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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 July 2009 (16.07.2009)

PCT

(10) International Publication Number
WO 2009/088114 A1

(51) International Patent Classification:
G06F 15/00 (2006.01)

(21) International Application Number:
PCT/KR2008/000193

(22) International Filing Date: 11 January 2008 (11.01.2008)

(25) Filing Language: Korean

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **SLIM DISC CORP.** [KR/KR]; Jungbu Bldg., 4F., 968-6, Daechi-dong, Gangnam-gu, Seoul 135-848 (KR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SEO, One Hyoung** [KR/KR]; 4f., 743-2, Gwangmyeong 7-dong, Gwangmyeong-si, Gyeonggi-do 423-819 (KR).

(74) Agent: **CHANG & HAN PATENT & LAW FIRM**; 1405, Gangnam Building, 1321-1, Seocho-dong, Seocho-gu, Seoul 137-857 (KR).

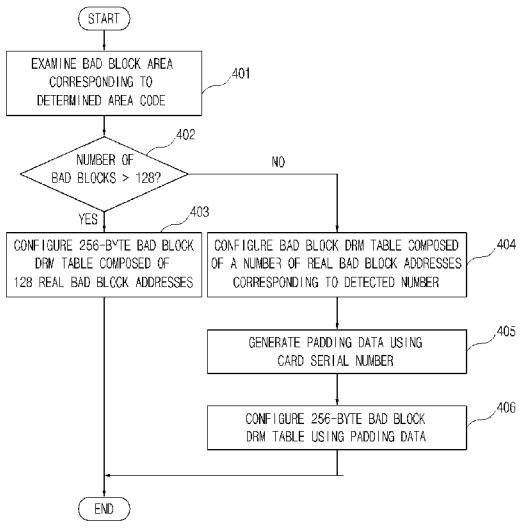
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, 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*

(54) **Title:** DRM METHOD USING BAD PATTERN, AND DIGITAL CONTENTS RECORDER/PLAYER AND METHOD USING THAT

[Fig. 4]



(57) **Abstract:** The present invention relates to a Digital Rights Management (DRM) method using bad patterns, a method of recording/playing digital contents using the DRM method, a digital contents storage medium for the methods, and a computer readable recording medium for storing programs for implementing the methods. The DRM method of the present invention includes the steps of examining unit area-based bad patterns of a memory device constituting a digital contents storage medium, and determining a bad pattern extraction area, recording an area code value of the determined bad pattern extraction area in a table select code field of a card ID, examining an area corresponding to the area code value recorded in the table select code field, and configuring a bad pattern DRM table based on information about the bad patterns, and generating a bad pattern encryption key based on the bad pattern information.

WO 2009/088114 A1

Description

DRM METHOD USING BAD PATTERN, AND DIGITAL CONTENTS RECORDER/PLAYER AND METHOD USING THAT

Technical Field

[1] The present invention relates, in general, to a Digital Rights Management (DRM) method using bad patterns, a method of recording/playing digital contents using the DRM method, a digital contents storage medium for the methods, and a computer readable recording medium for storing programs for implementing the methods, and, more particularly, to a DRM method using bad patterns, a method of recording/playing digital contents using the DRM method, a digital contents storage medium for the methods, and a computer readable recording medium for storing programs for implementing the methods, which are capable of protecting copyrights on digital contents by utilizing bad patterns (bad blocks, bad pages, bad bits, etc.) which are the physical characteristics of a memory device such as flash memory (for example, NAND flash memory or the like) as an encryption key.

Background Art

[2] Flash memory is a memory device enabling data to be uninterruptedly stored therein even when power is removed. Further, flash memory is capable of freely storing/erasing data. Such flash memory is classified into a NOR type and a NAND type according to the internal structure thereof. The NOR flash memory has a structure in which cells are connected in parallel, and the NAND flash memory has a structure in which cells are connected in series.

[3] Therefore, the NAND flash memory is mainly used for a Secure Digital (SD) card or a memory stick among various memory cards, and the NOR flash memory is mainly used for a Multimedia Card (MMC) or compact flash memory.

[4] Such flash memory has the characteristics of low power consumption and the retention of stored information without it being lost even when power is turned off. That is, flash memory is non-volatile memory to which power is continuously supplied, and is not only capable of retaining the stored information in an unchanged state even when the power is shut off, unlike Dynamic Random Access Memory (DRAM), but also is capable of freely inputting or outputting information. Accordingly, flash memory is widely used in digital Televisions (TV), digital camcorders, mobile phones, digital cameras, Personal Digital Assistants (PDA), game playing devices, MP3 players, etc.

[5] However, recently, with the realization of ultra high speed Internet infrastructures,

the improvement of the performance of PCs, and the large-capacity of storage units, a great number of illegally copied audio and video sources, and digital contents, such as educational contents, are exposed to typical users without being appropriately paid for, and are then illegally shared and used therebetween. Due thereto, an idea that digital contents is provided for free has become fixedly lodged in the mind of typical users, thus resulting in the withering of markets for recorded musical, video, and educational media.

[6] Although the problem of the protection of digital contents rights has seriously arisen due to the spreading of the illegal use, it is almost impossible in actual situations to inhibit users who have experienced the use of free contents and know the methods for using contents for free from spreading and using illegally copied digital contents, and to induce them to pay costs suitable for the rights to the contents and to use the contents. Although a service for providing digital contents over a network has recently switched to a charged service as part of such efforts, such a charged network service does not greatly influence the protection of the copyrights of copyright holders and the activation of offline media markets in the situation in which the same digital contents has already been distributed as free illegal digital contents over the Internet. The reason for this is that, if many users know methods of obtaining and using illegally copied digital contents for free when determining whether to use digital contents having the same quality using a charged service or to obtain and use illegally copied digital contents for free, they desire to obtain and use the illegally copied digital contents for free over the Internet even if some efforts are required.

[7] For example, when it is assumed that a specific singer A released his or her first record on Compact Discs (CDs), the audio sources of songs recorded on the first record of the singer may leak to Internet markets, in which infinite illegal copy is possible and digital contents can be shared among users, without any protection equipment for protecting copyrights, while the CDs are sold to users in offline stores. After the singer's CDs (audio source storage media) have leaked to illegal copy markets in this way, it is difficult to give satisfactory results even if users are prompted to pay a proper royalty and use the audio sources of digital contents through any charged services or national policies.

[8] This situation equally apply to the case of Digital Versatile Discs (DVDs) which are video storage media. Digital Rights Management (DRM) has been applied with area codes or other methods, but all of the area codes or the methods have been exposed, and thus illegally copied digital contents on DVDs have been used by users over the Internet without a proper royalty being paid.

[9] That is, by means of CDs or DVDs which are digital contents storage media currently and universally being used, at the same time that copyright holders record their

contents on such storage media and release the contents to the markets, the contents leak to markets enabling the illegal copy of the contents so that the contents may be illegally copied without any copyright protection equipment being provided.

Disclosure of Invention

Technical Problem

[10] Therefore, in the current technical fields, there is an urgently required scheme for completely protecting the copyrights of contents. An infringement of copyrights to contents stored in storage media such as CDs or DVDs cannot be sufficiently prevented due to the illegal copy of storage media such as CDs or DVDs using users' computers and sharing and illegal use of contents based on high-speed Internet infrastructures and in which a vicious circle of the withering of record, video and multimedia education markets and the reduction of creative activities is continuously repeated, and thus a subject of the present invention is to comply with such a requirement.

[11] Accordingly, an object of the present invention is to provide a DRM method using bad patterns, a method of recording/playing digital contents using the DRM method, a digital contents storage medium for the methods, and a computer readable recording medium for storing programs for implementing the methods, which are capable of protecting copyrights to digital contents by utilizing bad patterns (bad blocks, bad pages, bad bits, etc.) which are the physical characteristics of a memory device such as flash memory (for example, NAND flash memory or the like) as an encryption key.

[12] The above and other objects, features and advantages of the present invention will be more clearly understood from the following detailed description taken in conjunction with the accompanying drawings and will be more clearly described from embodiments of the present invention. Further, it will be easily understood that the objects and advantages of the present invention may be implemented by the means disclosed in the claims and combinations thereof.

Technical Solution

[13] In order to accomplish the above object, the present invention provides a Digital Rights Management (DRM) method, comprising the steps of examining unit area-based bad patterns of a memory device constituting a digital contents storage medium, and determining a bad pattern extraction area; recording an area code value of the determined bad pattern extraction area in a table select code field of a card ID; and examining an area corresponding to the area code value recorded in the table select code field, and configuring a bad pattern DRM table based on a bad pattern table.

[14] In this case, the bad pattern table is generated at a time of formatting the memory device of the digital contents storage medium, and is configured such that address values of the unit area-based bad patterns which are possible physical characteristics of

the memory device are recorded in the bad pattern table.

[15] Further, the bad pattern DRM table may be configured using only the bad pattern table.

[16] Further, the bad pattern DRM table may be configured using a card serial number field of the card ID, and is configured by padding values that are generated by sequentially performing an XOR operation on values of the bad pattern table and a value of a card serial number.

[17] Further, the bad patterns may be one of bad blocks, bad pages, and bad bits.

[18] Further, the bad pattern extraction area may be one of an area including all blocks of the memory device, an area including more than a threshold number of bad patterns, and an area including a maximum number of bad patterns.

[19] Further, the unit areas may be areas set based on multiples of 2048 blocks.

[20] Further, the threshold number may be 128, which is the number of bad blocks.

[21] Further, the bad pattern DRM table may have a size of 256 bytes.

[22] Further, the memory device may be NAND flash memory.

[23] Meanwhile, in order to accomplish the above object, the present invention provides a Digital Rights Management (DRM) method, comprising the steps of extracting physical characteristics of a digital contents storage medium; and generating an encryption key using the extracted physical characteristics of the digital contents storage medium.

[24] Further, in order to accomplish the above object, the present invention provides a Digital Rights Management (DRM) method, comprising the steps of examining unit area-based bad patterns of a memory device constituting a digital contents storage medium, and determining a bad pattern extraction area; recording an area code value of the determined bad pattern extraction area in a table select code field of a card ID; examining an area corresponding to the area code value recorded in the table select code field, and configuring a bad pattern DRM table based on information about the bad patterns; and generating a bad pattern encryption key based on the bad pattern information.

[25] Further, in order to accomplish the above object, the present invention provides a method of recording digital contents, comprising the steps of examining unit area-based bad patterns of a memory device constituting a digital contents storage medium and determining a bad pattern extraction area; recording an area code value of the determined bad pattern extraction area in a table select code field of a card ID; examining an area corresponding to the area code value recorded in the table select code field, and configuring a bad pattern DRM table based on a bad pattern table; and recording digital contents in the storage medium by utilizing the bad pattern DRM table as an encryption key.

[26] Further, in order to accomplish the above object, the present invention provides a method of recording digital contents, comprising the steps of extracting physical characteristics of a digital contents storage medium; generating an encryption key using the extracted physical characteristics of the digital contents storage medium; and recording digital contents on the digital contents storage medium using the generated encryption key.

[27] Further, in order to accomplish the above object, the present invention provides a method of recording digital contents, comprising the steps of setting an area, in which addresses of bad areas of memory used are recorded, in a header data area which is an area for storing characteristics of a memory card (digital contents storage medium), rather than in a data storage space, and recording the addresses in the set area; and extracting encryption feature values by combining the addresses of the bad areas, encrypting original contents data using the encryption feature values, and recording the encrypted contents data in a normal area of the memory and not in the bad areas.

[28] Further, in order to accomplish the above object, the present invention provides a method of recording digital contents, comprising the steps of marking bad areas of memory used, at defined locations of corresponding spare areas, as bad areas, and extracting encryption feature values by combining addresses of the bad areas; and encrypting original contents data using the encryption feature values, and recording the encrypted contents data in a normal area of the memory and not in the bad areas.

