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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 April 2003 (03.04.2003)

PCT

(10) International Publication Number
WO 03/028025 A1

(51) International Patent Classification⁷: G11B 20/00, H04N 7/18

(21) International Application Number: PCT/GB02/04372

(22) International Filing Date: 26 September 2002 (26.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0123140.6 26 September 2001 (26.09.2001) GB

(71) Applicant *(for all designated States except US)*: **ORBB LIMITED** [GB/GB]; Academic Surgical Unit, 10th Floor, QEQM, St Mary's Hospital, Praed Street, Paddington, London W2 1NL (GB).

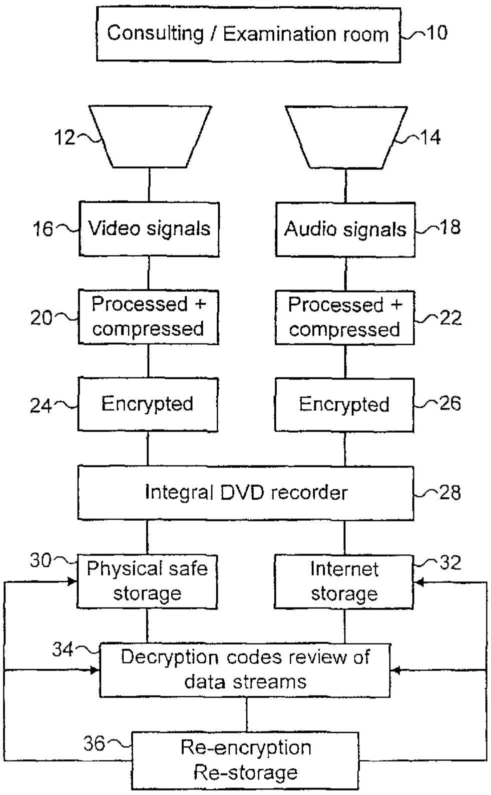
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **EDWARDS, Lee, David** [GB/GB]; 516A London Road, West Cliff On Sea, Essex SS0 9LD (GB). **DARZI, Ara, Warkes** [IE/GB]; 3 Elmwood Park, Gerrards Cross, Buckinghamshire SL9 7EP (GB). **MACKAY, Sean** [AU/AU]; P.O. Box 1256, North Fitzroy 3068, Melbourne (AU). **DRAPER, Edward** [GB/GB]; 771 London Road, Loudwater, Buckinghamshire HP11 1HW (GB). **YANG, Guang-Zhong** [GB/GB]; 4 Mxkenzie Way, Clamendor Park, Epson KT19 7ND (GB).

(74) Agent: **ROBSON, Aidan, John**; Reddie & Grose, 16 Theobalds Road, London WC1X 8PL (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,

[Continued on next page]

(54) Title: A SYSTEM FOR REAL TIME DATA ENCRYPTION



(57) Abstract: A system for monitoring the execution of a procedure within a predetermined environment comprising means for recording information from the procedure during the time in which the procedure is executed wherein the information from the procedure includes the status of the instrumentation used during the procedure, encrypting said recorder information from the procedure and storing said encrypted information.

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, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, 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.

A System for Real Time Data Encryption

The present invention relates to a system for the recording and real time encryption of multiple data streams before storing the data streams on a storage facility.

It is apparent that patient safety and the monitoring of clinical competence are of ever increasing importance. The impact of clinical negligence, in an extremely litigious environment, is becoming increasingly burdensome to the medical profession and the healthcare industry as a whole.

The presence of professional chaperones during potentially intimate examinations is common practice in most hospitals. Chaperones or nurses seconded from their normal duties are present during patient examinations specifically to protect both the patient and the practitioner from the risk of spurious charges.

There are many environments outside of the hospital including GP consulting rooms, osteopath or physiotherapist rooms, dental surgeries and alternative healthcare surgeries where a one-to-one interface in potentially intimate situations exposes the healthcare profession to risk.

