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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 June 2006 (29.06.2006)

PCT

(10) International Publication Number
WO 2006/067405 A1

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

(21) International Application Number:
PCT/GB2005/004910

(22) International Filing Date:
19 December 2005 (19.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/018,105 20 December 2004 (20.12.2004) US

(71) Applicant *(for all designated States except US)*: MACROVISION EUROPE LIMITED [GB/GB]; Malvern House, 14-18 Bell Street, Maidenhead, Berkshire SL6 1BR (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: DOYLE, William, Henry, Christopher [IE/GB]; Flat2, 18 Western Elms Avenue, Reading, Berkshire RG30 2AN (GB).

(74) Agent: NEEDLE, Jacqueline; Beck Greener, Fulwood House, 12 Fulwood Place, London WC1V 6HR (GB).

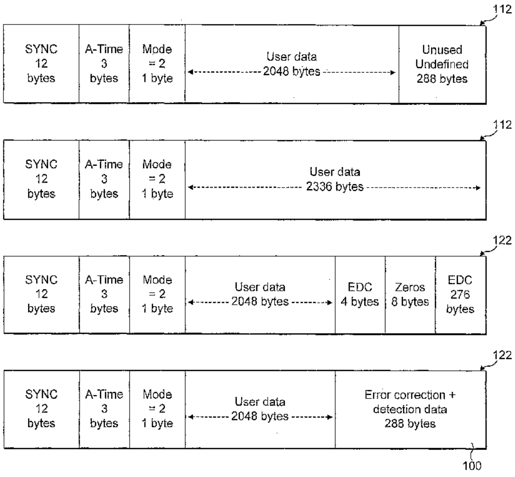
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: COPY PROTECTION FOR OPTICAL DISCS



(57) Abstract: Optical discs, such as CDs, have been protected by the use of an authenticating signature which cannot be copied to another disc. A playing device is required to identify the existence of the authenticating signature in order to access the content of the disc. The authenticating signature may comprise bad sectors at known locations. CD writers now available to consumers allow error detection and error correction data to be specified and this has led to circumvention techniques designed to simulate an original disc. During the writing of a copy disc, bad sectors are identified and provided with alternative data together with incorrect error detection and error correction data. When the copy disc is played bad sectors are reported in exactly the same locations as reported by the original disc thereby enabling the disc to be played even though it is a copy. To defeat techniques which use the error detection and error correction data to circumvent the copy protection, it is proposed to store authenticating signatures in sectors (112) in Mode 2 format. Sectors formatted in this way are not subject to error detection and correction.

WO 2006/067405 A1

COPY PROTECTION FOR OPTICAL DISCS

The present invention relates to a copy protected optical disc carrying an authentication signature, to a method of copy protecting optical discs, and to a content file for use in manufacturing a copy protected optical disc.

Optical discs, such as the various formats of compact discs (CDs), and of digital versatile discs (DVDs), are increasingly used for carrying information for many different applications. The information encoded onto the optical discs is generally very valuable, and accordingly, they are increasingly copied by counterfeiters. Furthermore, recordable CDs are available, and CD writers for writing the information content from one disc to such recordable discs are readily available to the domestic consumer. This means that new and effective methods for copy protecting the optical discs are required.

There is described, for example, in WO 98/57413, a method of providing an optical disc with an authenticating signature. This authenticating signature is arranged so that it is not, or cannot be, copied by available devices for reading and writing data from CDs. For example, in WO 98/57413, a sector of a CD is provided with a pattern of errors which cannot be corrected by the error correcting rules and thereby constitutes an uncorrectable sector or "bad sector" on the disc. The existence of the expected bad sector is taken as an authenticating signature and is used to identify a genuine disc.

WO 02/11136 also describes the use of an authenticating signature but, in this case, the inherent limitations of currently available CD writers are exploited. Thus, in WO 02/11136 it is proposed that during mastering an authenticating signature is written to the glass master. This authenticating signature is made up of data patterns which cannot be accurately written by a writer for recordable discs so that when attempts are made to copy an original disc made from the glass master, the consumer's CD writer will find it difficult or impossible to write the authenticating signature to the copy disc with good readability. However, the much more sophisticated encoders used in mastering houses, for example, can be controlled to accurately write such an authenticating signature to the glass master.