[29] Further, in order to accomplish the above object, the present invention provides a method of recording digital contents, comprising the steps of marking bad areas of memory used, at defined locations of corresponding spare areas, as bad areas, and extracting encryption feature values using specific values recorded in the memory; and encrypting original contents data using the encryption feature values, and recording the encrypted contents data in a normal area of the memory and not in the bad areas.

[30] In this case, the specific values may be serial numbers.

[31] Meanwhile, in order to accomplish the above object, the present invention provides a digital contents storage medium, wherein an area code value of a bad pattern extraction area is recorded in a table select code field of a card ID, and digital contents is recorded by utilizing a Digital Rights Management (DRM) encryption table, which is configured based on a bad pattern table by examining an area corresponding to the area code value recorded in the table select code field, as an encryption key.

[32] Further, in order to accomplish the above object, the present invention provides a method of playing digital contents, comprising the steps of when a digital contents storage medium is inserted, examining an area corresponding to an area code recorded in a table select code field of a card ID, and configuring a bad pattern Digital Rights Management (DRM) table based on a bad pattern table; examining whether patterns

having real bad pattern address values in the bad pattern DRM table are real bad patterns; and playing digital contents by utilizing the bad pattern DRM table as a decryption key on a basis of results of the examination.

[33] In this case, the step of examining whether patterns having real bad pattern address values in the bad pattern DRM table are real bad patterns may be performed to examine whether the patterns are real bad patterns by disabling a Write Protect (WP) pin and writing 0xAA55 and 0x55AA in corresponding pages of the real bad patterns.

[34] Meanwhile, in order to accomplish the above object, the present invention provides a method of playing digital contents, comprising the steps of extracting physical characteristics of a digital contents storage medium; generating a decryption key using the extracted physical characteristics of the digital contents storage medium; and playing digital contents using the generated decryption key.

[35] Further, in order to accomplish the above object, the present invention provides a method of playing digital contents, comprising the steps of when a digital contents storage medium is inserted, reading addresses of bad areas from a header data area, and calculating encryption feature values used for encryption of contents data by combining the addresses of the bad areas; and recovering original digital contents data using the encryption feature values while sequentially reading the contents data from the memory excepting the bad areas, wherein the encryption feature values are calculated by combining unique values, such as addresses of different bad areas for respective memory devices used, and thus it is physically impossible to perform perfect copy unless bad areas of memory used for copy are entirely identical to those of original memory.

[36] Further, in order to accomplish the above object, the present invention provides a method of playing digital contents, comprising the steps of when a digital contents storage medium is inserted, examining memory, reading addresses of bad areas from the memory, and calculating encryption feature values used for encryption of contents data by combining the addresses of the bad areas; and recovering original contents data using the encryption feature values while sequentially reading data from the memory excepting the bad areas, wherein the encryption feature values are calculated by combining unique values, such as addresses of different bad areas for respective memory devices used, and thus it is physically impossible to perform perfect copy unless bad areas of memory used for copy are entirely identical to those of original memory.

[37] Further, in order to accomplish the above object, the present invention provides a method of playing digital contents, comprising the steps of when a digital contents storage medium is inserted, examining memory, reading specific values recorded in the memory from the memory, and calculating encryption feature values used as the

specific values; and recovering original contents data using the encryption feature values while sequentially reading data from the memory excepting the bad areas, wherein the encryption feature values are calculated by combining unique values, such as addresses of different bad areas for respective memory devices used, and thus it is physically impossible to perform perfect copy unless bad areas of memory used for copy are entirely identical to those of original memory.

[38] Meanwhile, when the digital contents storage medium is inserted, whether the bad areas are physically formed or simply marked for copy may be determined through a process for writing/reading data in/from the bad areas.

[39] Further, in order to accomplish the above object, the present invention provides a computer-readable recording medium for storing, in a Digital Rights Management (DRM) apparatus having a processor, a program for implementing a function of examining unit area-based bad patterns of a memory device constituting a digital contents storage medium, and determining a bad pattern extraction area; a function of recording an area code value of the determined bad pattern extraction area in a table select code field of a card ID; and a function of examining an area corresponding to the area code value recorded in the table select code field and configuring a bad pattern DRM table based on a bad pattern table.

[40] Further, in order to accomplish the above object, the present invention provides a computer-readable recording medium for storing, in a Digital Rights Management (DRM) apparatus having a processor, a program for implementing a function of extracting physical characteristics of a digital contents storage medium; and a function of generating an encryption key using the extracted physical characteristics of the digital contents storage medium.

[41] Further, in order to accomplish the above object, the present invention provides a computer-readable recording medium for storing, in a digital contents recording apparatus having a processor, a program for implementing a function of examining unit area-based bad patterns of a memory device constituting a digital contents storage medium and determining a bad pattern extraction area; a function of recording an area code value of the determined bad pattern extraction area in a table select code field of a card ID; a function of examining an area corresponding to the area code value recorded in the table select code field, and configuring a bad pattern Digital Rights Management (DRM) table based on a bad pattern table; and a function of recording digital contents on the storage medium by utilizing the bad pattern DRM table as an encryption key.

[42] Further, in order to accomplish the above object, the present invention provides a computer-readable recording medium for storing, in a digital contents recording apparatus having a processor, a program for implementing a function of extracting physical characteristics of a digital contents storage medium; a function of generating

an encryption key using the extracted physical characteristics of the digital contents storage medium; and a function of recording digital contents on the digital contents storage medium using the generated encryption key.

[43] Further, in order to accomplish the above object, the present invention provides a computer-readable recording medium for storing, in a digital contents play apparatus having a processor, a program for implementing a function of, when a digital contents storage medium is inserted, examining an area corresponding to an area code value recorded in a table select code field of a card ID, and configuring a bad pattern Digital Rights Management (DRM) table based on a bad pattern table; a function of examining whether patterns having real bad pattern address values in the bad pattern DRM table are real bad patterns; and a function of playing digital contents by utilizing the bad pattern DRM table as a decryption key on a basis of results of the examination.

[44] Further, a computer-readable recording medium for storing, in a digital contents play apparatus having a processor, a program for implementing a a function of extracting physical characteristics of a digital contents storage medium; a function of generating a decryption key using the extracted physical characteristics of the digital contents storage medium; and a function of playing digital contents using the generated decryption key.

Advantageous Effects

[45] The present invention is advantageous in that, since physical characteristics such as the bad patterns (bad blocks, bad pages, bad bits, etc.) of digital contents media implemented as, for example, NAND flash memory, are utilized as encryption factors, different unique DRM encryption tables (bad pattern DRM tables) may be provided for respective digital contents storage media. That is, when there are 100 digital contents storage media, they are encrypted using 100 different bad pattern DRM tables (DRM encryption tables).

[46] Further, since the present invention is configured to acquire bad patterns which are the physical characteristics of a relevant storage medium, generate bad pattern DRM tables and encrypt digital contents using the bad pattern DRM tables during a media authentication process, without using tables previously recorded in specific areas of a digital contents storage medium, the logical copy of the storage medium is meaningless. This will be verified at a real bad pattern examination step performed by a media authentication unit, which will be described in detail later.

[47] Further, since the present invention is configured to acquire bad patterns which are the physical characteristics of a relevant storage medium, generate bad pattern DRM tables, and examine real bad patterns on the basis of the generated bad pattern DRM tables during a digital contents media authentication process, the physical copy of

storage media is meaningless.

[48] Furthermore, the present invention is advantageous in that, since the copy of digital contents recorded on digital contents storage media to which DRM apply is actually impossible and meaningless due to the above reasons, copyrights to digital contents can be sufficiently protected compared to existing storage media such as CDs or DVDs which are frequently illegally copied, so that reasonable compensation may be provided to copyright holders, thus realizing the creation of digital contents and development of related technologies.

Best Mode for Carrying out the Invention

[49] The above and other objects, features and advantages of the present invention will be more clearly understood from the following detailed description taken in conjunction with the accompanying drawings, and thus those skilled in the art can easily implement the technical spirit of the present invention. In the following description of the present invention, if detailed descriptions of related well-known constructions or functions are determined to make the gist of the present invention unclear, the detailed descriptions will be omitted. Hereinafter, embodiments of the present invention will be described in detail with reference to the attached drawings.

[50] In the embodiment of the present invention, for convenience of description, a specified file system suitable for a read only storage medium, rather than a public file system such as a File Allocation Table (FAT) 16 or FAT32, is described by way of example together with the fundamental structure of NAND flash memory. However, it should be noted that the present invention is not limited to this example.

[51] The construction of the file system, as described later, is also characterized in that digital contents is encrypted using the bad pattern DRM table (DRM encryption table) of a previously fixed storage medium at the time of recording the digital contents. That is, in the structure of the file system, the entire area, excepting a minimum region required to detect the bad pattern DRM table (DRM encryption table) of the storage medium, is encrypted through relevant Digital Rights Management (DRM), and thus typical access to the area is blocked.

[52] Generally, the physical block number '0' of the flash memory (hereinafter referred to as the 'zero block') is used by the manufacturing company thereof to guarantee that the block is not a bad block. Therefore, in the zero block, format-related information of the storage medium, a medium ID (card ID), etc. are stored.

[53] Hereinafter, a block in which bad bits are present (that is, a bad block) according to bad bit information is described by way of example. However, it should be noted that the present invention can also be equally applied to a page (that is, a bad page) in which bad bits are present according to bad bit information. Therefore, in the case of

bad blocks, a bad block DRM table may be used as a DRM encryption table, and in the case of bad pages, a bad page DRM table may be used as a DRM encryption table. The bad block DRM table and the bad page DRM table may be collectively called a 'bad pattern DRM table (DRM encryption table)'.

[54] With reference to FIG. 1, the construction of the zero block of flash memory is described below.

[55] In a Master Boot Recorder (MBR) corresponding to 'page number 0 of the zero block', information about the construction of the flash memory and the file system is recorded.

[56] Further, in 'page numbers 1 to 5 of the zero block', bad block marking information is recorded. In particular, in 'page number 9 of the zero block', a card ID corresponding to a medium ID is stored. Such a card ID is composed of pieces of specific information (for example, card version, a DRM table select code, an area code, a manufacturing company code, a copyright holder ID [writer ID], and card serial number information) of a digital contents storage medium implemented as flash memory, as shown in FIG. 2.

[57] In particular, in the DRM table select code field of the card ID (page number 9 of zero block), information about the code of an area (area code) in which bad patterns (bad blocks, bad pages, bad bits, etc.) desired to be used for a DRM encryption table (bad block DRM table) are present (that is, an area having more than a threshold number of bad blocks or an area having a maximum number of bad blocks) is recorded when DRM using bad patterns (bad blocks, bad pages, bad bits, etc.) which are the physical characteristics of the storage medium is implemented.

[58] At this time, the bad pattern extraction area of the storage medium implemented as flash memory may be either an entire block area of the flash memory or only a specific area. Further, the DRM encryption table (bad block DRM table) using the extracted bad patterns may be configured to have various sizes, such as 128 bytes, 256 bytes, or 512 bytes.

[59] However, for convenience of description, in the present embodiment, an example will be described on the assumption that the DRM encryption table has a size of 256 bytes and the bad pattern extraction area required for the configuration of the DRM encryption table is a specific area of the flash memory, rather than the entire area. However, it should be noted that the present invention is not limited to this example.

[60] In the above description, the term 'specific area' means that, for example, all the blocks of the flash memory can be divided by 2048 blocks and can be processed thereby. That is, as shown in FIG. 3, the bad pattern extraction area required for the configuration of the DRM encryption table (bad block DRM table) is determined in such a way that respective areas are set based on multiples of 2048 blocks in all the

blocks of the flash memory, and an area complying with a specific criterion, among the areas, is determined to be a bad pattern extraction area required for the configuration of the DRM encryption table (bad block DRM table).

