

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
22 June 2006 (22.06.2006)

PCT

(10) International Publication Number
WO 2006/064314 A1

(51) International Patent Classification:
G11B 20/00 (2006.01)

(21) International Application Number:
PCT/IB2005/001872

(22) International Filing Date: 31 May 2005 (31.05.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/015,581 18 December 2004 (18.12.2004) US

(71) Applicant and

(72) Inventor: **AL-KHATEEB, Osama Othman Mostaeen**
[SY/KW]; P.O. Box 2145, Safat 13022 (KW).

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, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, 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, 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, IS, IT, LT, 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).

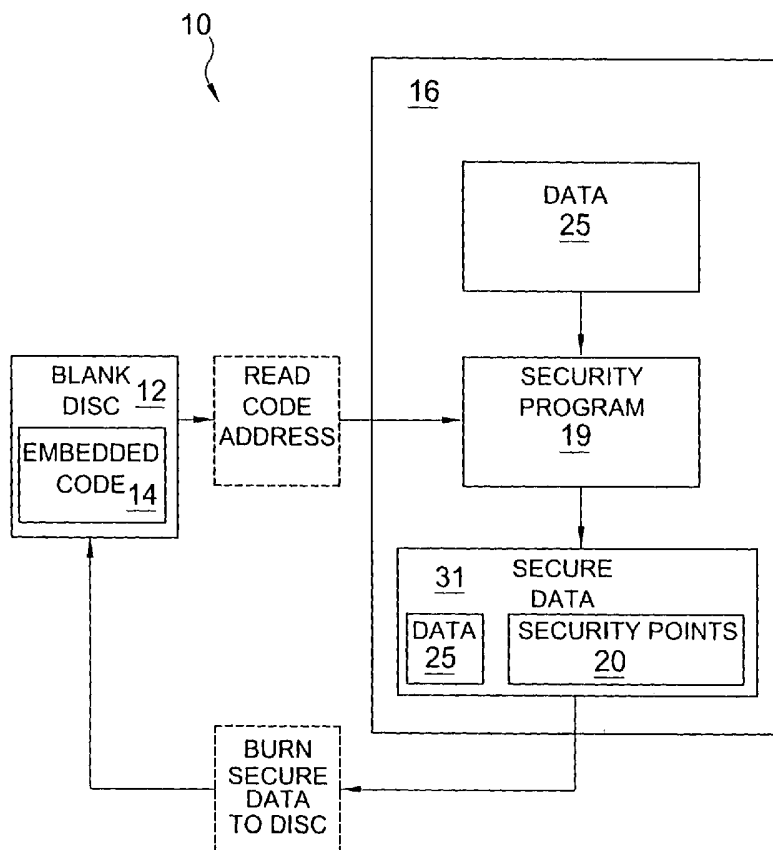
Published:

— with international search report

(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,

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: SECURITY SYSTEM FOR PREVENTING UNAUTHORIZED COPYING OF DIGITAL DATA



(57) Abstract: In a digital data security system, a data (25) is fed into the manufacturers copy device (16) as is the security software program (19) that is unique to the data (25) to be protected and the embedded security code (14) on the blank disc (12). The security program (19) uses a security reader head to read the embedded code (14) on the disc (12) and check to ensure that the proper embedded code (14) and data (25) are present. Once verified, the security program (19) will analyze the address (the location of the embedded code (14) relative to the start point of data area on the disc (12)) and inserts the security code equal to embedded code (14) and the embedded code address into the security point (20).

WO 2006/064314 A1

Security System for Preventing Unauthorized Copying of Digital Data**Description****Technical Field**

The present invention relates generally to digital media security devices and more specifically, to a digital media security device utilizing hardware and software applications to provide redundant security means to prevent the unauthorized reproduction of software programs, CD's, DVD's, MP3's and other like media that are subject to piracy.

Disclosure of the Invention

A primary object of the present invention is to provide a method and apparatus for preventing unauthorized reproductions of digital data.

Another object of the present invention is to provide a method and apparatus for preventing unauthorized reproductions of digital data wherein blank discs such as CD's, DVD's and the like are manufactured with unique readable codes embedded therein.

Yet another object of the present invention is to provide a method and apparatus for preventing unauthorized reproductions of digital data wherein a plurality of security points are integrated with the data to be protected prior to reproduction.

Still another object of the present invention is to provide a method and apparatus for preventing unauthorized reproductions of digital data wherein each security point contains the security code equal to the embedded code and the address (specific location) of the embedded security code in the security area in relation to the starting point of the data area on the disc.