It is desirable to have a fully integrated, real time visual and audio recording, data collection and retrieval system that offers the medical professions and healthcare industry the benefit of monitoring a procedure. A data recording system provides essential backup that will reduce the number of spurious claims, potentially reduce medical defence premiums and create an environment within which the healthcare profession and the patient will feel comfortable and protected.

In order to protect the identity of the subjects within the recorded procedure and maximise the security of sensitive data it is advantageous to encrypt all data before storing.

PCT/GB01/03801 describes a data recording system in which multiple data streams are stored centrally on a data storage device. The system monitors the execution of a procedure within a predetermined environment using multiple recording devices including cameras and microphones. The data streams are synchronised and stored. The procedure may be reviewed by downloading the data from the storage device.

Embodiments of the present invention provides a self contained data recorder capable of monitoring a procedure using multiple data streams in which the data streams are encrypted before being stored directly to DVD. Storing the data directly to DVD negates the need for large processors or hard disc space. Encryption is typically executed using a key system to maximise confidentially. The encrypted data streams may be accessed from the storage facility using decoding keys in order to review the monitored procedure.

The invention is defined in its various aspects in the appended claims to which reference should now be made.

Embodiments of the present invention will now be described with reference to the accompanying drawings in which;

Figure 1 is a block diagram showing the path of multiple data streams within an embodiment of the present invention;

Figure 2 shows the hardware included in an embodiment of the invention;

Figure 3 shows the data flow within an embodiment of the present invention;

Figure 4 is a block diagram of an embodiment of the present invention including data connections;

Figure 5 is block diagram of an embodiment of the present invention including data connections.

Figure 1 shows a consulting or examination room 10 which is monitored by audio recording equipment 12 and video recording equipment 14.

Multiple digital video signals 16 are recorded from multiple video cameras 12 positioned around the monitored area. Multiple video signals are helpful in giving different views of the environment but in some applications only one video signal may be required. Sometimes the video signals are not recorded at all.

Audio ambient and directional signals 18 are recorded by one or more audio receivers 14 positioned around the monitored area 10. These signals may be recorded by static microphones or microphones attached to subjects within the consulting or examination room 10. Sometimes the audio signals are not recorded at all.

Further embodiments of the invention include sensors to record other types of information including movement or the output from equipment used during the procedure.

This further information increases the detail available during a review of the procedure.

The audio and video signals are processed and compressed at 20 and 22 respectively. The compressed signals are then encrypted at 24 and 26. Encryption is typically executed using private and / or public key systems. The encrypted signals are then transferred and stored at an integral DVD recorder 28. It is also possible to replace the DVD recorder using any suitable data storage medium. It is also possible to simultaneously store the data on multiple storage facilities.

The data stored at 28 may be downloaded and stored onto further storage devices 30 or onto the internet 32.

The data may only be accessed and reviewed through use of decryption codes at 34. Access is only be available to those data streams to which the user has the decryption codes. The encryption programme ensures that review of the recording is only undertaken with the consent of the clinician and the patient. An independent, third party regulatory body may hold the final key to the data and provide the access protocols.

After review the data may be re-encrypted and re-stored at 36.

Figure 2 shows the hardware layout for a real time compression and encryption system used in an embodiment of the present invention. The system includes a PCI plug in board 40 with a single chip encryption processor. The encryption card 42 is linked to an IDE 44. The IDE 44 is then linked to a PCI bus 40 which is connected to the host PC 46.

Figure 3 shows the software dataflow within an embodiment of the present invention. The data from the preocedure is forwarded from an integrated drive electronics (IDE) 50 to the encryption driver 52 where the data is encrypted. The encryption driver has a dedicated processor which facilitates real-time encryption of high bandwidth data channels such as streaming media including video and audio. The system utilises one time only hardware and driver installation which makes all software application security enabled.

The embodiment of figure 3 emulates a virtual disk for the windows operating system. Any data written to the virtual disk is encrypted in real time and stored to an integrated storage media 54 for example floppy disk, hard disk, CDR or DVD-R. The system uses public key technology 56 and private key technology 58 and allows the user to exchange data with other parties. No decrypted data is stored on any physical media in order to provide added system level protection.