[61] Here, the term 'specific criterion' means a criterion required to determine whether a relevant area is an area suitable for the configuration of a 256-byte DRM encryption table (bad block DRM table). For example, when an area including more than a threshold number of (for example, 128) bad blocks is present, the relevant area is determined to be the bad pattern extraction area. However, when an area including more than 128 bad blocks is not present, an area including a maximum number of bad blocks, among the plurality of areas (areas set based on multiples of 2048 blocks), is determined as the bad pattern extraction area required for the configuration of the DRM encryption table (bad block DRM table).

[62] The bad pattern extraction area is determined based on a bad block table generated while a memory card is formatted at the time of manufacturing the digital contents storage medium (the memory card). The area code value of the relevant area determined at that time is recorded in the DRM table select code field of the card ID of FIG. 2.

[63] FIG. 4 is a flowchart showing an example of a bad block DRM table configuration method for digital rights management according to an embodiment of the present invention. The flowchart shows a procedure for examining an area corresponding to the area code recorded in the DRM table select code field of the card ID, and configuring a bad block DRM table (DRM encryption table).

[64] As described above, the procedure for configuring the bad block DRM table (DRM encryption table) is described below. In all the blocks of the flash memory, respective areas are set based on multiples of the number of blocks (for example, based on multiples of 2048 blocks). Among the areas, a bad pattern extraction area meeting a specific criterion (for example, an area having more than a threshold number of [for example, 128] bad blocks, or an area having a maximum number of bad blocks), is determined on the basis of the bad block table. The code value of the relevant area (area code) is recorded in the DRM table select code field of the card ID.

[65] Thereafter, the area corresponding to the determined bad pattern extraction area (that is, the area corresponding to the area code) is examined at step 401, so that the bad block DRM table (DRM encryption table) can be configured, as shown in FIG. 5 or 7, at steps 402 to 406. Here, FIG. 5 illustrates a 256-byte bad block DRM table (DRM encryption table), generated on the basis of the bad block table of area 1 (block 0 ~ block 2047) having more than 128 bad blocks, and FIG. 7 illustrates a 256-byte bad block DRM table (DRM encryption table), generated by attaching padding data to the bad block table (refer to FIG. 6) of area 2 (block 2048 ~ block 4095), having 128 or fewer

bad blocks.

[66] This is described in detail. When an examination target area (area corresponding to the area code) has more than 128 sufficient bad blocks so as to configure a 256-byte bad block DRM table (DRM encryption table) at step 402, a 256-byte bad block DRM table (DRM encryption table)[refer to FIG. 5] composed of 128 real bad block addresses is generated on the basis of the bad block table of an area having more than 128 (256 byte) bad blocks (for example, area 1 having blocks 0 to 2047) at step 403.

[67] FIG. 5 illustrates a 256-byte bad block DRM table (DRM encryption table) generated on the basis of the bad block table corresponding to area 1 (block 0 ~ block 2047) having more than 128 bad blocks. That is, more than 128 real bad blocks are present in the area 1, so that the 256-byte bad block DRM table (DRM encryption table) is configured using only the addresses of the bad blocks. In this case, the padding operation of FIG. 7 is not required.

[68] Meanwhile, when a relevant area (examination target area, that is, the area corresponding to the area code) does not include bad blocks sufficient to configure a 256-byte bad block DRM table (DRM encryption table) at step 402, a padding operation is performed using an appropriate method, as described later, at steps 404 and 405, thus configuring the 256-byte bad block DRM table (DRM encryption table) [refer to FIG. 7] at step 406. In this case, the bad block DRM table (DRM encryption table) is composed of 18 (36 byte) real bad block addresses and 110 (220 byte) pieces of padding data.

[69] Here, as a padding method, various methods may exist, but, in the present embodiment, the bad block DRM table (DRM encryption table) is configured using the card serial number field (16 byte) of the card ID. For example, the 256-byte bad block DRM table (DRM encryption table) of FIG. 7 is configured using padding values obtained by sequentially performing an XOR operation on existing real bad block table values and a card serial number value.

[70] That is, in the bad block table of area 2 having 128 or fewer bad blocks of FIG. 6, an XOR operation is sequentially performed on the real bad block table values and the card serial number value, so that a 256-byte bad block DRM table (DRM encryption table) [refer to FIG. 7] is generated by attaching padding data (that is, values obtained by sequentially performing an XOR operation on the bad block table values and the card serial number value) to the bad block table (that is, the bad block table having 18 [36 byte] real bad block addresses in FIG. 6) of area 2 (block 2048 to block 4095) having 128 or fewer bad blocks. In this case, the bad block DRM table (DRM encryption table) is composed of 36 bytes of real bad block addresses and 220 bytes of padding data (*0x09, 0x10, 0x0B, 0x17, ...*).

[71] FIG. 6 illustrates a bad block table generated on the basis of 128 or fewer bad blocks

(for example, 18 [36 bytes] real bad blocks) in area 2 (block 2048 ~ block 4095). That is, when only 18 bad blocks (36 byte) from 0x0812 to 0x0CFE are present in area 2, the bad block table corresponding thereto is exemplified.

[72] In order to generate a 256-byte bad block DRM table (DRM encryption table) on the basis of the bad block table composed of 18 (36 byte) real bad block addresses of FIG. 6, a padding operation must be performed. If the card serial number is assumed to be "0x01020304050607080900010203040506", padding values obtained by sequentially performing an XOR operation on the bad block table values and the card serial number value are given as '0x09', '0x10', '0x0B', '0x17', ...

[73] Therefore, the padding data (values obtained by sequentially performing an XOR operation on the bad block table values and the card serial number value) is attached to the bad block table (refer to FIG. 6) composed of 18 (36 byte) real bad block addresses, and thus the 256-byte bad block DRM table (DRM encryption table) is configured, as shown in FIG. 7.

[74] The bad block DRM table (DRM encryption table) formed using the above-described method is a unique factor that is determined according to the possible physical characteristics of a given storage medium (that is, the memory card implemented as a memory device), and that is unique in all probability.

[75] FIG. 8 is a flowchart showing an example of a digital contents recording method according to an embodiment of the present invention, in which a procedure for manufacturing a digital contents storage medium is shown.

[76] First, the flash memory (for example, NAND flash memory) of the digital contents storage medium (memory card implemented as a memory device) is formatted to a low level at step 801, so that bit-based bad pages (pages including bad bits) or bit-based bad blocks (blocks including bad bits) are examined by writing 0xAA55, and the pages or blocks including bad bits are marked as bad pages or bad blocks at step 802. That is, blocks having bad bits according to bad bit information detected at the time of initialization (formatting) are marked as bad blocks, and pages having bad bits according to bad bits detected at the time of initialization are marked as bad pages.

[77] Thereafter, the bad blocks are recorded in a bad block table at step 803. At this time, the bad block table may be provided for each of areas into which all the blocks of the flash memory are divided by 2048 blocks.

[78] Next, after the flash memory has been formatted to a low level, an area satisfying a specific condition (criterion) is determined with reference to the recorded bad block table, and then the area code value of the relevant area is recorded in the DRM table select code field of the Card ID (page number 9 of the zero block) at step 804. For example, all the blocks of the flash memory are divided by 2048 blocks, and then respective areas are set. Among the areas, an area satisfying the specific condition

(criterion) is determined to be a bad pattern extraction area required for the configuration of the DRM encryption table (bad block DRM table), and thereafter the area code of the determined area is recorded in the DRM table select code field of the card ID.

[79] Here, the term 'specific condition (criterion)' means a criterion required to determine whether a given area is an area suitable for the configuration of a 256-byte DRM encryption table (bad block DRM table). For example, an area having more than a threshold number of bad blocks, or an area having a maximum number of (for example, 128) bad blocks may be determined to be a bad pattern extraction area. At this time, the determination of the bad pattern extraction area may be performed to assign priority for the determination of an area in such a way that whether an area having more than a threshold number of (for example, 128) bad blocks is present is determined, and an area having a maximum number of bad blocks, among the plurality of areas (areas set based on multiples of 2048 blocks), is determined to be the bad pattern extraction area if it is determined that the area is not present.

[80] The area code value of the area determined to be the bad pattern extraction area is recorded in the DRM table select code field of the card ID of FIG. 2 at step 804.

[81] Thereafter, if the examination target area (area corresponding to the area code) has more than 128 bad blocks sufficient to configure a 256-byte bad block DRM table (DRM encryption table) at step 805, a 256-byte bad block DRM table (DRM encryption table) [refer to FIG. 5], composed of 128 real bad block addresses, is generated on the basis of the bad block table of the area having more than 128 (256 byte) bad blocks at step 806. This means that, since more than 128 (256 byte) real bad blocks are present in, for example, area 1 (block 0 ~ block 2047), the 256-byte bad block DRM table (DRM encryption table) can be configured using only the addresses of the real bad blocks.

[82] Meanwhile, when the relevant area (examination target area [area corresponding to the area code]) does not include bad blocks sufficient to configure a 256-byte bad block DRM table (DRM encryption table) at step 805, a padding operation is performed, so that the 256-byte bad block DRM table (DRM encryption table) [refer to FIG. 7] is generated at step 807. That is, the 256-byte bad block DRM table (DRM encryption table) is configured, as shown in FIG. 7, using padding values generated by sequentially performing an XOR operation on the real bad block table values and the card serial number value.

[83] For example, in the bad block table of area 2 having 128 or fewer bad blocks of FIG. 6, an XOR operation is sequentially performed on the real bad block table values and the card serial number value, thus generating a 256-byte bad block DRM table (DRM encryption table) [refer to FIG. 7], in which padding data (values generated by se-

quentially performing an XOR operation on the bad block table values and the card serial number value [for example, '0x0102030405060708090001020304050 6']) is attached to the bad block table of area 2 (block 2048 ~ block 4095) (that is, in FIG. 6, a bad block table having 18 (36 byte) real bad block addresses]). As a result, the bad block DRM table (DRM encryption table) composed of 36 bytes of real bad block addresses and 220 bytes of padding data (*0x09, 0x10, 0x0B, 0x17,...*) is configured.

[84] Next, after the bad block table, extracted and recorded in the zero block, is deleted while the flash memory is formatted to a low level at step 808, digital contents is recorded on the digital contents storage medium implemented as the memory device (for example, NAND flash memory) by utilizing the generated bad block DRM table (DRM encryption table) as an encryption key at step 809.

[85] FIG. 9 is a flowchart showing an example of an authentication process for playing digital contents according to an embodiment of the present invention, in which a procedure for playing digital contents is shown.

[86] First, when a digital contents storage device implemented as a memory device (for example, NAND flash memory) is inserted into a digital contents provision apparatus (media play apparatus) at step 901, the digital contents provision apparatus (media play apparatus) reads the information of the card ID (page number 9 of zero block), and starts an authentication process at step 902. At this time, in the DRM table select code field of the card ID, information about the code of an area (area having more than a threshold number of bad blocks, or an area having a maximum number of bad blocks), in which bad patterns (bad blocks, bad pages, bad bits, etc.) desired to be used for a DRM decryption table (bad block DRM table) are present, is recorded, and thus the information of the card ID is determined at the time of playing media.

[87] Therefore, an area corresponding to the DRM table select code of the card ID is examined at step 903, so that the bad block DRM table (DRM decryption table) is configured at step 904.

[88] For example, when the area corresponding to an area code recorded in the DRM table select code field has more than 128 sufficient bad blocks, a 256-byte bad block DRM table (DRM decryption table) [refer to FIG. 5] composed of 128 real bad block addresses is configured on the basis of the bad block table of the area having more than 128 (256 byte) bad blocks.

[89] However, when the area corresponding to the area code recorded in the DRM table select code field does not include bad blocks sufficient to configure a 256-byte bad block DRM table (DRM decryption table), a padding operation is performed, and thus a 256-byte bad block DRM table (DRM decryption table)[refer to FIG. 7] is configured. That is, through the use of padding values generated by sequentially performing an XOR operation on the real bad block table values and the card serial

number value, the 256-byte bad block DRM table (DRM decryption table) of FIG. 7 is configured.

