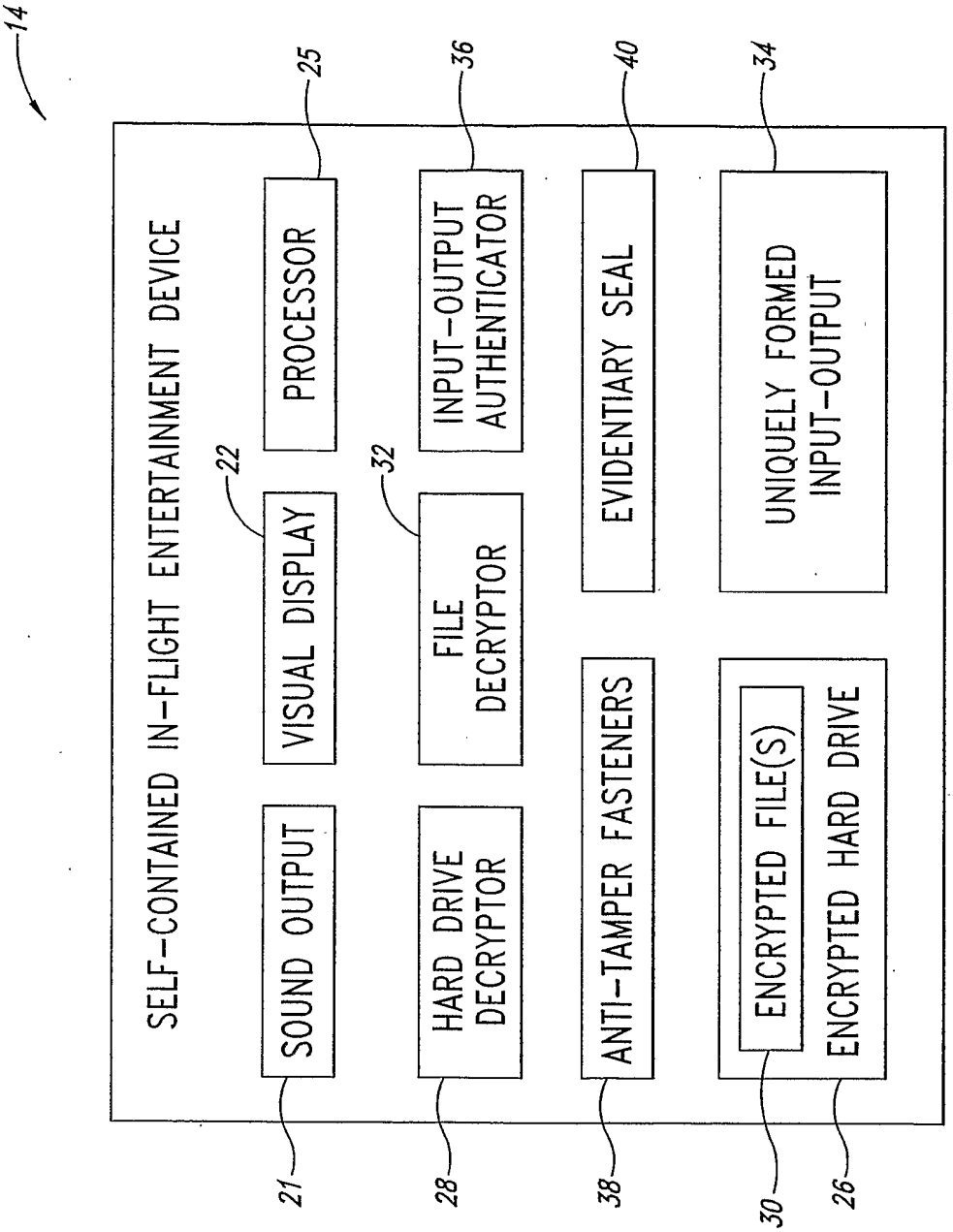

14
SELF-CONTAINED IN-FLIGHT ENTERTAINMENT DEVICE
SOUND OUTPUT
VISUAL DISPLAY
PROCESSOR
HARD DRIVE DECRYPTOR
FILE DECRYPTOR
INPUT-OUTPUT AUTHENTICATOR
ANTI-TAMPER FASTENERS
EVIDENTIARY SEAL
ENCRYPTED FILE(S)
ENCRYPTED HARD DRIVE
UNIQUELY FORMED INPUT-OUTPUT
21
22
25
26
28
30
32
34
36
38
40