Once stored on the storage device 54 data streams can only be decrypted using public keys 56 or private keys 58. The user can also exchange data with other parties. If a user does not have the required key to access a particular data stream, that data stream will not be decrypted and will be unreadable to the user. The system is easy to set up and once installed it enables multiple software applications 60 with disk access to have a secure route of storing security sensitive data. The system is fully network compatible and can turn a share network drive fully secure. The system is also fully compatible with the Internet and can also be used for secure transmission of data through the Internet.

Figure 4 is a block diagram an embodiment of the present invention. Figure 4 includes the hardware included in the system and shows the power connections between each component.

The system is powered by an ATX power supply 72 which is powered by the mains at 70. The ATX power supply has multiple power outputs including a 12 V output, 5 V output 74 and an ATX output 76.

The ATX output is used to power a single board computer 78 at the ATX input 80. The ON/OFF state of the single board computer is determined by the state of the ON/OFF switch 82 which is connected to the ATX CTRL at 84. A CPU fan 100 and ventilation fan 102 are powered through the single board computer.

The remaining hardware components in this embodiment are powered by the 12 V, 5 V output from the ATX power supply. The system includes a controller 86, an inverter 88, a TFT LCD display 90, a DVD RAM drive 92, a hard disk drive 94, a camera 96 and a video connector 98 all of which are powered by the 12 V / 5 V output 74 of the ATX power supply 72.

Figure 5 shows the data connections within an embodiment of the present invention. The information is first recorded by the camera 96. The data streams from the camera are forwarded to the video connector 98. The data streams are then forwarded to the MPEG2 card 100 where they are converted into digital signals. The MPEG2 card is connected to a peripheral component interconnect (PCI) 102 on the single board computer 78. A second PCI 104 within the single board computer 78 transfers the digital data streams to an encryption card 106. Further embodiments of the invention may include facilities to record other types of information. The corresponding data streams can also be connected to the encryption card at 106. The digital signals are encrypted at 106 and forwarded to the real time data compression and encryption unit 108. The encrypted data stored within the data compression and encryption unit 108 may be downloaded onto a further storage facility. The embodiment of figure 5 includes a DVD RAM drive 92 and a hard disk drive 94 onto which the encrypted data can be downloaded from the data compression and encryption unit 108.

The DVD RAM drive 92 and hard disk drive 94 are connected to the single board computer 78 via integrated drive electronics (IDE) at 112 and 110 respectively. These connections facilitate downloading of the data for review from the DVD RAM drive 92 and hard disk drive 94. The data may be accessed using a touch screen 114 which is connected to the controller 86. The controller 86 is connected to the single board computer 78 using an RS232 connection 116. The accessed data is displayed on the TFT LDC display 90 via the TTL connection 118.

It is clear from the above description that embodiments of the present invention provide a means for comprehensively monitoring a particular environment. Multiple data streams are recorded, encrypted in real time and stored on a data storage facility. No data is stored which is not encrypted in order to maximise the security of sensitive data. The data streams can only be decoded using the associated private or public keys.

It is understood that the methods employed by this invention extend beyond medical practice and facilitate a means for monitoring a variety of environments. When monitoring a preferred environment, sensors and data streams suitable for use in that environment should be employed.

Claims

1. A system for monitoring the execution of a procedure within a predetermined environment comprising means for recording information from the procedure during the time in which the procedure is executed wherein the information from the procedure includes the status of the instrumentation used during the procedure, encrypting said recorded information from the procedure and storing said encrypted information.

2. A system for monitoring the execution of a procedure within a predetermined environment according to claim 1 in which the information from the procedure comprises visual information and is recorded using cameras.

3. A system for monitoring the execution of a procedure within a predetermined environment according to claim 1 or 2 in which the information from the procedure comprises audio information and is recorded using audio receivers.

4. A system for monitoring the execution of a procedure within a predetermined environment according claim 1, 2, or 3 in which the information from the procedure comprises the movements of subjects within the environment which are monitored using sensors positioned on the subjects.

