A data carrier having security mark and apparatus for handling such data carrier

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 May 2005 (26.05.2005)

PCT

(10) International Publication Number
WO 2005/048256 A2

(51) International Patent Classification[7]: G11B 20/00, G06K 19/14

(21) International Application Number: PCT/IB2004/003611

(22) International Filing Date: 4 November 2004 (04.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03300217.1 14 November 2003 (14.11.2003) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA EINDHOVEN (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **TUYLS, Pim, Theo** [BE/NL]; Société Civile SPID c/o, 156 Boulevard Haussmann, F-75008 PARIS (FR). **LINNARTZ, Johan, Paul, Marie, Gerard** [NL/NL]; Société Civile SPID c/o, 156 Boulevard Haussmann, F-75008 PARIS (FR).

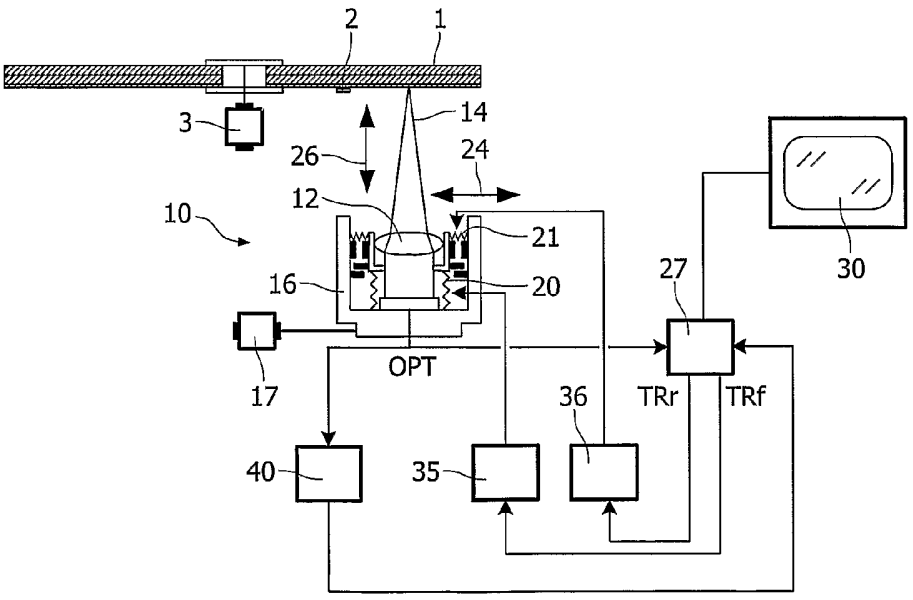
(74) Agent: **CHAFFRAIX, Jean**; Société Civile SPID, 156 Boulevard Haussmann, F-75008 PARIS (FR).

(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, 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, 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).

[Continued on next page]

(54) Title: A DATA CARRIER HAVING SECURITY MARK AND APPARATUS FOR HANDLING SUCH DATA CARRIER.



(57) Abstract: The present invention relates to a data carrier (1) having a security mark (2) in which a code is embedded, which security mark is of an optical type. For instance, the mark is of the POWF (Physical One Way Functions) type which gives a speckle pattern for a specific light. From this speckle pattern it is possible to determine a code from which it is possible to get an authentication mark or a decrypting key. In an alternative, it is possible to use a hologram from which a key or authentication mark can be derived by using a unique spatial modulation filter at the level of the analysis of the security mark.

WO 2005/048256 A2

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations 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, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, 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, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Published:

— *without international search report and to be republished upon receipt of that 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 data carrier having security mark and apparatus for handling such data carrier.

FIELD OF THE INVENTION

The present invention relates to a data carrier having a security mark.

BACKGROUND OF THE INVENTION

This kind of data carrier is well known and finds its application, especially in the avoidance of fraudulent copying of its contents.

It is well known to put some security mark on a data carrier, for instance a hole in a floppy disc in a defined place. This makes it difficult to copy the floppy disc with the hole in the right place with respect to the data. In the apparatus designed to handle the data contained in the floppy disc, means are provided for checking the place of hole and for refusing to operate if it is not found in the right place. These old measures are not very well suited for optical discs and not sufficient from a content protection point of view. The invention proposes an above-mentioned data carrier, notably an optical disc, in which measures are provided for obtaining a better authentication of the data carrier.