[90] Thereafter, in the bad block DRM table (DRM decryption table) configured in this way, whether blocks corresponding to the real bad block table values, rather than the padding values, are real bad blocks is determined at step 905. For example, whether blocks having real bad block addresses are real bad blocks in the bad block DRM table (DRM decryption table) of FIG. 7, composed of 36 bytes of real bad block addresses and 220 bytes of padding data (0x09, 0x10, 0x0B, 0x17, ...), is determined.

[91] A procedure for determining whether blocks are real bad blocks is described below. For example, about 10 bad blocks are randomly selected from the real bad block table, and whether the selected bad blocks are real bad blocks is examined at step 906. At this time, a Write Protect (WP) pin is disabled, and 0xAA55 and 0x55AA are written in the corresponding page of each real bad block, and thus whether the bad blocks are real bad blocks is determined at step 907.

[92] If it is determined at step 907 that bad blocks are real bad blocks, a predetermined number of (about 10) real bad blocks are additionally examined using the same method at step 906. Similarly, for the additionally selected bad blocks, a procedure for disabling a WP pin and writing 0xAA55 and 0x55AA in the corresponding page of each real bad block is performed at step 907.

[93] In this way, when the additionally performed examination on the real bad blocks has succeeded (that is, when the authentication of the use of the medium has succeeded), the use of the digital contents medium (play or reading) is permitted at step 908.

[94] Therefore, when the authentication of the use of the medium has succeeded, digital contents data is provided to the user while being decrypted using the bad block DRM table (DRM decryption table) at step 909.

[95] However, when the authentication of the use of the medium has failed, notification of the failure of authentication is provided to the user, and request the user to check the digital contents storage medium at step 910.

[96] In the above procedure for determining whether bad blocks are real bad blocks, several conditions may be given in relation to the determination of which is the number of real bad blocks that are examination targets, the determination of whether encryption and decryption are to be applied to the entire digital contents in the encryption and decryption of digital contents by using the generated bad block DRM table (DRM encryption/decryption table), or the determination of whether encryption and decryption are to be applied only to a specific area. However, in the present embodiment, the case where application is performed on the basis of values corresponding to the lower 4 bits of the last bad block address of the real bad block table is described by way of example.

[97] For example, when the bad block table is given as shown in FIG. 6 (that is, the bad block table of FIG. 6 is a bad block table having 18 (36 byte) real bad block addresses), the last bad block address is '0xFE', and the lower 4 bits thereof are '0x0E (= a decimal number of 14)', and thus the above conditions are determined on the basis of the 'decimal number of 14'.

[98] That is, the determination of real bad blocks is performed by examining bad blocks corresponding to a multiple of 14. If the number of bad blocks which are examination targets does not exceed 5, bad blocks from a first bad block are additionally included in the sequential examination targets, and thus the total number of examination target bad blocks is maintained at at least 5.

[99] Similarly, a description will be made on the basis of the above conditions. The encryption of digital contents data is also performed on blocks having block addresses corresponding to a multiple of 14. Decryption thereof is also performed on the basis of the same criterion and condition as those of encryption.

[100] The above-described method of the present invention can be applied to various fields in consideration of the entire performance and other conditions of the system to which DRM is applied. For example, the method can be applied to an asymmetric encryption system.

[101] An example of the application is described below. As described above, a bad pattern DRM table (DRM encryption table) is generated using bad patterns. A seed key is generated using a Hash function that uses the bad pattern DRM table (DRM encryption table) as a transform parameter. From the seed key, a public key and a private key are generated through a Public Key Infrastructure (PKI) algorithm (Rivest-Shamir-Adleman [RSA], Elliptic Curve Cryptography [ECC], etc.), and they can be applied to PKI solutions that have been used in various existing fields. This shows that the bad patterns of each of digital contents storage media are factors causing the generation of a private key, and the contents of the private key does not need to be logically recorded using any method, thus further strengthening the security of an asymmetric encryption system using the above example. That is, a client may download contents data, encrypted by a server using the public key, and may decrypt the encrypted contents data using the private key extracted from the digital contents data.

[102] As described above, when the physical characteristics (bad blocks, bad pages, bad bits, etc.) of the memory device constituting the digital contents storage medium (memory card) in which respective pieces of digital contents are recorded, are used as an encryption key, respective digital contents storage media have different bad block DRM tables (DRM encryption tables). Because of this, a disadvantage in that existing DRM using a specific physical algorithm or an encryption table loses its value as

DRM, as the specific algorithm or the encryption table of the existing DRM is open to the public, can be overcome.

[103] Even if a memory device (for example, NAND flash memory) constituting the digital contents storage medium is digitally copied using any of the methods used for the purpose of illegal copy, or even if a digital contents storage medium identical to the original is copied using a memory dump method in a physical manner, the copied digital contents storage medium is not effective. The reason for this is that, even if a digital contents storage medium physically identical to the original is copied, the bad patterns (bad blocks, bad pages, bad bits, etc.) which are physical characteristics of a memory device (for example, NAND flash memory) constituting the storage medium are not copied. That is, although even marking of bad blocks or bad pages is copied in the spare areas of a flash memory block, such marking cannot physically correlate to real bad blocks or bad pages. As a result, a copied digital contents storage medium (even bad patterns are not copied) fails in authentication in the real bad block examination procedure of a digital contents media authentication process when the storage medium is used (played). Accordingly, the copied digital contents storage medium is then determined to be an ineffective storage medium.

[104] For that reason, the present invention can sufficiently protect the digital contents data of a copyright holder, unlike existing storage media, such as a CD or a DVD, having contradiction indicating that the existing storage media become media capable of providing profit to the copyright holder of digital contents data, and, simultaneously, they become media through which the copyright holder's digital contents is infinitely copied because they are infinitely exposed to illegal copy by typical users.

[105] Meanwhile, other examples of methods of preventing the illegal copy of the entirety of the flash memory may include an encryption/decryption method using different bad areas (blocks, pages, sub-pages, or locations) for respective memory devices.

[106] For example, an area in which the addresses of bad areas of memory used (blocks, pages, sub-pages, or locations) are recorded, is set in a header data area in which the characteristics of the memory card (digital contents storage medium) are recorded, rather than a data storage space, and the set area is recorded. The addresses of the bad areas are combined with each other to extract encryption feature values (for example, encryption feature values based on a bad block DRM table [DRM encryption table]). Thereafter, original contents data is encrypted using such encryption feature values, and thus the encrypted contents data is recorded in the normal areas of the memory and not in the bad areas of the memory.

[107] Thereafter, when the memory card is inserted into a play apparatus, the play apparatus reads the addresses of the bad areas from the header data area, calculates encryption feature values (for example, encryption feature values based on the bad block

DRM table [DRM encryption table]) used for the encryption of contents data by combining the addresses of the bad areas with each other, and recovers original contents data using the encryption feature values while sequentially reading data from the memory excepting the bad areas. At this time, the encryption feature values are calculated through a combination of unique values, such as the addresses of different bad areas for respective memory devices used, so that perfect copy is physically impossible unless the bad areas of the memory used for copy and bad areas of the original memory are entirely identical to each other.

[108] As another example, the play apparatus marks bad areas (blocks, pages, sub-pages or locations) of memory used, at defined locations of spare areas corresponding thereto, as bad areas, and extracts encryption feature values (for example, encryption feature values based on the bad block DRM table [DRM encryption table]) by combining the addresses of the bad areas. Thereafter, the play apparatus encrypts original contents data using the encryption feature values, and records the encrypted contents data in the normal areas of the memory and not in the bad areas of the memory.

[109] Thereafter, when the memory card is inserted into the play apparatus, the play apparatus reads the addresses of bad areas through the examination of the memory, calculates encryption feature values used for the encryption of contents data by combining the addresses of the bad areas (for example, encryption feature values based on the bad block DRM table [DRM encryption table]), and recovers original contents data using the encryption feature values while sequentially reading data from the memory excepting the bad areas. At this time, since the encryption feature values are calculated by combining unique values, such as the addresses of different bad areas for respective memory devices, perfect copy is physically impossible unless the bad areas of memory used for copy and the bad areas of original memory are entirely identical to each other.

[110] As a further example, the play apparatus marks the bad areas (blocks, pages, sub-pages, and locations) of memory used, at defined locations of spare areas corresponding thereto, as bad areas, and extracts encryption feature values (for example, encryption feature values based on the bad block DRM table [DRM encryption table]) using specific values (for example, a serial number, etc.) recorded in the memory. Thereafter, the play apparatus encrypts original contents data using the encryption feature values, and records the encrypted contents data in normal areas of the memory and not in the bad areas of the memory.

[111] Thereafter, when such a memory card is inserted into the play apparatus, the play apparatus reads the specific values recorded in the memory by examining the memory, calculates encryption feature values (for example, encryption feature values based on the bad block DRM table [DRM encryption table]) used as specific values, and

recovers original contents data using the encryption feature values while sequentially reading data from the memory excepting the bad areas. At this time, the encryption feature values are calculated through a combination of specific values recorded in the memory used, so that perfect copy is physically impossible unless the bad areas of memory used for copy and the bad areas of original memory are completely identical to each other.

[112] In the above description, in order to prevent copy from being performed in such a way that the bad areas of a memory card, intellectual property rights of which are guaranteed, are read, the normal areas of the memory card desired to be copied are equally marked as bad areas, and identical encryption feature values are generated so as to copy the memory card, the play apparatus determines whether bad areas of the flash memory are physically formed or are merely marked for copy through a procedure of recording/reading data in/from the bad areas when the memory card is inserted. If it is determined that the bad areas are merely marked, the play apparatus classifies the memory card as an 'illegally copied memory card', and does not play recorded digital contents data. As described above, the present invention determines the authenticity of bad areas, thus identifying an illegally copied memory card.

[113] FIG. 10 is a diagram showing an example of the construction of a bad pattern DRM table configuration apparatus for digital rights management according to an embodiment of the present invention. For convenience of description, a description will be made on the basis of the operation of the apparatus for generating a bad block DRM table (DRM encryption table).

[114] A bad pattern detection unit 101 sets areas based on multiples of the number of blocks (/bad pages) (for example, based on multiples of 2048 blocks) in all the blocks of the flash memory, and detects bad blocks (/bad pages) in each of the areas.

[115] A real bad pattern examination unit 102 determines a bad pattern extraction area meeting a specific criterion (for example, an area having more than a threshold number of bad blocks [/bad pages], or an area having a maximum number of bad blocks [/bad pages]), and records the code value (area code) of the relevant area in the DRM table select code field of the card ID. At this time, the area code value, recorded in the DRM table select code field of the card ID, is the area code of the bad pattern extraction area meeting the specific condition among the areas obtained by dividing all the blocks of the flash memory by 2048 blocks. The specific condition is, for example, a criterion required to determine whether a specific area is an area suitable for the configuration of a bad block (/bad page) DRM table (DRM encryption table). According to such a specific condition, an area having more than a threshold number of (for example, 128) bad blocks (/bad pages), or an area having a maximum number of bad blocks (/bad pages), can be determined to be the bad pattern extraction area.

[116] A bad pattern table configuration unit 103 records the addresses of bad blocks (/bad pages) of the area corresponding to the area code, recorded in the DRM table select code field of the card ID, in the bad block (/bad page) table.

[117] A bad pattern DRM table calculation unit 104 examines the area corresponding to the area code recorded in the DRM table select code field of the card ID. That is, whether the area corresponding to the area code has bad blocks (/bad pages) sufficient to configure a bad block (/bad page) DRM table (DRM encryption table) is examined.

[118] A bad pattern DRM table generation unit 105 configures a bad block (/bad page) DRM table (DRM encryption table) on the basis of the bad pattern table (bad block table/bad page table) of the area corresponding to the area code recorded in the DRM table select code field of the card ID.