5. A system for monitoring the execution of a procedure within a predetermined environment according to claim 1, 2, 3 or 4 in which the recorded information is encrypted in real time.

6. A system for monitoring the execution of a procedure within a predetermined environment according to claim 5

in which said encrypted information is stored directly to DVD.

7. A system for monitoring the execution of a procedure within a predetermined environment according to claim 5 in which said encrypted information is stored directly to CD.

8. A system for monitoring the execution of a procedure within a predetermined environment according to claim 5 in which said encrypted information is stored directly to the hard drive of a pc.

9. A system for monitoring the execution of a procedure within a predetermined environment according to claim 6, 7 or 8 in which only encrypted data is stored.

10. A system for monitoring the execution of a procedure within a predetermined environment according to claim 9 in which data may only be selected, downloaded and decrypted through use of the associated public or private keys.

11. A system for monitoring the execution of a procedure within a predetermined environment substantially as herein described, with reference to the accompanying drawings.

12. A method for monitoring the execution of a procedure within a predetermined environment comprising the steps of recording information from the procedure during the time in which the procedure is executed wherein the information from the procedure includes the status of the instrumentation used during the procedure, encrypting said recorded information from the procedure and storing said encrypted information.

13. A method for monitoring the execution of a procedure within a predetermined environment according to claim 12 in which the information from the procedure comprises visual information and is recorded using cameras.

14. A method for monitoring the execution of a procedure within a predetermined environment according to claim 12 or 13 in which the information from the procedure comprises audio information and is recorded using audio receivers.

15. A method for monitoring the execution of a procedure within a predetermined environment according claim 12, 13 or 14 in which the information from the procedure comprises the movements of subjects within the environment which are monitored using sensors positioned on the subjects.

16. A method for monitoring the execution of a procedure within a predetermined environment according to claim 12, 13, 14 or 15 in which the recorded information is encrypted in real time.

17. A method for monitoring the execution of a procedure within a predetermined environment according to claim 16 in which said encrypted information is stored directly to DVD.

18. A method for monitoring the execution of a procedure within a predetermined environment according to claim 16 in which said encrypted information is stored directly to CD.

19. A method for monitoring the execution of a procedure within a predetermined environment according to claim 16 in which said encrypted information is stored directly to the hard drive of a pc.

20. A method for monitoring the execution of a procedure within a predetermined environment according to claim 17, 18 or 19 in which only encrypted data is stored.

21. A method for monitoring the execution of a procedure within a predetermined environment according to claim 22 in which data may only be selected, downloaded and decrypted through use of the associated public or private keys.

22. A method for monitoring the execution of a procedure within a predetermined environment substantially as herein described, with reference to the accompanying drawings.