SUMMARY OF THE INVENTION

The invention proposes to use a security mark which is of the optical type. The main idea of the invention is to use a device which is disclosed in the article: "Physical One-Way Function" by Ravikanth Pappu et al., in SCIENCE, Vol.297, 20 September 2002, pp.2026-2030.

These and other aspects of the invention are apparent from and will be elucidated, by way of non-limitative example, with reference to the embodiment(s) described hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described in more detail, by way of example, with reference to the accompanying drawings, wherein:

- Fig.1 shows a data carrier in accordance with the invention.

- Fig.2 shows an apparatus suitable for a data carrier shown in Fig.1, according to the invention.
- Fig.3 shows another embodiment of an apparatus according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

Fig.1 shows a data carrier according to the invention. The data carrier is an optical disc 1. In accordance with the invention, a mark 2 is put on the data carrier 1. This mark may be put on a dead zone ZD of the carrier, or even on an active zone ZA , in which case the mark has the reference 2'. The mark that the invention proposes in a preferred embodiment is disclosed in the document cited above.

Fig.2 shows an apparatus in which a data carrier 1, notably an optical disc, is placed. The data carrier 1 is shown in cross-section. On this carrier, which is driven into rotation by a motor 3, an optical head 10 comprising a lens 12 focuses a laser light beam 14. This optical head 10 is placed in a moving part using a sledge 16 for large displacements and using actuators 20 and 21 for small displacements. The sledge 16 is moved by a motor 17. These displacements are performed in directions indicated by arrows 24 and 26. The head 10 comprises a photo-detector for providing a signal OPT which represents the reflection of the beam 14 onto the carrier 1. This signal OPT is applied to a signal distributor 27, which provides signals for a display unit 30 so that the contents of disc can be displayed together with some other information pertinent to the use of the apparatus. The distributor 27 also provides other signals for the operation of the apparatus, notably for acting on the sledge 16 and on actuators 20 and 21 in that signals TRf and TRr, respectively, are supplied to control devices 35 and 36.

According to the first aspect of the invention, a speckle pattern analyzing device 40 is provided which provides an authentication code when the light is reflected from the mark 2. If this authentication is wrong or absent, reading of the carrier is stopped by cutting, for instance, the signal OPT. When actuated, the sledge 16 and the actuators 20 and 21, can position the optical head 10 on the optical security mark. The optical head is thus used for reading the data recorded in the data carrier and for anlyzing the optical mark as well.

The first proposed solution is based on the theory of "Physical One Way Functions" (POWFs) [R.Pappu, et al.] cited above. According to the idea, it is proposed to embed a weakly non-linear optical microstructure into a disc. When a coherent laser beam irradiates the optical microstructure, it produces a speckle pattern that can be recorded by a camera.

Preferably, the optical head 10 is used for this purpose, i.e. for analyzing the speckle pattern. The speckle pattern analyzing device 40 applies an algorithm (e.g. based on a wavelet transform) to the recorded speckle pattern in order to turn it into a string of bits. This string of bits is then the unique identification string associated with the disc having the embedded microstructure. It is noted that several bit strings may be derived from a POWF. The bit strings that are derived depend on the way in which the POWF is challenged.

In another embodiment of the invention shown in Fig.3, an additional optical head 60 is provided for analyzing the security mark 2. This head 60 may be in a well defined position along the radius of the optical disc. This is found to be not too limitative for security as the analyzing of the mark is estimated to be strong enough for the authentication. The reading of the stream gives the string that enables the operation of the apparatus. The additional optical head 60 is set to a given wavelength, to a 3D angle, and to a spatial light modulation pattern such that the speckle pattern can be processed.

The idea is that such a microstructure is difficult to clone and that it is impossible to simulate the passage of light through such disordered media. Commercial applications could then be supported in according with the following procedure.

The content provider issues content (software, music, movies, ...) on a disc, which also contains an identification string. A microstructure with weak non-linearity properties that is difficult to clone is embedded in this disc.

The content provider then stores for various challenges (different wavelengths, 3D angles, ...) the unique fingerprint of the microstructure together with the identification string in a database.

When the user of the content asks for some service, he sends his identification string (that he finds on his disc) to the content provider.

The content provider then sends a challenge to the user in order to find out whether he is a legitimate user.

Then, the owner lets his physical device probe the microstructure in the disc in accordance with the challenge and sends the reply to the content provider.