[119] For example, when the area corresponding to the area code has more than 128 bad blocks sufficient to configure a 256-byte bad block DRM table (DRM encryption table), a 256-byte bad block DRM table (DRM encryption table) [refer to 5] composed of 128 real bad block addresses is configured on the basis of the bad block table of the area (for example, area 1 having block 0 ~ block 2047) having more than 128 (256 byte) bad blocks.

[120] Further, when the area corresponding to the area code does not include bad blocks sufficient to configure a 256-byte bad block DRM table (DRM encryption table), a 256-byte bad block DRM table (DRM encryption table) [refer to FIG. 7] is generated by performing a padding operation. For example, the bad block DRM table (DRM encryption table) of FIG. 7 is configured using 18 (36 byte) real bad block addresses and 110 (220 byte) pieces of padding data. At this time, as an example of a padding method, a 256-byte bad block DRM table (DRM encryption table) can be configured, as shown in FIG. 7, using padding values, generated by sequentially performing an XOR operation on real bad block table values and a card serial number value.

[121] FIG. 11 is a diagram showing an example of the construction of a digital contents recording apparatus according to an embodiment of the present invention.

[122] A bad pattern examination and marking unit 111 formats the flash memory (for example, NAND flash memory) of a storage medium (memory card implemented as a memory device) to a low level, examines bit-based bad pages (pages having bad bits) or bit-based bad blocks (blocks having bad bits) by writing 0xAA55, and marks pages or blocks having bad bits as bad pages or bad blocks.

[123] A bad pattern area selection unit 112 formats the flash memory to a low level, and determines an area meeting a specific condition (criterion) with reference to a recorded bad block (/bad page) table. A media information recording unit 113 records the area code of the area in the DRM table select code field of the card ID (page number 9 of zero block).

[124] For example, all the blocks of the flash memory are divided by 2048 blocks, and thus respective areas are set. Among the areas, an area meeting a specific condition (criterion) is determined to be a bad pattern extraction area required for the configuration of a bad block (/bad page) DRM table (DRM encryption table). Thereafter, the area code of the determined area is recorded in the DRM table select code field of the card ID. The term 'specific condition (criterion)' means a criterion required to determine whether a specific area is an area suitable for the configuration of a bad block (/bad page) DRM table (DRM encryption table). For example, an area having more than a threshold number of (for example, 128) bad blocks (/bad pages), or an area having a maximum number of bad blocks (/bad pages) can be determined to be a bad pattern extraction area. The determination of the bad pattern extraction area may be performed by determining whether an area having more than a threshold number of (for example, 128) bad blocks (/bad pages) is present, and by determining an area, having a maximum number of bad blocks (/bad pages) among the plurality of areas (areas set based on multiples of 2048 blocks), to be the bad pattern extraction area if it is determined that the relevant area is not present. In this way, the area code value of the area determined to be the bad pattern extraction area is recorded in the DRM table select code field of the card ID of FIG. 2.

[125] A bad pattern DRM table generation unit 114 configures a bad block (/bad page) DRM table (DRM encryption table) on the basis of the bad pattern table (bad block table/bad page table) of the area corresponding to the area code recorded in the DRM table select code field of the card ID. For example, when the area corresponding to the area code has more than 128 sufficient bad blocks, a 256-byte bad block DRM table (DRM encryption table) [refer to FIG. 5] composed of 128 real bad block addresses is configured on the basis of the bad block table of the area (for example, area 1 having block 0 ~ block 2047) having more than 128 (256 bytes) bad blocks. When the area corresponding to the area code does not include bad blocks sufficient to configure a 256-byte bad block DRM table (DRM encryption table), a 256-byte bad block DRM table (DRM encryption table) [refer to FIG. 7] is configured by performing a padding operation.

[126] A contents encryption recording unit 115 records digital contents on the digital contents storage medium implemented as the memory device (for example, NAND flash memory) by utilizing the bad pattern DRM table (DRM encryption table), generated by the bad pattern DRM table generation unit 114, as an encryption key.

[127] FIG. 12 is a diagram showing an example of the construction of a digital contents play apparatus (media play apparatus) apparatus according to an embodiment of the present invention.

[128] When a digital contents storage device implemented as a memory device (for

example, NAND flash memory) is inserted into a digital contents provision apparatus (media play apparatus), the media information collection unit 121 reads information about a card ID (page number 9 of zero block). In this case, in the DRM table select code field of the card ID, the area code information of the area having bad patterns (bad blocks, bad pages, bad bits, etc.) (area having more than a threshold number of bad blocks [/bad pages], or an area having a maximum number of bad blocks [/bad pages]), desired to be used for a bad pattern DRM table (DRM decryption table) is recorded, and thus the information of the card ID is collected at the time of playing media.

[129] A bad pattern DRM table generation unit 122 configures a bad block (/bad page) DRM table (DRM decryption table) on the basis of the bad pattern table (bad block table/bad page table) of the area corresponding to the DRM table select code field of the card ID. For example, when the area corresponding to the area code recorded in the DRM table select code field has more than 128 sufficient bad blocks, the bad pattern DRM table generation unit 122 configures a 256-byte bad block DRM table (DRM decryption table) [refer to FIG. 5] composed of 128 real bad block addresses on the basis of the bad block table of the area having more than 128 (256 byte) bad blocks. When the area corresponding to the area code recorded in the DRM table select code field does not include bad blocks sufficient to configure a 256-byte bad block DRM table (DRM decryption table), the bad pattern DRM table generation unit 122 configures a 256-byte bad block DRM table (DRM decryption table) by performing a padding operation [refer to FIG. 7]. That is, the 256-byte bad block DRM table (DRM decryption table) of FIG. 7 is configured using padding values generated by sequentially performing an XOR operation on the real bad block table values and the card serial number value.

[130] A media authentication unit 123 determines whether blocks (/pages) corresponding to the real bad block (/bad page) table values, rather than padding values, in the bad block(/bad page) DRM table (DRM decryption table) generated by the bad pattern DRM table generation unit 122, are real bad blocks (/bad pages). For example, the media authentication unit 123 determines whether blocks having real bad block addresses in the bad block DRM table (DRM decryption table) of FIG. 7, composed of 36 bytes of real bad block addresses and 220 bytes of padding data (*0x09, 0x10, 0x0B, 0x17, ...*), are real bad blocks.

[131] In this case, in order to determine whether blocks are real bad blocks (/bad pages), about 10 bad blocks (/bad pages) are randomly selected from the real bad block (/bad page) table, and whether the selected bad blocks are real bad blocks (/bad pages) is examined. At this time, a Write Protect (WP) pin is disabled, and 0xAA55 and 0x55AA are written in the corresponding page of each real bad block (/bad page), so

that whether the blocks are real bad blocks (/bad pages) is determined. If it is determined that the blocks are real bad blocks (/bad pages), a suitable number of real bad blocks (/bad pages) are additionally examined using the same method. Even on the additionally selected bad blocks (/bad pages), a Write Protect (WP) pin is disabled, and 0xAA55 and 0x55AA are written in the corresponding page of each real bad block (/bad page), so that whether the additionally selected blocks are real bad blocks (/bad pages) is determined.

[132] A contents decryption and play unit 124 permits the use of the digital contents medium (play or read) on the basis of the results of the authentication performed by the media authentication unit 123. That is, when the authentication of the use of the medium has succeeded, the contents decryption and play unit 124 transmits digital contents data to a user while decrypting the digital contents data using the generated bad block (/bad page) DRM table (DRM decryption table). Further, when the authentication of the use of the medium has failed, the contents decryption and play unit 124 notifies the user of the failure of the authentication, thus requesting the user to check the digital contents storage medium.

[133] FIG. 13 is a diagram showing an example of the construction of a key generation apparatus for an asymmetric encryption system to which the present invention is applied.

[134] A bad pattern detection unit 131 sets areas based on multiples of the number of blocks (/pages) (for example, based on multiples of 2048 blocks) in all the blocks (/bad pages) of the flash memory, and detects bad blocks (/bad pages) from each of the areas.

[135] A bad pattern DRM table generation unit 132 configures a bad block (/bad page) DRM table (DRM encryption table) on the basis of the bad pattern table (bad block table/bad page table) of the area corresponding to the DRM table select code of the card ID. For example, when the area corresponding to the area code recorded in the DRM table select code field has more than 128 sufficient bad blocks, a 256-byte bad block DRM table (DRM encryption table) [refer to FIG. 5] composed of 128 real bad block addresses is configured on the basis of the bad block table of the area having more than 128 (256 byte) bad blocks. When the area corresponding to the area code recorded in the DRM table select code field does not include bad blocks sufficient to configure a 256-byte bad block DRM table (DRM encryption table), a 256-byte bad block DRM table (DRM encryption table) [refer to FIG. 7] is configured by performing a padding operation. That is, the 256-byte bad block DRM table (DRM encryption table) of FIG. 7 is configured using padding values generated by sequentially performing an XOR operation on real bad block table values and a card serial number value.

[136] A media authentication unit 133 determines whether blocks (/pages) corresponding to the real bad block (/bad page) table values, rather than padding values, in the bad block (/bad page) DRM table (DRM encryption table) generated by the bad pattern DRM table generation unit 132, are real bad blocks (/bad pages). For example, the media authentication unit 133 determines whether blocks having real bad block addresses are real bad blocks in the bad block DRM table (DRM encryption table) of FIG. 7 composed of 36 bytes of real bad block addresses and 220 bytes of padding data (*0x09, 0x10, 0x0B, 0x17*, ...).

[137] Here, in order to determine whether the blocks are real bad blocks (/bad pages), for example, about 10 bad blocks (/bad pages) are randomly selected from the real bad block (/bad page) table, and whether the selected bad blocks are real bad blocks (/bad pages) is examined. At this time, a Write Protect (WP) pin is disabled, and 0xAA55 and 0x55AA are written in the corresponding page of each real bad block (/bad page), so that whether the blocks are real bad blocks (/bad pages) is determined. At this time, if it is determined that the blocks are real bad blocks (/bad pages), a suitable number (for example, about 10) of real bad blocks (/bad pages) are additionally examined using the same method. Even on the additionally selected bad blocks (/bad pages), a Write Protect (WP) pin is disabled, and 0xAA55 and 0x55AA are written in the corresponding page of each real bad block (/bad page), so that whether the additionally selected blocks are real bad blocks (/bad pages) is determined.

[138] A seed key generation unit 134 generates a seed key through a Hash function which uses a bad pattern DRM table (DRM encryption table) as a transform factor.

[139] An asymmetric encryption key generation unit 135 generates a public key and a private key through a PKI algorithm (RSA, ECC, etc.) using the seed key generated by the seed key generation unit 134.

[140] The public key may be used to encrypt digital contents data, and the private key may be used to decrypt digital contents data.

[141] Meanwhile, the above-described methods of the present invention may be implemented in the form of computer programs. Further, codes and code segments constituting each program may be easily derived by computer programmers skilled in the art. Further, the implemented program is stored in computer-readable recording media (information storage media such as Application-Specific Integrated Circuit [ASIC], CD-Read Only Memory [ROM], Random Access Memory [RAM], ROM, a floppy disc, a hard disc, a magneto-optical disc, and an One-Time Programmable [OTP] memory device), and is read and executed by a computer, and thus the methods of the present invention are implemented. Further, the recording media may include all types of computer-readable recording media.

[142] In the present invention, various modifications, additions and substitutions can be

executed by those skilled in the art, without departing from the scope and spirit of the invention. Accordingly, the present invention is not limited to the above-described embodiments and attached drawings.

Industrial Applicability

[143] The present invention can be used for DRM technologies, digital contents recording/playing technology using bad patterns, digital storage media for the technologies, etc.