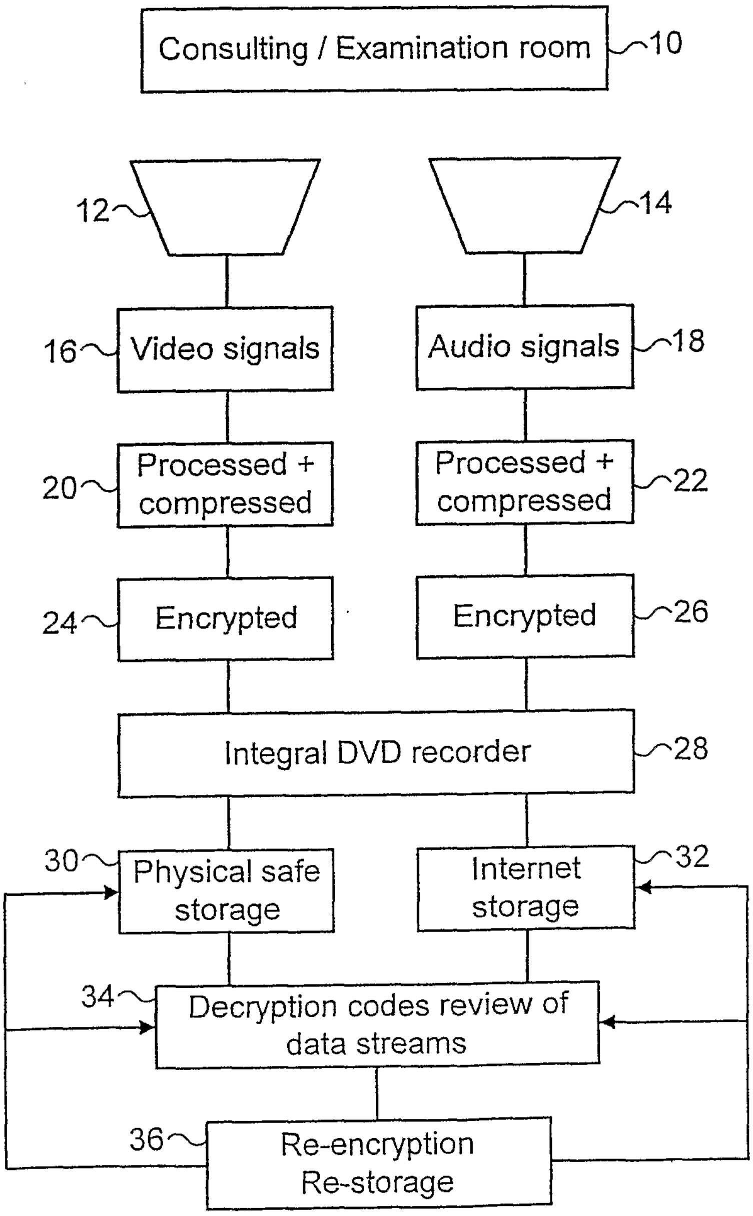

Consulting / Examination room
10
12
14
16
Video signals
Audio signals
18
20
Processed + compressed
Processed + compressed
22
24
Encrypted
Encrypted
26
Integral DVD recorder
28
30
Physical safe storage
Internet storage
32
34
Decryption codes review of data streams
36
Re-encryption Re-storage