In WO 02/11136, the data patterns of the authenticating signature are preferably chosen to cause digital sum value (DSV) problems for CD writers.

The two signature methods described above, in common with other signature methods, require that a correct signature is readable from the disc before the disc can be successfully operated. In addition, the existence of corrupted or otherwise incorrect data in the sector where the signature should have been can be used to signify that the disc is not original whereby its use may be prevented.

Originally devices for writing CDs generated the bit sequence to be written to disc, including error correction and error detection codes, automatically in dependence upon built in software including formatting rules. However, new generations of consumer CD writers allow error detection and correction codes to be specified by the user when copying an original disc. A number of circumvention devices make use of this facility to circumvent signature protection techniques so that a copied disc looks, to copy protection software, to be an original disc.

Thus, during play of a disc with an authenticating signature as set out, for example, in WO 98/57413, the playing device is controlled, at the outset, to find a bad sector in an expected location before it is enabled to access the content of the disc. By using a CD writer which allows a choice of error correcting and error detecting codes, it is possible to put any data into the sector which carried the authenticating signature on the original disc and then to change the error correcting and error detecting codes such that, upon play of the resultant copy disc, a bad sector is reported. The identification of a bad sector in the same location is taken by the copy protection software to signify a genuine disc.

Manipulation of the error correction and error detection codes similarly allows a disc copied from an original protected with an authenticating signal as described in WO 02/11136 to simulate an original disc.

The present invention seeks to defeat circumvention techniques which involve altering error correcting and error detecting codes.

According to a first aspect of the present invention there is provided a copy protected optical disc carrying an authentication signature, the authentication signature being arranged so that it cannot be accurately copied by a writer of recordable discs, and wherein the authenticating signature is located on the optical disc in a manner which identifies that there is no error detection nor error correction data associated therewith.

For example, where the optical disc carries data in sectors, the authenticating signature may be provided in at least one sector on the optical disc which is in Mode 2 format.

Mode 2 format is a format for sectors on an optical disc which do not include error detection nor error correction data. Accordingly, when a playback device sees a sector which is in the Mode 2 format it does not subject the data in the sector to the error detection and error correction routines. Similarly, circumvention devices making use of the error detection and error correction data to simulate an original disc will be prevented from simulating the authenticating signature by the format of the sector.

In a further embodiment of the invention, where the authenticating signature is provided in a Mode 2 format sector, the authenticating signature can additionally be accompanied in the or each sector by appropriate error detection and error correction data.

In this embodiment, the circumvention device still sees that this data is in Mode 2 format and is thereby unable to access the error detection and error correction data. However, it can be arranged for a playback device to use the error detection and error correction data to obtain a corrected authenticating signature.

The nature of the authenticating signature used in embodiments of the invention may be chosen as required.

In one embodiment, where the optical disc carries a sequence of bits representing data stored on the disc, and the sequence of bits is arranged in sectors, the authenticating signature may have been produced by altering selected bits in at least one sector to provide a pattern of erroneous bits which cannot be corrected during playback.

Preferably, the sequence of bits comprises bits representing content and error correction and error detection data, and the bits which have been altered are bits representing content.

Additionally and/or alternatively, the authenticating signature is made up of data patterns chosen to cause DSV problems for writers of recordable discs.

For example, the data patterns may be chosen to ensure that the DSV has a significant absolute value. Additionally and/or alternatively, the data patterns which are chosen to cause DSV problems may be arranged to have a DSV which has a rapid rate of change.

The present invention also extends to a copy protected optical disc carrying a sequence of bits representing the data stored on the disc, the sequence of bits being arranged in sectors, the optical disc having an authentication signature in at least one sector, the authentication signature having been produced by altering selected bits to provide a pattern of erroneous bits which cannot be corrected during playback, and wherein the authenticating signature is located on the optical disc in a manner which identifies that there is no error detection nor error correction data associated therewith.

According to a further aspect of the present invention there is provided a copy protected optical disc carrying data arranged in sectors and having an authenticating signature in at least one sector, wherein the authenticating signature is made up of data patterns chosen to cause DSV problems for writers of recordable discs, and wherein the authenticating signature is located on the optical disc in a manner which identifies that there is no error detection nor error correction data associated therewith.