Yet another object of the present invention is to provide a method and apparatus for preventing unauthorized reproductions of digital data wherein the user end standard copy head reaches a security point and reads security code and the address of the embedded security code.

Still yet another object of the present invention is to provide a method and apparatus for preventing unauthorized reproductions of digital data wherein during installation the user end copying device uses a security code reader head in the disc drive to read the embedded security code at the address provided by the security point, the copying device will stop installation if the exact embedded security code is not located at the specific address in the security area as indicated by the security point.

Yet another object of the present invention is to provide a method and apparatus for preventing unauthorized reproductions of digital data that is simple and easy to use.

Still yet another object of the present invention is to provide a method and apparatus for preventing unauthorized reproductions of digital data that is inexpensive to manufacture and operate.

Brief Description of the Drawings

In order that the invention may be more fully understood, it will now be described, by way of example, with reference to the accompanying drawing in which:

FIGURE 1 is a block diagram of the present invention during the manufacturing stage;

FIGURE 2 is a top view of secure data discs of the present invention;

FIGURE 3 is an illustrative view of the present invention;

FIGURE 4 is a flow chart of the present invention during the manufacturing stage; and

FIGURE 5 is a flow chart of the present invention during the end user stage.

The reference numerals utilized in the drawing figures are defined as follows.

- 10** Security System for Preventing the Unauthorized Copying of Digital Data
- 12** digital data disc
- 14** embedded security code
- 15** security area of disc
- 16** copying device
- 19** security software program
- 20** security point
- 22** security code
- 24** address of **14**
- 25** data
- 28** standard copy head
- 30** security code reader head
- 31** secure data
- 32** data area of **12**
- 34** start point of **32**

Detailed Description of the Preferred Embodiment

FIGURE 1 is a block diagram of the present invention **10** during the manufacturing stage. The data **25** is fed into the manufacturers copy device **16** as is the security software program **19** that is unique to the data **25** to be protected and the embedded security code **14** on the disc **12**. The security program **19** uses a security reader head to read the embedded code **14** on the disc **12** and check to ensure that the proper embedded code **14** and data **25** are present. Once verified, the security program

19 will analyze the address (the location of the embedded code **14** relative to the start point of data area on the disc **12**) and inserts the security code equal to embedded code **14** and the embedded code address into the security point **20**. The security program **19** may insert any number of security points **20** into the data **25** thereby resulting in secure data **31** to be burned through said standard copy head to the disc **12**.

FIGURE 2 is a top view of secure digital data discs **12** of the present invention. The embedded security code **14** is randomly disposed in the security area **15** of the disc **12** during manufacture. The security point **20** contains the security code **22** equal to the embedded code **14** and the embedded code address **24** relative to the starting point **34** of the data area **32**. Each embedded code address **24** relative to the start point **34** of the data area **32** provides each disc **12** with it's own unique fingerprint due to the random placement of the embedded code **14** in the code area during manufacture as demonstrated by the variation between disc A and disc B thereby making it impossible to copy the secure data from one disc to the other.

FIGURE 3 is an illustrative view of the present invention **10**. Shown is the digital data disc **12** in the copying device **16** wherein the standard copy head **28** is used on the manufacturer side to write data and on the user end to read the data and the information provided in each security point in the data area **32** of the disc **12**. The security code reader head **30** serves to read the embedded security code **14** at the specified address in the security area **15** of the disc **12**.

FIGURE 4 is a flow chart of the present invention **10** during the manufacturing stage. The present invention **10** starts with blank discs that have an embedded security code thereon that is specific for the program or data that is to be protected. The encoded disc is then placed in the copy device and the data to be protected is loaded onto the copying device. The security program of the present invention is installed onto the copying device. The security program analyzes the data that is to be copied and the embedded code to verify that they are compatible with one another and with the security program and upon verification notes the embedded code address in the security area. The security program inserts the security code equal to the embedded code and

it's address into a security point. The security program creates the secure copy by integrating as many security points in the data as is required. Each security point contains the security code equal to the embedded code and the address of the embedded code. Once all of the required security points are verified the secure data may then be copied to disc.