FIG. 1

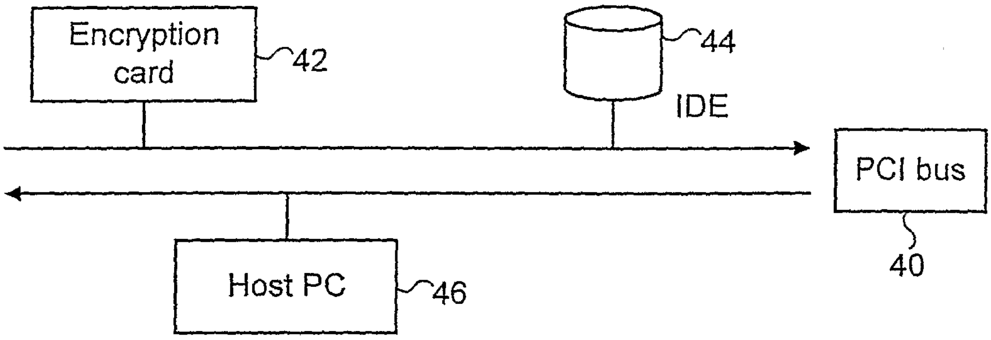

Encryption card
42
44
IDE
PCI bus
40
Host PC
46

FIG. 2

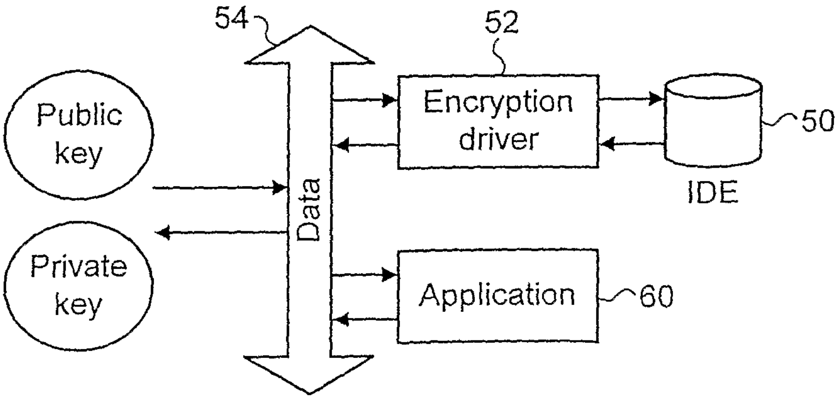

54
52
Public key
Private key
Data
Encryption driver
50
IDE
Application
60

FIG. 3

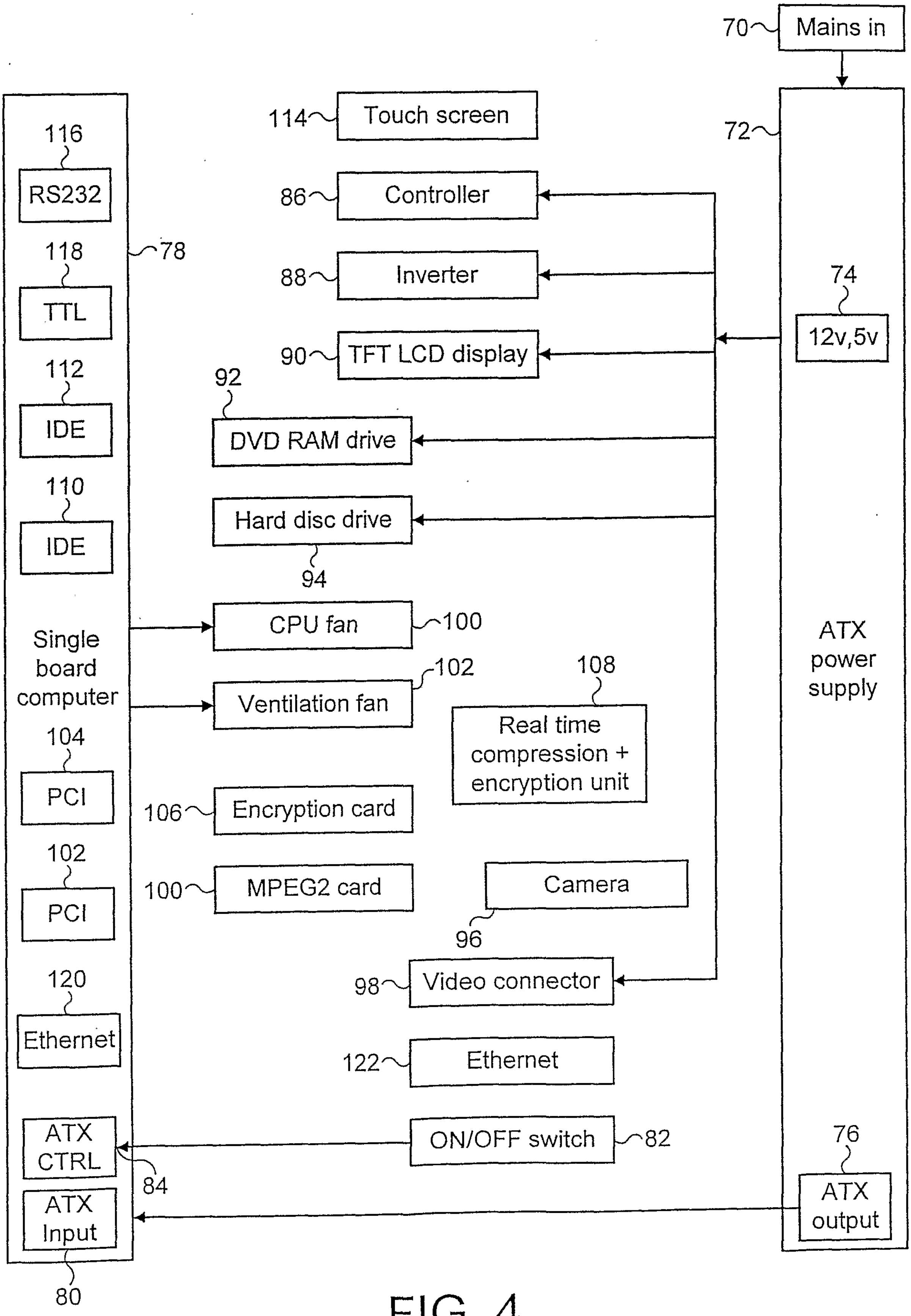

70
Mains in
72
ATX power supply
74
12v,5v
76
ATX output
114
Touch screen
86
Controller
88
Inverter
90
TFT LCD display
92
DVD RAM drive
Hard disc drive
94
CPU fan
100
Ventilation fan
102
108
Real time compression + encryption unit
106
Encryption card
100
MPEG2 card
Camera
96
98
Video connector
122
Ethernet
ON/OFF switch
82
78
116
RS232
118
TTL
112
IDE
110
IDE
Single board computer
104
PCI
102
PCI
120
Ethernet
ATX CTRL
84
ATX Input
80