Claims

[1] A Digital Rights Management (DRM) method, comprising the steps of:
examining unit area-based bad patterns of a memory device constituting a digital contents storage medium, and determining a bad pattern extraction area;
recording an area code value of the determined bad pattern extraction area in a table select code field of a card ID; and
examining an area corresponding to the area code value recorded in the table select code field, and configuring a bad pattern DRM table based on a bad pattern table.

[2] The DRM method according to claim 1, wherein the bad pattern table is generated at a time of formatting the memory device of the digital contents storage medium in which address values of the unit area-based bad patterns which are possible physical characteristics of the memory device are recorded.

[3] The DRM method according to claim 2, wherein the bad pattern DRM table is configured with only the bad pattern table.

[4] The DRM method according to claim 2, wherein the bad pattern DRM table is configured with a card serial number field of the card ID, and is configured by padding values generated by sequentially performing an XOR operation on values of the bad pattern table and a value of a card serial number.

[5] The DRM method according to any one of claims 1 to 4, wherein the bad patterns are one of bad blocks, bad pages, and bad bits.

[6] The DRM method according to claim 5, wherein the bad pattern extraction area is one of an area including all blocks of the memory device, an area including more than a threshold number of bad patterns, and an area including a maximum number of bad patterns.

[7] The DRM method according to claim 6, wherein the unit areas are areas set based on multiples of 2048 blocks.

[8] The DRM method according to claim 6, wherein the threshold number is 128, which is the number of bad blocks.

[9] The DRM method according to claim 8, wherein the bad pattern DRM table has a size of 256 bytes.

[10] The DRM method according to any one of claims 1 to 4, wherein the memory device is NAND flash memory.

[11] A Digital Rights Management (DRM) method, comprising the steps of:
extracting physical characteristics of a digital contents storage medium; and
generating an encryption key with the extracted physical characteristics of the digital contents storage medium.

[12] A Digital Rights Management (DRM) method, comprising the steps of:
examining unit area-based bad patterns of a memory device constituting a digital contents storage medium, and determining a bad pattern extraction area;
recording an area code value of the determined bad pattern extraction area in a table select code field of a card ID;
examining an area corresponding to the area code value recorded in the table select code field, and configuring a bad pattern DRM table based on information about the bad patterns; and
generating a bad pattern encryption key based on the bad pattern information.

[13] A method of recording digital contents, comprising the steps of:
examining unit area-based bad patterns of a memory device constituting a digital contents storage medium and determining a bad pattern extraction area;
recording an area code value of the determined bad pattern extraction area in a table select code field of a card ID;
examining an area corresponding to the area code value recorded in the table select code field, and configuring a bad pattern DRM table based on a bad pattern table; and
recording digital contents in the storage medium by utilizing the bad pattern DRM table as an encryption key.

[14] The method according to claim 13, wherein the bad pattern table is generated at a time of formatting the memory device of the digital contents storage medium in which address values of the unit area-based bad patterns which are possible physical characteristics of the memory device are recorded.

[15] The method according to claim 14, wherein the bad pattern DRM table is configured with only the bad pattern table.

[16] The method according to claim 14, wherein the bad pattern DRM table is configured using a card serial number field of the card ID, and is configured by padding values generated by sequentially performing an XOR operation on values of the bad pattern table and a value of a card serial number.

[17] The method according to any one of claims 13 to 16, wherein the bad patterns are one of bad blocks, bad pages, and bad bits.

[18] The method according to claim 17, wherein the bad pattern extraction area is one of an area including all blocks of the memory device, an area including more than a threshold number of bad patterns, and an area including a maximum number of bad patterns.

[19] A method of recording digital contents, comprising the steps of:
extracting physical characteristics of a digital contents storage medium;
generating an encryption key with the extracted physical characteristics of the

digital contents storage medium; and
recording digital contents on the digital contents storage medium using the generated encryption key.

[20] A method of recording digital contents, comprising the steps of:
setting an area, in which addresses of bad areas of memory used are recorded, in a header data area which is an area for storing characteristics of a memory card (digital contents storage medium), rather than in a data storage space, and recording the addresses in the set area; and
extracting encryption feature values by combining the addresses of the bad areas, encrypting original contents data using the encryption feature values, and recording the encrypted contents data in a normal area of the memory and not in the bad areas.

[21] A method of recording digital contents, comprising the steps of:
marking bad areas of memory used, at defined locations of corresponding spare areas, as bad areas, and extracting encryption feature values by combining addresses of the bad areas; and
encrypting original contents data using the encryption feature values, and recording the encrypted contents data in a normal area of the memory and not in the bad areas.

[22] A method of recording digital contents, comprising the steps of:
marking bad areas of memory used, at defined locations of corresponding spare areas, as bad areas, and extracting encryption feature values using specific values recorded in the memory; and
encrypting original contents data using the encryption feature values, and recording the encrypted contents data in a normal area of the memory and not in the bad areas.

[23] The method according to claim 22, wherein the specific values are serial numbers.

[24] A digital contents storage medium, wherein:
an area code value of a bad pattern extraction area is recorded in a table select code field of a card ID, and digital contents is recorded by utilizing a Digital Rights Management (DRM) encryption table, which is configured based on a bad pattern table by examining an area corresponding to the area code value recorded in the table select code field, as an encryption key.

[25] A method of playing digital contents, comprising the steps of:
when a digital contents storage medium is inserted, examining an area corresponding to an area code recorded in a table select code field of a card ID, and configuring a bad pattern Digital Rights Management (DRM) table based on a

bad pattern table;

examining whether patterns having real bad pattern address values in the bad pattern DRM table are real bad patterns; and

playing digital contents by utilizing the bad pattern DRM table as a decryption key on a basis of results of the examination.

[26] The method according to claim 25, wherein the bad pattern table is generated at a time of formatting a memory device of the digital contents storage medium, and is configured such that address values of unit area-based bad patterns which are possible physical characteristics of the memory device are recorded in the bad pattern table.

[27] The method according to claim 26, wherein the bad pattern DRM table is configured with only the bad pattern table.

[28] The method according to claim 26 wherein the bad pattern DRM table is configured using a card serial number field of the card ID, and is configured by padding values that are generated by sequentially performing an XOR operation on values of the bad pattern table and a value of a card serial number.

[29] The method according to any one of claims 25 to 28, wherein the bad patterns are one of bad blocks, bad pages, and bad bits.

[30] The method according to claim 29, wherein the step of examining whether patterns having real bad pattern address values in the bad pattern DRM table are real bad patterns is performed to examine whether the patterns are real bad patterns by disabling a Write Protect (WP) pin and writing 0xAA55 and 0x55AA in corresponding pages of the real bad patterns.

[31] A method of playing digital contents, comprising the steps of:

extracting physical characteristics of a digital contents storage medium;

generating a decryption key using the extracted physical characteristics of the digital contents storage medium; and

playing digital contents using the generated decryption key.

[32] A method of playing digital contents, comprising the steps of:

when a digital contents storage medium is inserted, reading addresses of bad areas from a header data area, and calculating encryption feature values used for encryption of contents data by combining the addresses of the bad areas; and

recovering original digital contents data using the encryption feature values while sequentially reading the contents data from the memory excepting the bad areas,

wherein the encryption feature values are calculated by combining unique values, such as addresses of different bad areas for respective memory devices used, and thus it is physically impossible to perform perfect copy unless bad areas of

memory used for copy are entirely identical to those of original memory.

[33] A method of playing digital contents, comprising the steps of:
when a digital contents storage medium is inserted, examining memory, reading addresses of bad areas from the memory, and calculating encryption feature values used for encryption of contents data by combining the addresses of the bad areas; and
recovering original contents data using the encryption feature values while sequentially reading data from the memory excepting the bad areas,
wherein the encryption feature values are calculated by combining unique values, such as addresses of different bad areas for respective memory devices used, and thus it is physically impossible to perform perfect copy unless bad areas of memory used for copy are entirely identical to those of original memory.

[34] A method of playing digital contents, comprising the steps of:
when a digital contents storage medium is inserted, examining memory, reading specific values recorded in the memory from the memory, and calculating encryption feature values used as the specific values; and
recovering original contents data using the encryption feature values while sequentially reading data from the memory excepting the bad areas,
wherein the encryption feature values are calculated by combining unique values, such as addresses of different bad areas for respective memory devices used, and thus it is physically impossible to perform perfect copy unless bad areas of memory used for copy are entirely identical to those of original memory.

[35] The method according to any one of claims 32 to 34, wherein, when the digital contents storage medium is inserted, whether the bad areas are physically formed or simply marked for copy is determined through a process for writing/reading data in/from the bad areas.

[36] A computer-readable recording medium for storing, in a Digital Rights Management (DRM) apparatus having a processor, a program for implementing:
a function of examining unit area-based bad patterns of a memory device constituting a digital contents storage medium, and determining a bad pattern extraction area;
a function of recording an area code value of the determined bad pattern extraction area in a table select code field of a card ID; and
a function of examining an area corresponding to the area code value recorded in the table select code field and configuring a bad pattern DRM table based on a bad pattern table.

[37] A computer-readable recording medium for storing, in a Digital Rights Management (DRM) apparatus having a processor, a program for implementing:

a function of extracting physical characteristics of a digital contents storage medium; and

a function of generating an encryption key using the extracted physical characteristics of the digital contents storage medium.

[38] A computer-readable recording medium for storing, in a digital contents recording apparatus having a processor, a program for implementing:

a function of examining unit area-based bad patterns of a memory device constituting a digital contents storage medium and determining a bad pattern extraction area;

a function of recording an area code value of the determined bad pattern extraction area in a table select code field of a card ID;

a function of examining an area corresponding to the area code value recorded in the table select code field, and configuring a bad pattern Digital Rights Management (DRM) table based on a bad pattern table; and

a function of recording digital contents on the storage medium by utilizing the bad pattern DRM table as an encryption key.

[39] A computer-readable recording medium for storing, in a digital contents recording apparatus having a processor, a program for implementing:

a function of extracting physical characteristics of a digital contents storage medium;

a function of generating an encryption key using the extracted physical characteristics of the digital contents storage medium; and

a function of recording digital contents on the digital contents storage medium using the generated encryption key.

[40] A computer-readable recording medium for storing, in a digital contents play apparatus having a processor, a program for implementing:

a function of, when a digital contents storage medium is inserted, examining an area corresponding to an area code value recorded in a table select code field of a card ID, and configuring a bad pattern Digital Rights Management (DRM) table based on a bad pattern table;

a function of examining whether patterns having real bad pattern address values in the bad pattern DRM table are real bad patterns; and

a function of playing digital contents by utilizing the bad pattern DRM table as a decryption key on a basis of results of the examination.

[41] A computer-readable recording medium for storing, in a digital contents play apparatus having a processor, a program for implementing:

a function of extracting physical characteristics of a digital contents storage medium;

a function of generating a decryption key using the extracted physical characteristics of the digital contents storage medium; and

a function of playing digital contents using the generated decryption key.