FIGURE 5 is a flow chart of the present invention **10** during the end user stage. When the disc is loaded on the user end, the user end copying device downloads the primary file to operate the data. The copying device continues downloading until the standard copy head reaches a security point. The copying device will then read the security code and embedded code address contained in the security point and then compare it with the embedded code at that address. A security reader head is provided specifically to read the embedded security code. If the address provided by the security point is wrong, the security reader head will not find the embedded code and loading will be discontinued. If the address is correct the security reader head will read the embedded code. Any differentiation between the embedded code and the security code provided by the security point will cause the copying device to discontinue the download and send an error message to the user. If the information provided by the security point corresponds to the embedded code, the download will continue. This procedure is repeated each time the standard copy head reaches a security point. Once verification is successful at each security point the installation can be completed and a message sent to the user informing them thereof.

CLAIMS

1. A security system for preventing the unauthorized copying of digital data comprising:

- a) a blank digital data disc manufactured with a security area having an embedded security code randomly located therein, thereby establishing an embedded code address relative to the start point of the data area on said disc;
- b) original digital data to be copied to the disc wherein each set of data to be copied has it's own unique corresponding embedded security code address on the discs it is to be copied to;
- c) a copying device on the manufacturing end for copying said original data to said disc, said copying device including a standard copy head to write the data and a security reader head to read the embedded security code on said disc;
- d) a data specific security software program to be loaded into said copying device for creating and integrating security points into said data, wherein said security program is designed to work specifically with a particular set of data and its corresponding embedded security code;
- e) a copying device including a standard copy head on the user end for copying said data from said disc; and
- f) means disposed within said user end copying device for reading said embedded security code.

2. A security system for preventing the unauthorized copying of digital data as recited in claim 1, wherein said digital data disc is a compact disc.

3. A security system for preventing the unauthorized copying of digital data as recited in claim 1, wherein said digital data disc is a digital video disc.

4. A security system for preventing the unauthorized copying of digital data as recited in claim 1, wherein said digital data is video.

5. A security system for preventing the unauthorized copying of digital data as

recited in claim 1, wherein said digital data is MP3.

6. A security system for preventing the unauthorized copying of digital data as recited in claim 1, wherein said digital data is a software program.

7. A security system for preventing the unauthorized copying of digital data as recited in claim 1, wherein said manufacturer copying device is a computer.

8. A security system for preventing the unauthorized copying of digital data as recited in claim 1, wherein the protected digital data discs are manufactured by:

- a) inserting said blank disc with embedded security code into the manufacturers copying device;
- b) feeding said original digital data into said copying device;
- c) installing said data specific security software program onto said copying device;
- d) having the security program analyze the original digital data to be protected and the embedded security code.
- e) analyzing the address of the embedded code for inclusion in said security point.

9. A security system for preventing the unauthorized copying of digital data as recited in claim 8, wherein any deviation between said security program, said data and said embedded security code will deny verification and require the operator to repeat the procedure from the beginning.

10. A security system for preventing the unauthorized copying of digital data as recited in claim 8, wherein verification of compatibility between said security program, said data and said embedded security code will allow said security program to proceed to create a final secure copy of the data by integrating a pre-selected quantity of security points into said data.

11. A security system for preventing the unauthorized copying of digital data as recited in claim 9, wherein said security program checks the data to verify that all required security points are inserted into said data.

12. A security system for preventing the unauthorized copying of digital data as recited in claim 11, wherein failure to verify the presence of all required security points in said data causes the security program to continue the security point integration process.

13. A security system for preventing the unauthorized copying of digital data as recited in claim 11, wherein verification of a secure copy of said data containing all of the required security points results in the commencement of burning said secure data onto said disc.

14. A security system for preventing the unauthorized copying of digital data as recited in claim 1, wherein each said security point includes the security code that should be equal to the embedded code on said disc and the address of said embedded security code relative to the start of the data area.

15. A security system for preventing the unauthorized copying of digital data as recited in claim 1, wherein said end user copy device is a computer.

16. A security system for preventing the unauthorized copying of digital data as recited in claim 1, wherein said end user copy device is a CD writer.

17. A security system for preventing the unauthorized copying of digital data as recited in claim 1, wherein said end user copy device is a DVD writer.

18. A security system for preventing the unauthorized copying of digital data as recited in claim 1, wherein said reader means in said end user copying device includes a security reader head which is an additional reader head exclusively for reading said

embedded security code.

19. A security system for preventing the unauthorized copying of digital data as recited in claim 1, wherein the end user initiates the download of said secure data by inserting the disc into said end user copying device and the primary file will be downloaded to operate the data and the data will continue to download until a security point is reached.

20. A security system for preventing the unauthorized copying of digital data as recited in claim 19, wherein said end user copying device retrieves said security code and its address from said security point via said standard copy head.