FIG. 4

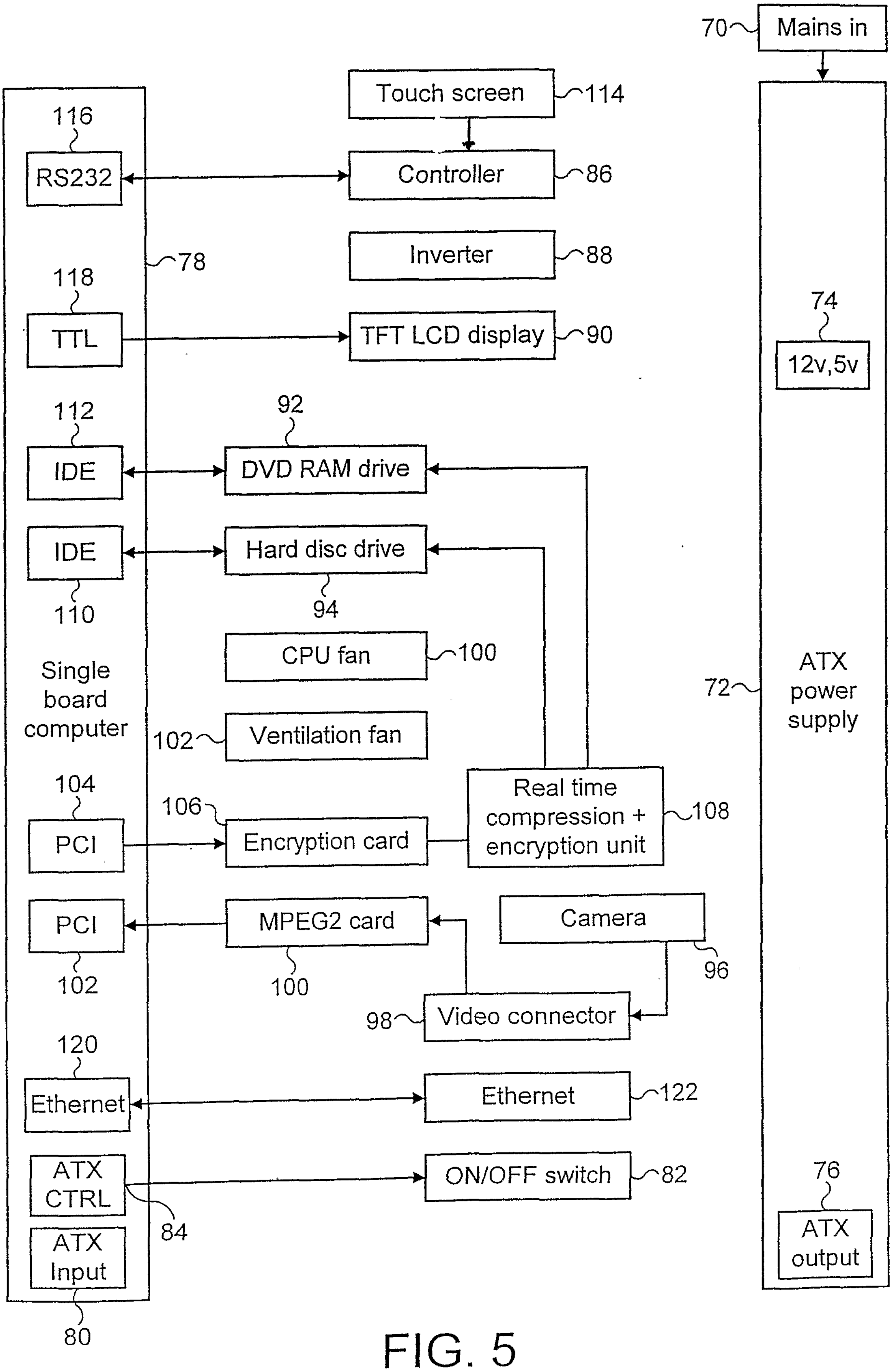

70
Mains in
Touch screen
114
116
RS232
Controller
86
Inverter
88
78
118
TTL
TFT LCD display
90
74
12v,5v
112
IDE
92
DVD RAM drive
IDE
Hard disc drive
110
94
CPU fan
100
Single board computer
102
Ventilation fan
72
ATX power supply
104
106
PCI
Encryption card
Real time compression + encryption unit
108
PCI
MPEG2 card
Camera
96
102
100
98
Video connector
120
Ethernet
Ethernet
122
ATX CTRL
ON/OFF switch
82
84
76
ATX Input
ATX output
80

FIG. 5

INTERNATIONAL SEARCH REPORT

PCT/GB 02/04372

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 H04N7/18

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 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	US 5 689 442 A (MOEN JERRY M ET AL) 18 November 1997 (1997-11-18) abstract column 3, line 35 -column 5, line 30 column 10, line 35 -column 11, line 26 figure 1 ---	1-22
X	US 5 497 419 A (HILL BRIAN R) 5 March 1996 (1996-03-05) abstract column 4, line 38 -column 7, line 37 figure 1 --- -/--	1-22

☒ Further documents are listed in the continuation of box C.

☒ 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 20 November 2002	Date of mailing of the international search report 09/12/2002
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 Sucher, R

INTERNATIONAL SEARCH REPORT

PCT/GB 02/04372