Fig. 3

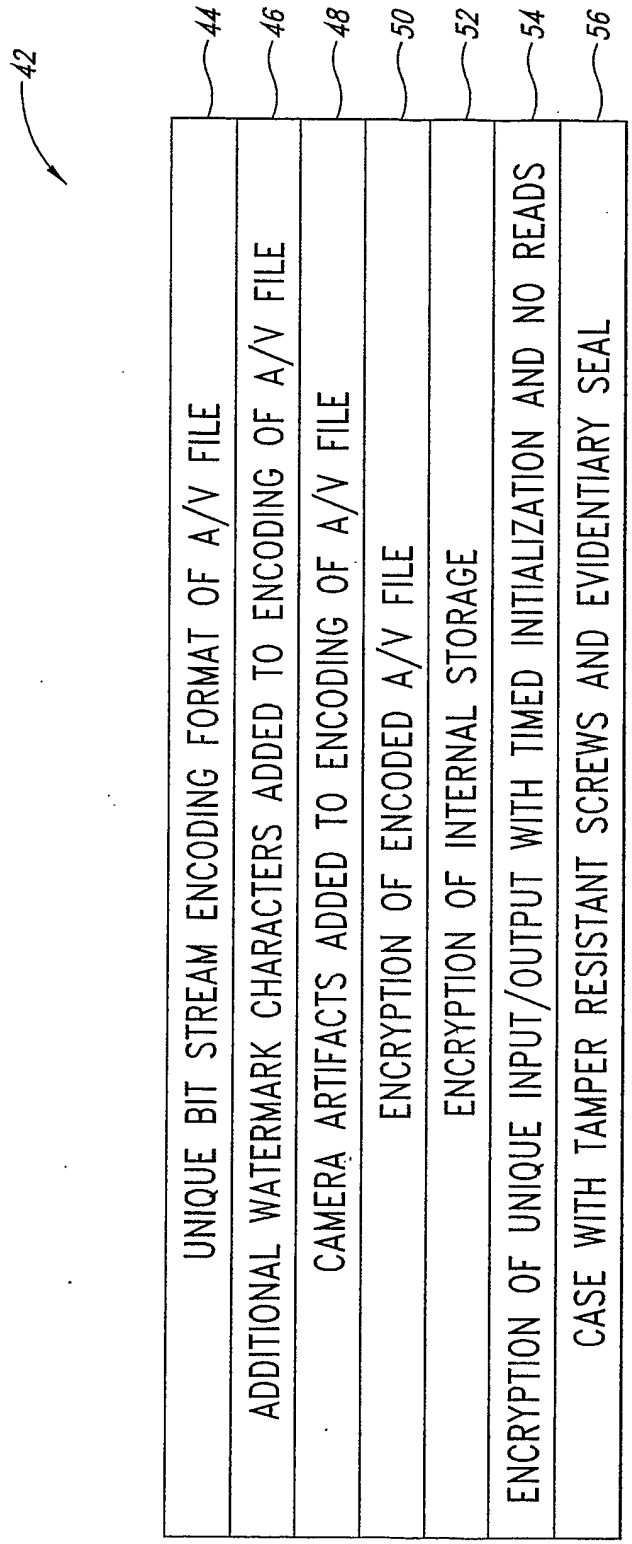

42
44
46
48
50
52
54
56
UNIQUE BIT STREAM ENCODING FORMAT OF A/V FILE
ADDITIONAL WATERMARK CHARACTERS ADDED TO ENCODING OF A/V FILE
CAMERA ARTIFACTS ADDED TO ENCODING OF A/V FILE
ENCRYPTION OF ENCODED A/V FILE
ENCRYPTION OF INTERNAL STORAGE
ENCRYPTION OF UNIQUE INPUT/OUTPUT WITH TIMED INITIALIZATION AND NO READS
CASE WITH TAMPER RESISTANT SCREWS AND EVIDENTIARY SEAL