21. A security system for preventing the unauthorized copying of digital data as recited in claim 20, wherein said end user copying device compares said security code retrieved from said security point with said embedded security code by using said standard copy head to read said security code and said embedded code address and using said security reader head to read said embedded security code at the address contained in said security point.

22. A security system for preventing the unauthorized copying of digital data as recited in claim 21, wherein the download will cease if no embedded security code is found at said address.

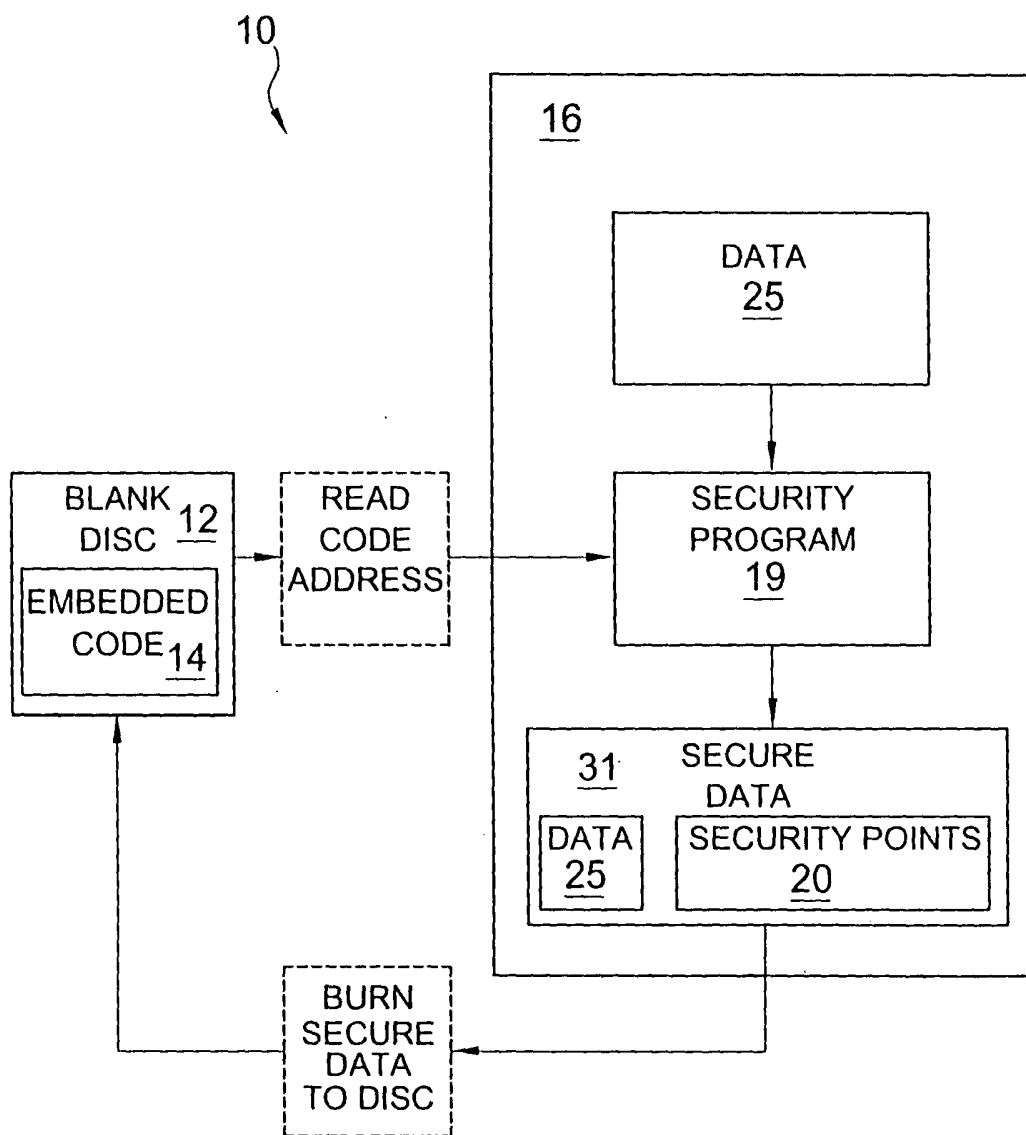
23. A security system for preventing the unauthorized copying of digital data as recited in claim 21, wherein the download will cease if the embedded security code does not match the security code provided by said security point.