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 99 62741 A (SCAMAN ROBERT JEFF) 9 December 1999 (1999-12-09) abstract page 2, line 22 -page 3, line 6 page 4, line 6 -page 6, line 11 page 7, line 22 -page 11, line 21 figure 1 ---	1-22
Y	US 5 654 750 A (HODGDON DANA ET AL) 5 August 1997 (1997-08-05) abstract column 1, line 1 - line 39 column 2, line 35 -column 3, line 15 figures 1,2 ---	1-22
Y	WO 00 08585 A (CONTEC MEDICAL LTD) 17 February 2000 (2000-02-17) abstract page 4, paragraph 3 ---	1-22
A	WO 92 08321 A (COOPER ROGER DENNIS) 14 May 1992 (1992-05-14) abstract page 8, line 1 -page 12, line 11 -----	1-22

INTERNATIONAL SEARCH REPORT

Information on patent family members

PCT/GB 02/04372

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
US 5689442	A	18-11-1997	WO	9912354	A1	11-03-1999
			AU	4238297	A	22-03-1999
US 5497419	A	05-03-1996	CA	2188250	A1	26-10-1995
			EP	0761051	A1	12-03-1997
			WO	9528783	A1	26-10-1995
			US	5646994	A	08-07-1997
WO 9962741	A	09-12-1999	AU	4223399	A	20-12-1999
			EP	1082234	A2	14-03-2001
			WO	9962741	A2	09-12-1999
			US	2002135679	A1	26-09-2002
			US	2002145666	A1	10-10-2002
			US	6211907	B1	03-04-2001
			US	2001005217	A1	28-06-2001
US 5654750	A	05-08-1997	NONE			
WO 0008585	A	17-02-2000	EP	1103028	A2	30-05-2001
			WO	0008585	A2	17-02-2000
WO 9208321	A	14-05-1992	AU	8748791	A	26-05-1992
			WO	9208321	A1	14-05-1992