The content provider compares the answers with the responses stored in his database according to the identification string.

If the answers correspond to the data stored in the database, the content provider knows that he is doing business with someone who is a legitimate owner of the content.

It follows that someone who has copied the content on the disc cannot copy the microstructure, so the protocol will not be successfully finished.

As a second application, the "storage" of a key is claimed. This key is derived from the POWF by irradiations with a laser beam and is embedded in an optical disc.An example is an optical microstructure (weakly non-linear optical medium) which when irradiated with a laser beam gives a unique fingerprint of the structure (as before). The robust part of the speckle pattern may be used as (part of) a key with which the content on the disc can be encrypted.

Another embodiment of the invention is to "store" the key by embedding a holographic medium (keys can be stored in contrast in a holographic medium) in the disc in which the key is stored. So the security mark is qualified as being of holographic type. Then the device 40 has to be modified by the application of a unique spatial modulation filter, which has to be put on top of the holographic medium in order to retrieve the key. Again, it is the idea that the structures are difficult to clone and can therefore be used for content protection purposes.

The term "security mark" means a mark which can be used for authentication and/or encryption. The authentication mark may be derived by feeding a challenge. The security mark may be used as a key with which the contents of optical disc can be decrypted.

Finally, this physical identifier may also be used for disc type recognition.

CLAIMS:

1) A data carrier having a security mark, characterized in that this security mark is of an optical type.

2) A data carrier as claimed in claim 1, wherein the security mark is a mark from which an authentication code can be derived in that a challenge is fed into said mark.

3) A data carrier as claimed in claim 1 or 2, characterized in that this security mark is of the POWF (Physical One Way Functions) type.

4) A data carrier as claimed in claim 1 or 2, characterized in that the security mark is of the holographic type.

5) A data carrier as claimed in claims 1 to 4, characterized in that the data carrier is an optical disc.

6) A data carrier as claimed in claim 1, 2, 3 or 5, characterized in that the security mark provides a speckle pattern from which said security is derived.

7) A data carrier as claimed in claim 4 or 5, characterized in that the security mark comprises an hologram from which said authentication code is derived.

8) An apparatus suited for handling a data carrier as claimed in claim 3 or 6, characterized in that it comprises a speckle pattern analyzing device.

9) An apparatus suited for handling a data carrier as claimed in claim 4 or 7, characterized in that it comprises a unique spatial modulation filter for determining the hologram from which an authentication code is derived.

10) An apparatus as claimed in claim 8 or 9, characterized in that it comprises one optical head for reading the data recorded in the data carrier and for reading the optical mark

11) An apparatus as claimed in claimss 8 or 9, characterized in that it comprises a first optical head for reading the data recorded in the data carrier and a second optical head for treading the optical mark.

12) An apparatus as claimed in claims 8 to 11, comprising an authentication detector for deriving said authentication code and for enabling the handling of the data carrier when the authentication code is judged to be correct.

13) Optical data carrier with a security mark from which an embedded key is derived by means of which the contents can be decrypted.