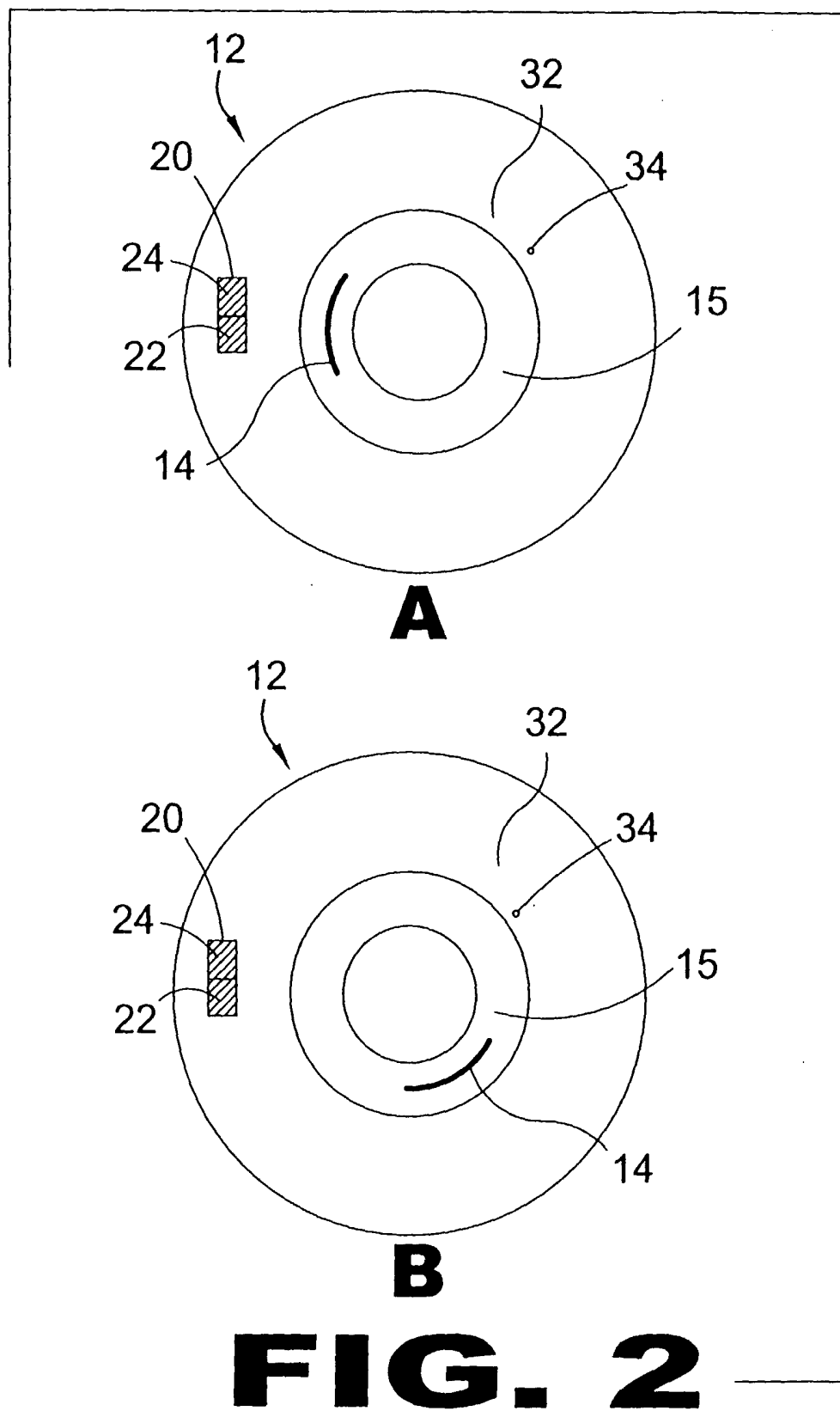
24. A security system for preventing the unauthorized copying of digital data as recited in claim 21, wherein the download will continue if the exact security code and address retrieved from said security point matches those of said embedded security code.

25. A security system for preventing the unauthorized copying of digital data as recited in claim 24, wherein the aforementioned verification process will be repeated each time a security point is reached, if every present security point is successfully verified, the download will be complete.