[Fig. 1]

Page Number	Page Name
0	MBR(Master Boot Recorder)
1	Bad Block Marking
2	Bad Block Marking
3	Bad Block Marking
4	Bad Block Marking
5	Bad Block Marking
6	reserved
7	reserved
8	reserved
9	Card ID
10	reserved
...	...
...	...
...	...
31	reserved

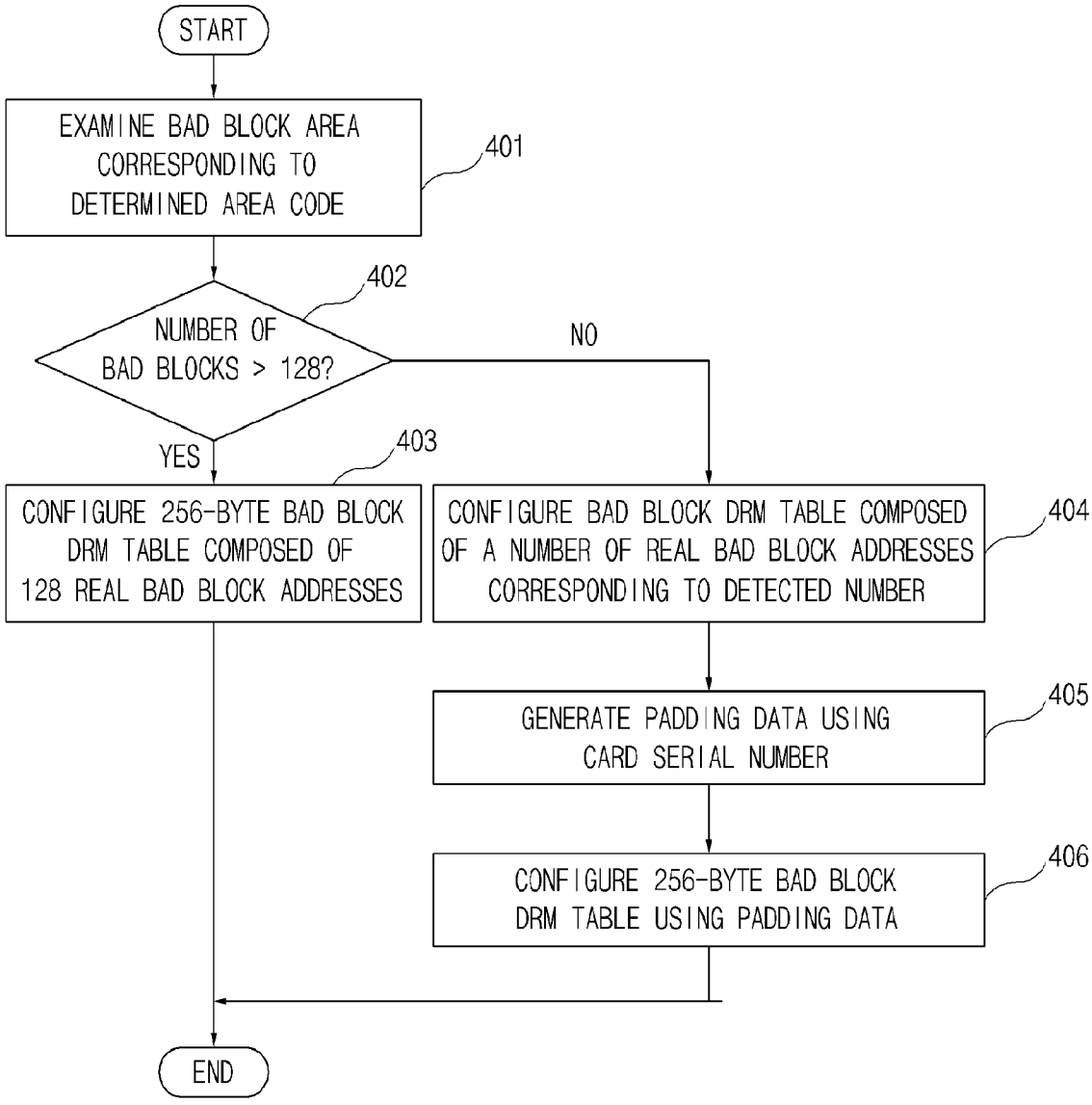
[Fig. 2]

Offset	Length	Contents	Example
0	2	Card Version	0x0001
2	2	DRM Table Select Code	0x0003
4	2	Area Code	0x0000
6	2	Manufacturing Company Code	0x0001
8	2	Writer ID	0x0001
10	2	Current Used Card Serial Number Class	0x0001
12	16	Card Serial Number Class1	0x000000~01
28	16	Card Serial Number Class2	-
44	16	Card Serial Number Class3	-
		reserved	
~511			-

[Fig. 3]

0	1	2	3	4	...	...	...	...	
									1 Area
								2047	
2048	2049	2050	...	...	...	...	...	...	
									2 Area
								4095	
4096	4097	4098	...	...	...	...	...	...	
									3 Area
								6143	
6144	6145	6146	...	...	...	...	...	...	
									4 Area
								8191	

[Fig. 4]



[Fig. 5]

	0	1	2	3	4	5	6	7	···	···	···	15
0	0x00	0x12	0x00	0x13	0x01	0x02	0x01	0x3E	···	···	···	0x30
1	0x02	0x23	0x02	0x2D	0x02	0x2E	0x02	0x2F	···	···	···	0x23
2	0x02	0xFE	0x02	0xFF	0x03	0x01	0x03	0x05	···	···	···	0x27
···	···	···	···	···	···	···	···	···	···	···	···	0x01
15	0x05	0x04	0x05	0x45	0x06	0x5E	0x06	0x5F	···	···	···	0x08

[Fig. 6]

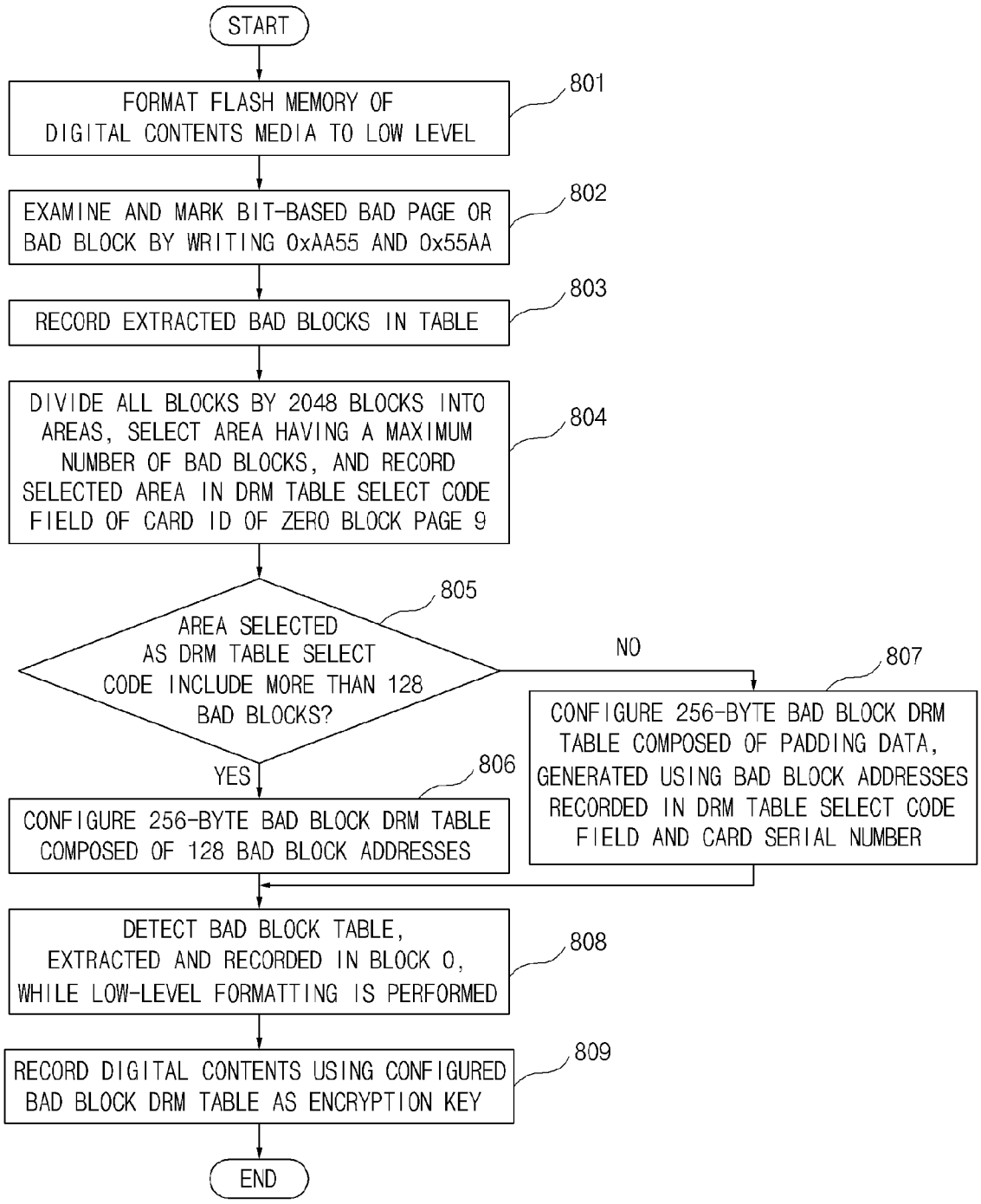
	0	1	2	3	4	5	6	7	···	···	···	15
0	0x08	0x12	0x08	0x13	0x09	0x02	0x09	0x3E	···	···	···	0x30
1	0x0A	0x23	0x0A	0x2D	0x0A	0x2E	0x0A	0x2F	···	···	···	0x23
2	0x0C	0x0E	0x0C	0xFE	d	d	d	d	···	···	···	d
···	···	···	···	···	···	···	···	···	···	···	···	d
15	d	d	d	d	d	d	d	d	···	···	···	d

d : don't care

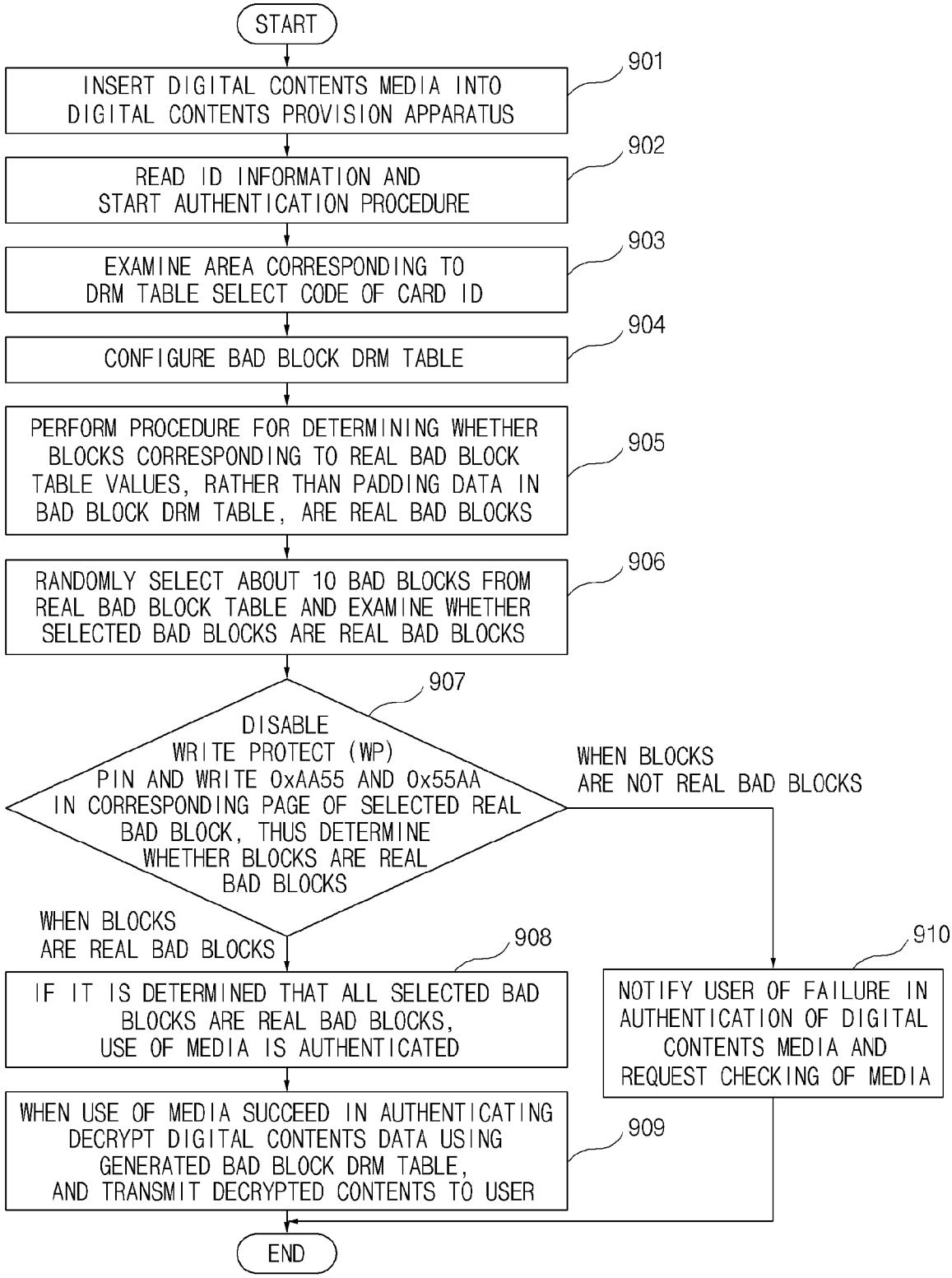
[Fig. 7]