Fig. 4

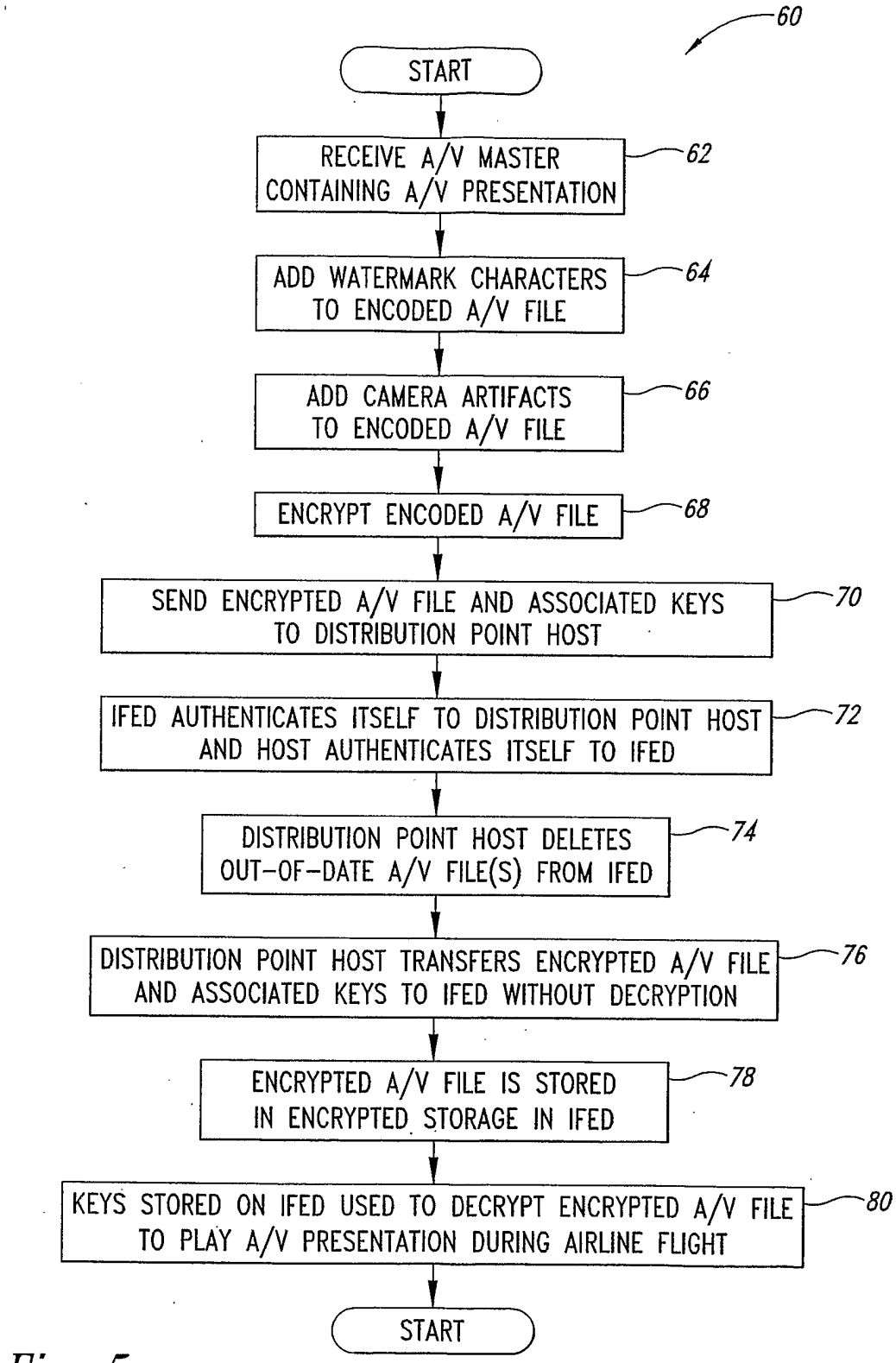

60
START
RECEIVE A/V MASTER CONTAINING A/V PRESENTATION
62
ADD WATERMARK CHARACTERS TO ENCODED A/V FILE
64
ADD CAMERA ARTIFACTS TO ENCODED A/V FILE
66
ENCRYPT ENCODED A/V FILE
68
SEND ENCRYPTED A/V FILE AND ASSOCIATED KEYS TO DISTRIBUTION POINT HOST
70
IFED AUTHENTICATES ITSELF TO DISTRIBUTION POINT HOST AND HOST AUTHENTICATES ITSELF TO IFED
72
DISTRIBUTION POINT HOST DELETES OUT-OF-DATE A/V FILE(S) FROM IFED
74
DISTRIBUTION POINT HOST TRANSFERS ENCRYPTED A/V FILE AND ASSOCIATED KEYS TO IFED WITHOUT DECRYPTION
76
ENCRYPTED A/V FILE IS STORED IN ENCRYPTED STORAGE IN IFED
78
KEYS STORED ON IFED USED TO DECRYPT ENCRYPTED A/V FILE TO PLAY A/V PRESENTATION DURING AIRLINE FLIGHT
80
START

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/29137

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : GO6F 11/30; H04L 9/00; H04K 1/00; H04N 7/167
US CL : 713/165, 176, 182, 200-201, 380/200-203, 210-211

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. : 713/165, 176, 182, 200-201, 380/200-203, 210-211

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4,630,821 A (GREENWALD) 23 December 1986, see col. 1, lines 49-67, col. 2, lines 4-67.	1-5
A,P	US 6,785,815 B1(SERRET-AVILA et al.) 31 AUGUST 2004, see col. 2, lines 46-67, col. 3, lines 1-46, col. 4, lines 36-67, col. 10, lines 13-67, col. 12, lines 1-45.	1-5
A	US 4,866,515 A (TAGAWA et al.) 12 SEPTEMBER 1989, see col. 1, lines 55-68, col. 2, lines 1-55, col. 5, lines 55-68, col. 6, lines 1-46,	1-5

☐ 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 application or patent 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
21 December 2004 (21.12.2004)

Date of mailing of the international search report
19 JAN 2005

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Authorized officer
Ayaz Shiekh

Telephone No. (571) 272-3791

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US04/29137

Continuation of B. FIELDS SEARCHED Item 3:
West searched; search terms used, in flight entertainment, passenger seats, screen or display or tv, watermarking, encode, encrypt or scrambling