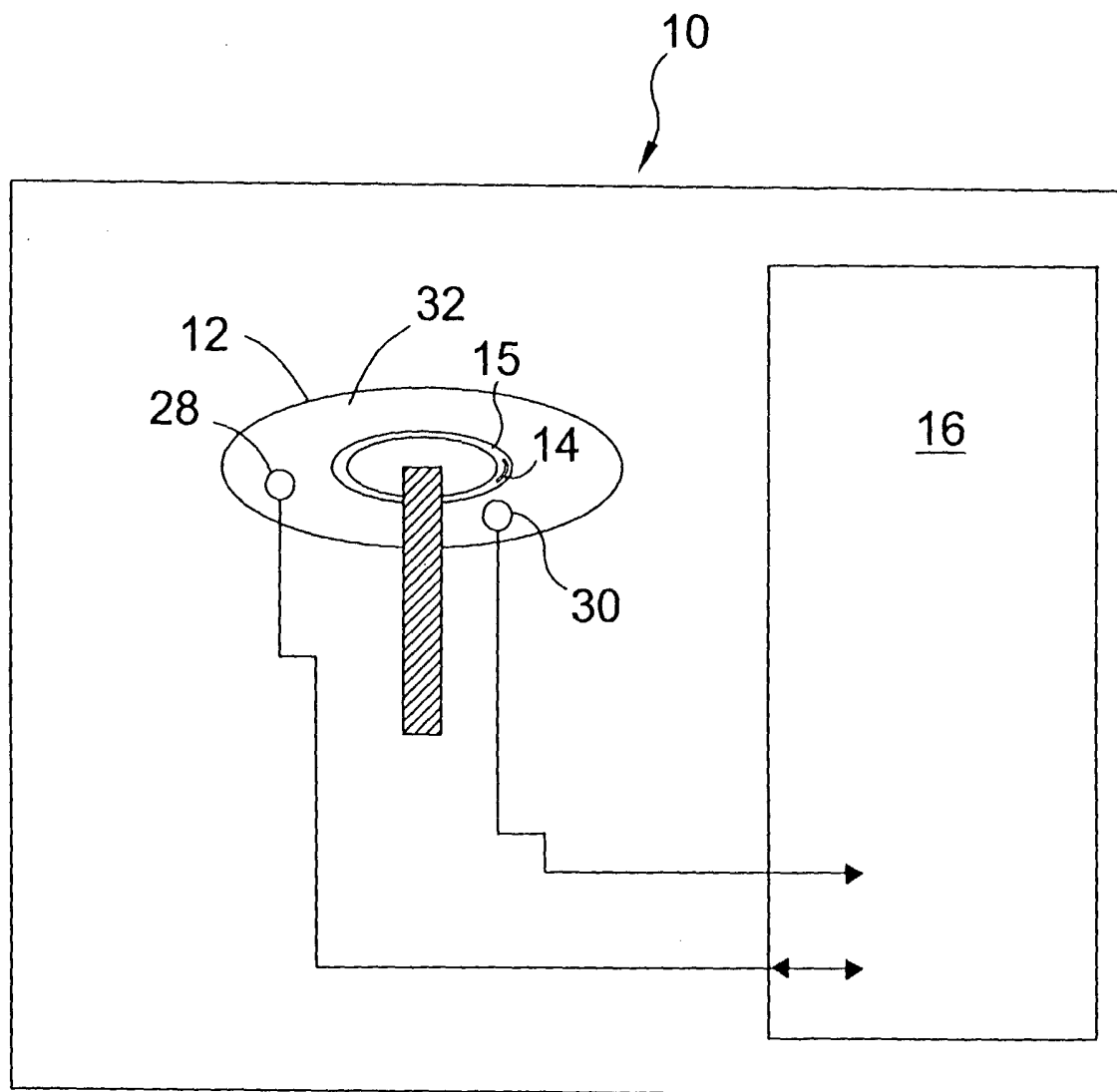
26. A security system for preventing the unauthorized copying of digital data as recited in claim 1, wherein the random placement of the address of said embedded code relative to the starting point of the data area of said disc provides each disc with a unique fingerprint that cannot be duplicated.