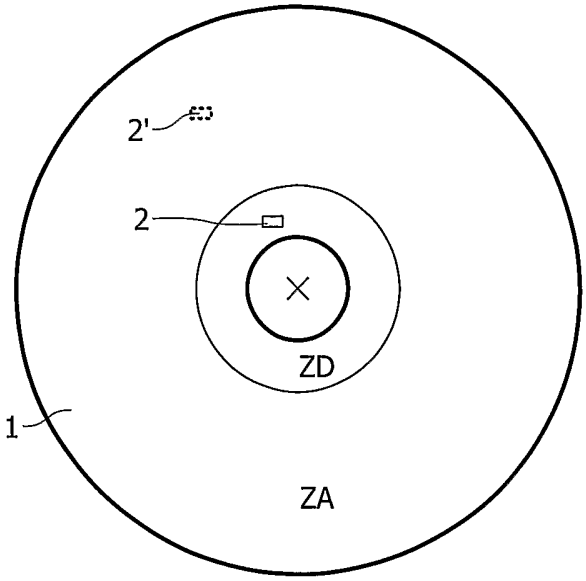


FIG.1

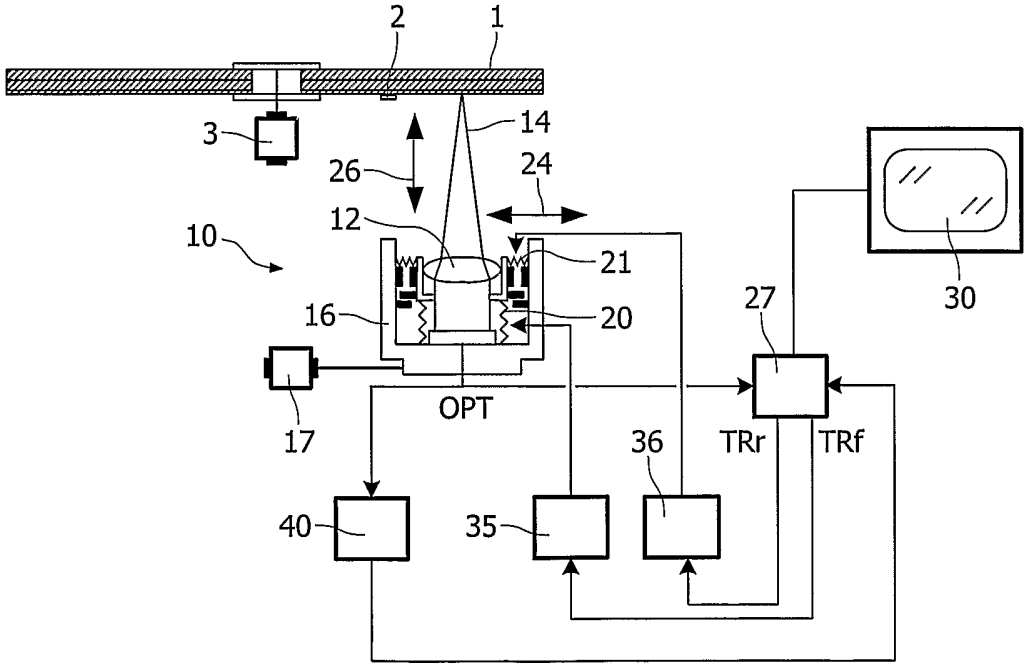


FIG.2

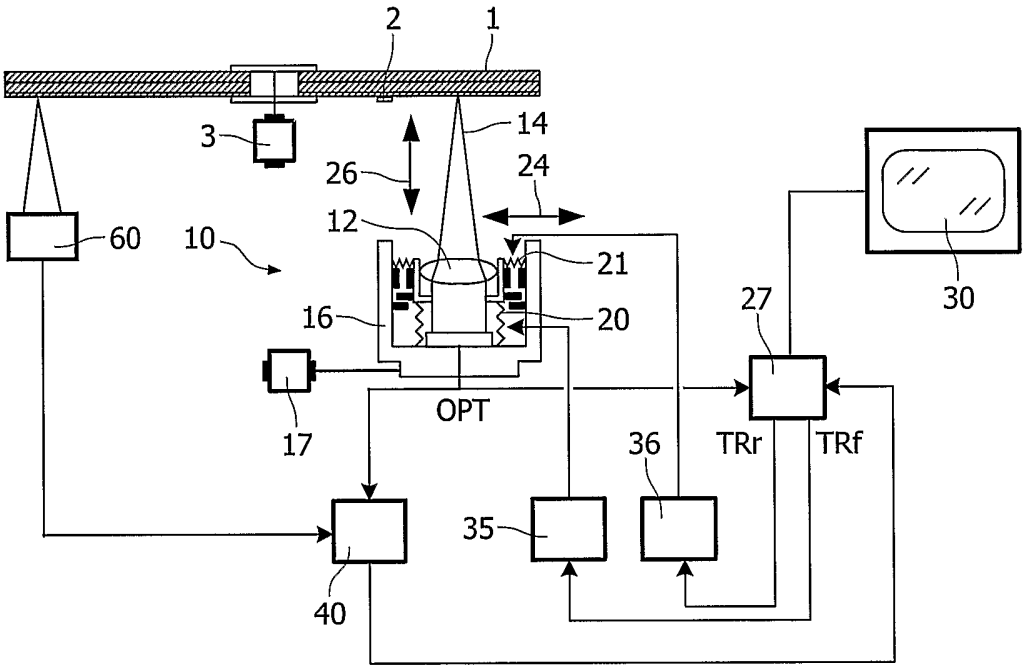


FIG.3