	0	1	2	3	4	5	6	7	···	···	···	15
0	0x08	0x12	0x08	0x13	0x09	0x02	0x09	0x3E	···	···	···	0x30
1	0x0A	0x23	0x0A	0x2D	0x0A	0x2E	0x0A	0x2F	···	···	···	0x23
2	0x0C	0x0E	0x0C	0xFE	*0x09*	*0x10*	*0x0B*	*0x17*	···	···	···	···
···	···	···	···	···	···	···	···	···	···	···	···	···
15	···	···	···	···	···	···	···	···	···	···	···	···

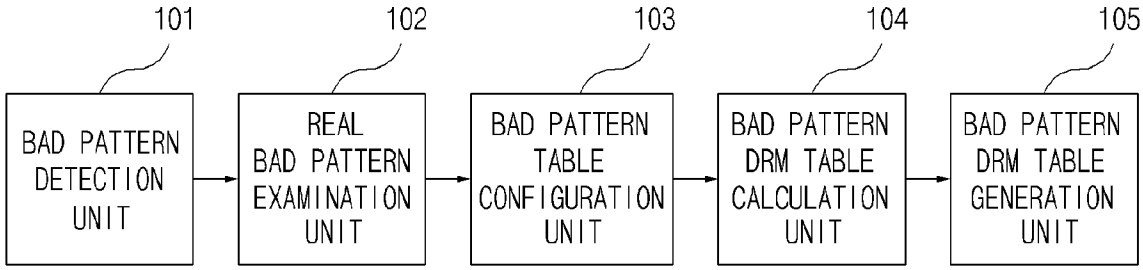
[Fig. 8]


START
FORMAT FLASH MEMORY OF DIGITAL CONTENTS MEDIA TO LOW LEVEL
801
EXAMINE AND MARK BIT-BASED BAD PAGE OR BAD BLOCK BY WRITING 0xAA55 AND 0x55AA
802
RECORD EXTRACTED BAD BLOCKS IN TABLE
803
DIVIDE ALL BLOCKS BY 2048 BLOCKS INTO AREAS, SELECT AREA HAVING A MAXIMUM NUMBER OF BAD BLOCKS, AND RECORD SELECTED AREA IN DRM TABLE SELECT CODE FIELD OF CARD ID OF ZERO BLOCK PAGE 9
804
AREA SELECTED AS DRM TABLE SELECT CODE INCLUDE MORE THAN 128 BAD BLOCKS?
805
NO
807
CONFIGURE 256-BYTE BAD BLOCK DRM TABLE COMPOSED OF PADDING DATA, GENERATED USING BAD BLOCK ADDRESSES RECORDED IN DRM TABLE SELECT CODE FIELD AND CARD SERIAL NUMBER
YES
806
CONFIGURE 256-BYTE BAD BLOCK DRM TABLE COMPOSED OF 128 BAD BLOCK ADDRESSES
DETECT BAD BLOCK TABLE, EXTRACTED AND RECORDED IN BLOCK 0, WHILE LOW-LEVEL FORMATTING IS PERFORMED
808
RECORD DIGITAL CONTENTS USING CONFIGURED BAD BLOCK DRM TABLE AS ENCRYPTION KEY
809
END

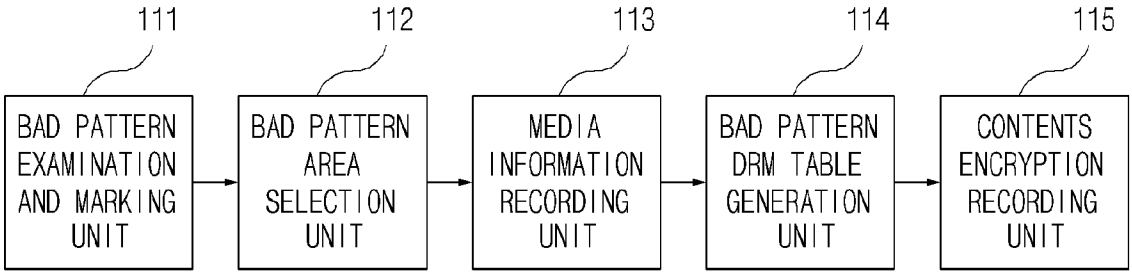
[Fig. 9]


START
INSERT DIGITAL CONTENTS MEDIA INTO DIGITAL CONTENTS PROVISION APPARATUS
901
READ ID INFORMATION AND START AUTHENTICATION PROCEDURE
902
EXAMINE AREA CORRESPONDING TO DRM TABLE SELECT CODE OF CARD ID
903
CONFIGURE BAD BLOCK DRM TABLE
904
PERFORM PROCEDURE FOR DETERMINING WHETHER BLOCKS CORRESPONDING TO REAL BAD BLOCK TABLE VALUES, RATHER THAN PADDING DATA IN BAD BLOCK DRM TABLE, ARE REAL BAD BLOCKS
905
RANDOMLY SELECT ABOUT 10 BAD BLOCKS FROM REAL BAD BLOCK TABLE AND EXAMINE WHETHER SELECTED BAD BLOCKS ARE REAL BAD BLOCKS
906
907
DISABLE WRITE PROTECT (WP) PIN AND WRITE 0xAA55 AND 0x55AA IN CORRESPONDING PAGE OF SELECTED REAL BAD BLOCK, THUS DETERMINE WHETHER BLOCKS ARE REAL BAD BLOCKS
WHEN BLOCKS ARE NOT REAL BAD BLOCKS
WHEN BLOCKS ARE REAL BAD BLOCKS
908
IF IT IS DETERMINED THAT ALL SELECTED BAD BLOCKS ARE REAL BAD BLOCKS, USE OF MEDIA IS AUTHENTICATED
910
NOTIFY USER OF FAILURE IN AUTHENTICATION OF DIGITAL CONTENTS MEDIA AND REQUEST CHECKING OF MEDIA
WHEN USE OF MEDIA SUCCEED IN AUTHENTICATING DECRYPT DIGITAL CONTENTS DATA USING GENERATED BAD BLOCK DRM TABLE, AND TRANSMIT DECRYPTED CONTENTS TO USER
909
END

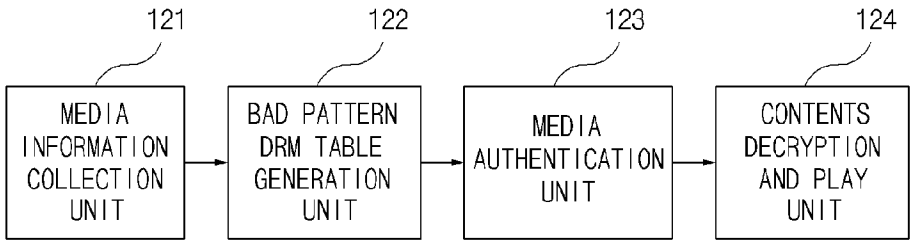
[Fig. 10]



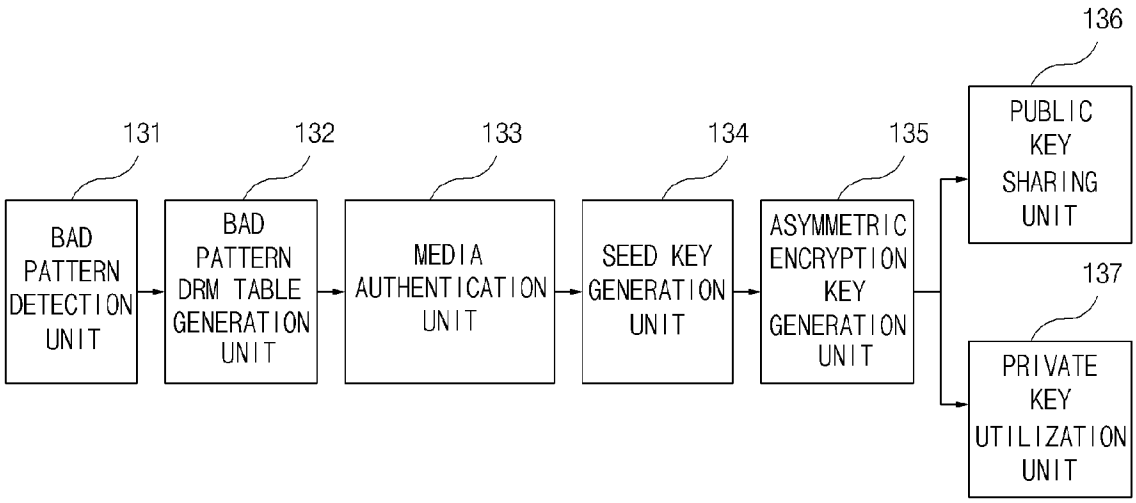
[Fig. 11]



[Fig. 12]



[Fig. 13]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2008/000193

A. CLASSIFICATION OF SUBJECT MATTER

G06F 15/00(2006.01)i

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 8 : G06F

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

Korean utility models and applications for utility model since 1975

Japanese utility models and applications for utility model since 1975

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

eKIPASS(KIPO internal), Google, IEEE xpl, "bad", "pattern", "encryption"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1051011 A2 (SAMSUNG ELECTRONICS CO., LTD) 2000.11.08 See abstract, Figure 7, paragraphs [0129]-[0132], claims	11, 19-21, 31-33, 37, 39, 41
---		---
Y		35
Y	EP 0745925 A2 (T.T.R. TECHNOLOGIES LIMITED) 1996.12.04 See abstract, row 13 column 5 - row 42 column 7, claims	35
A	WO 2000-55736 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V.) 2000.09.21 See abstract, claims	1-41

☐ 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 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 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	Date of mailing of the international search report
23 SEPTEMBER 2008 (23.09.2008)	**23 SEPTEMBER 2008 (23.09.2008)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer LEE, Jong Ick Telephone No. 82-42-481-8373

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2008/000193

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1051011 A2	08.11.2000	CN 1205779 C	01.06.2005
		CN 1272734 A	08.11.2000
		DE 69924236 T2	02.02.2006
		JP 2000-324098 A2	24.11.2000
		JP 2007-124717 A2	17.05.2007
		KR 10-2000-0072849 A	05.12.2000
EP 0745925 A2	04.12.1996	IL 113890 A0	04.08.1996
		JP 9054691 A2	25.02.1997
WO 2000-55736 A1	21.09.2000	CA 2332008 AA	21.09.2000
		CA 2332034 AA	21.09.2000
		DE 60015269 C0	02.12.2004
		EP 1076857 A1	21.02.2001
		EP 1086467 A1	28.03.2001
		JP 2002-539557 T2	19.11.2002
		JP 2003-505752 T2	12.02.2003
		KR 10-2001-0043582 A	25.05.2001
		KR 10-2001-0071254 A	28.07.2001
		US 2007-162982 AA	12.07.2007
		US 7178036 BA	13.02.2007
		WO 2000-55861A1	21.09.2000