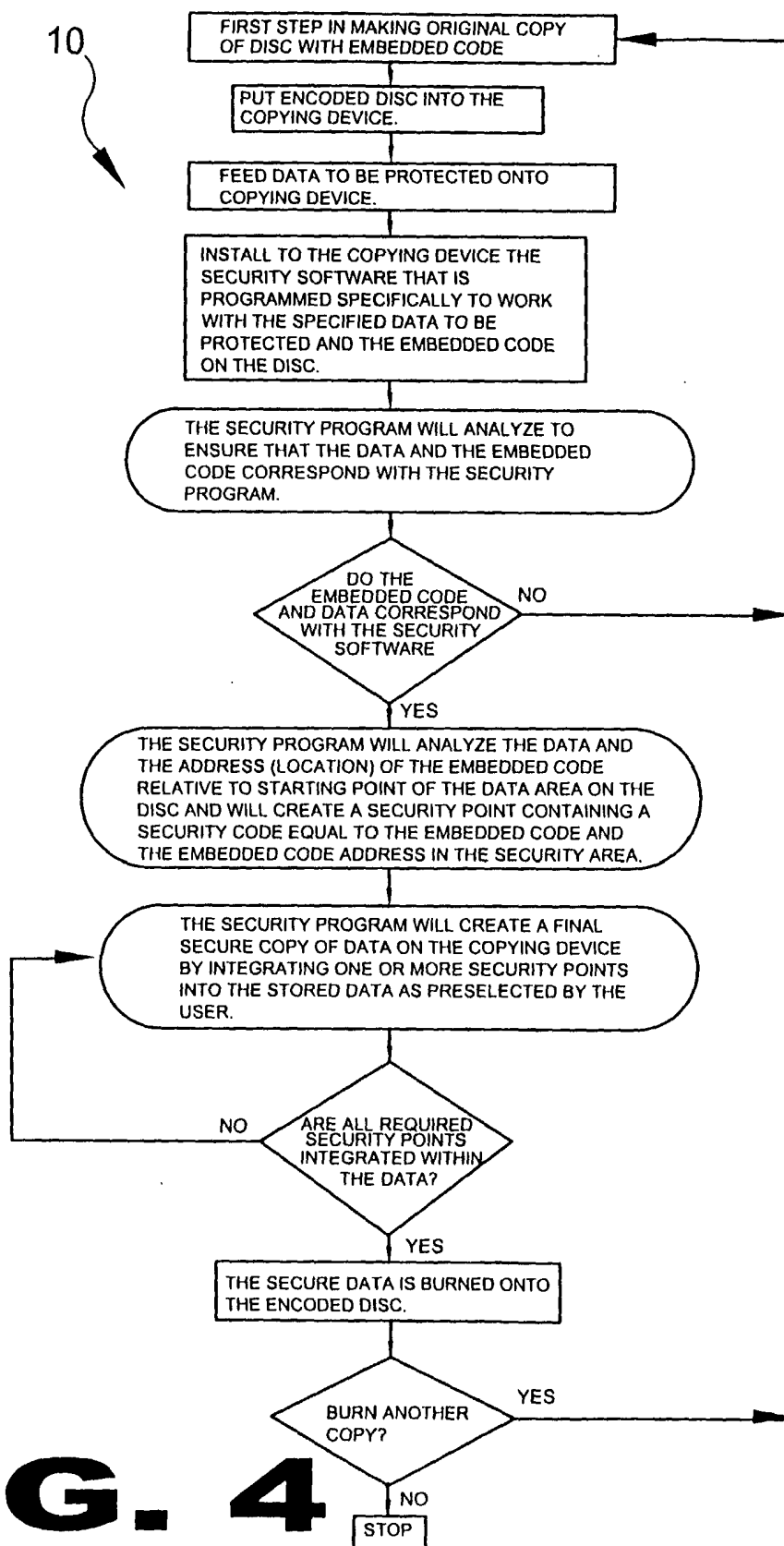
1/5

**FIG. 1**

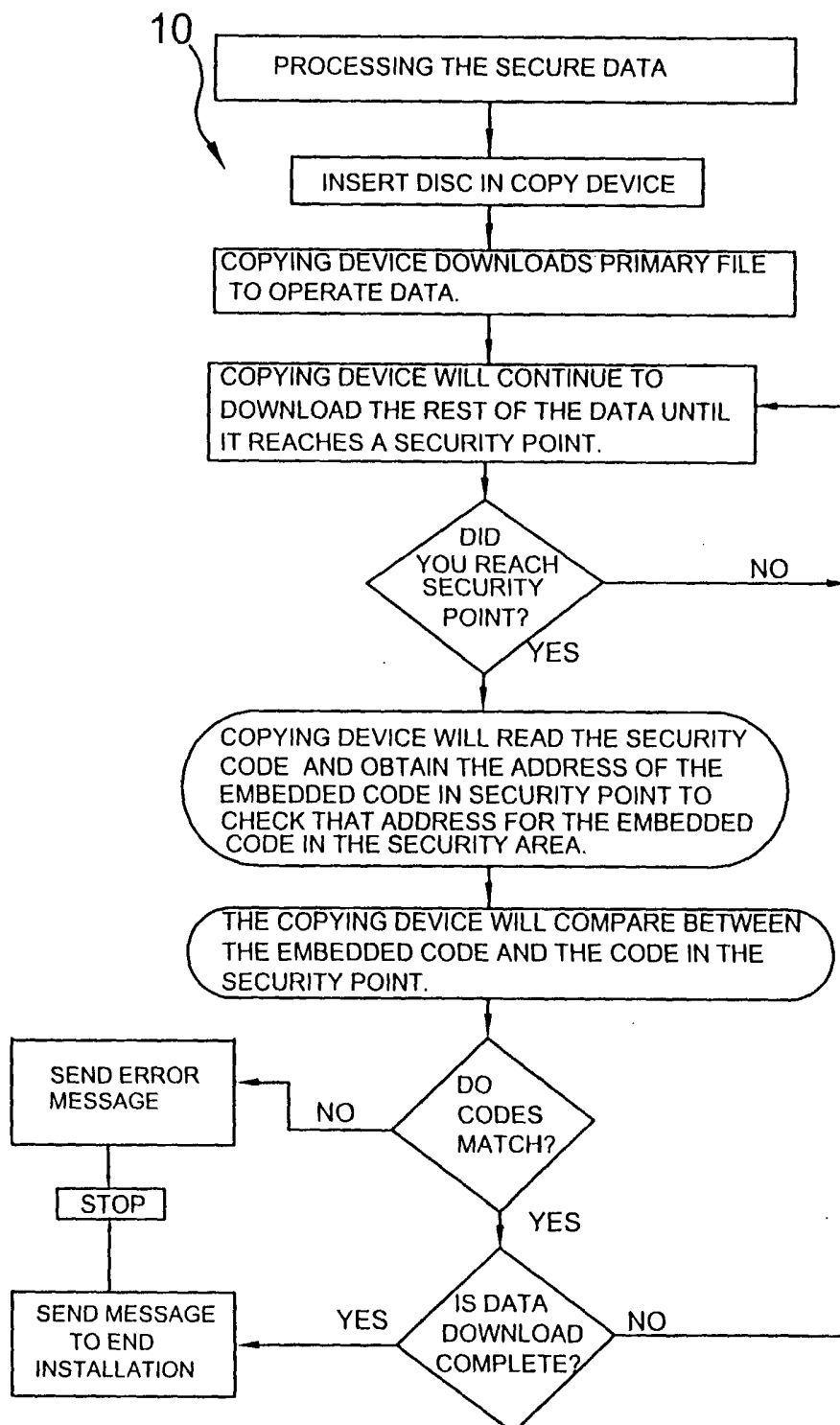


3/5

**FIG. 3**



5/5

**FIG. 5**

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/IB2005/001872

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 935 242 A (SEGA ENTERPRISES, LTD) 11 August 1999 (1999-08-11) paragraph '0007! - paragraph '0026! paragraph '0030! - paragraph '0035! paragraph '0041! - paragraph '0080! paragraph '0082! paragraph '0091! - paragraph '0098! paragraph '0102! - paragraph '0126! figures 1-5,7-11	1-26
Y	----- WO 99/17288 A (ODME INTERNATIONAL B.V; WIJN, JOSEPHUS, MARINUS; VAN DER STAPPEN, ARNO) 8 April 1999 (1999-04-08) the whole document ----- -/--	1-26

☒ 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

14 October 2005

Date of mailing of the international search report

27/10/2005

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

Barel-Faucheux, C

INTERNATIONAL SEARCH REPORT

Inter- national Application No
PCT/IB2005/001872

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 634 741 A (FUJITSU LIMITED) 18 January 1995 (1995-01-18) the whole document column 1, line 12 - line 27 column 4, line 9 - column 7, line 8 column 8, line 44 - column 11, line 43 column 12, line 43 - line 46 column 18, line 13 - column 21, line 5 column 27, line 4 - column 32, line 55 -----	1-26

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter 1al Application No
PCT/IB2005/001872

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
EP 0935242	A	11-08-1999	WO	9910884 A1	04-03-1999
			TW	408313 B	11-10-2000
WO 9917288	A	08-04-1999	AU	9191098 A	23-04-1999
			DE	69822488 D1	22-04-2004
			DE	69822488 T2	03-03-2005
			EP	1018115 A1	12-07-2000
			NL	1007123 C2	29-03-1999
			US	6865554 B1	08-03-2005
EP 0634741	A	18-01-1995	DE	69431777 D1	09-01-2003
			DE	69431777 T2	10-04-2003
			KR	186891 B1	15-04-1999