The present invention also extends to a method of copy protecting optical discs, the method comprising adding an authenticating signature to an optical disc during its mastering process, the authenticating signature being arranged so that it cannot be accurately copied by a writer for recordable discs, and the method further comprising locating the authenticating signature on the optical disc in a manner which identifies that there is no error detection nor error correction data associated therewith.

In an embodiment, the method further comprises arranging data carried by the optical disc in sectors, and providing the authenticating signature in at least one sector on the optical disc which is in Mode 2 format.

Additionally and/or alternatively, the method further comprises accompanying the authenticating signature in the or each sector with appropriate error detection and error correction data.

A method of an embodiment of the invention further comprises representing data on the optical disc by a sequence of bits encoded onto the disc, and arranging the bits of the sequence in sectors, and producing the authenticating signature by altering selected bits to provide a pattern of erroneous bits which cannot be corrected during playback.

Additionally and/or alternatively, the method comprises making up the authenticating signature from data patterns chosen to cause DSV problems for writers of recordable discs, arranging data carried by the disc in sectors, and locating the authenticating signature in at least one sector.

According to a still further aspect of the present invention there is provided a content file for use in manufacturing a copy protected optical disc carrying an authentication signature, the authentication signature being arranged so that it cannot be accurately copied by a writer of recordable discs, the content file comprising data to be stored on the optical disc, the data being arranged in sectors and being provided with appropriate error detection and error correction data, and the data including the authentication signature which is arranged in at least one sector, the or each sector containing the authentication signature being formatted in a manner which identifies that there is no error detection nor error correction data associated with the authenticating signature.

Preferably the content file is arranged to be used by an encoder during mastering of an optical disc.

Preferably, the or each sector in which the authenticating signature is arranged is in Mode 2 format.

Additionally and/or alternatively, the or each sector containing the authenticating signature also contains appropriate error detection and error correction data.

In an embodiment, the data is to be encoded to form a sequence of bits to be stored on the optical disc, and the content file includes means for altering selected bits of the sequence of bits during encoding to provide a pattern of erroneous bits defining the authenticating signature.

Additionally and/or alternatively, the authenticating signature is made up of data patterns chosen to cause DSV problems for writers of recordable discs.

In an embodiment, the data patterns are chosen to ensure that the DSV has a significant absolute value.

Additionally and/or alternatively, the data patterns which are chosen to cause DSV problems are arranged to have a DSV which has a rapid rate of change.

Embodiments of the present invention will hereinafter be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 shows the surface of a compact disc, very much enlarged, showing the pits thereon,

Figure 2 shows a cross-section of a pit illustrating the data associated therewith,

Figure 3 shows schematically a process for encoding data onto a CD,

Figure 4 shows schematically a mastering process for a CD in which an authenticating signature is added to the disc, Figure 5 shows a logical map of the recording area of a CD having an authenticating signature,

Figure 6 shows the DSV associated with the pits and lands illustrated,

Figure 7 illustrates a Mode 1 sector format,

Figure 8 illustrates a Mode 2 sector format,

Figure 9 illustrates a first example of an embodiment of the present invention,

Figure 10 illustrates a further example of an embodiment of the present invention,

Figure 11 shows a further implementation of an embodiment of the present invention, and

Figure 12 shows a fourth implementation of an embodiment of the present invention.

In the description which follows, the invention is described specifically by reference to the encoding of a CD-ROM and hence with reference to the use of the present invention for copy protecting such a CD-ROM. However, it will be appreciated that the present invention is not limited to use with a CD-ROM and finds application to all data carrying optical discs. Specifically, the invention is applicable to all formats of CDs and to all formats of DVDs.

Furthermore, the description which follows gives one example of the encoding of data onto a CD. Other encoding modes are possible and it will be appreciated that the invention is not limited to the encoding mode.

It will be appreciated that the data to be encoded onto a CD is formatted according to well known standards such that an extensive description of the formatting and encoding is not required and is not provided.

Figure 1 shows an enlarged view of part of a CD showing the pits 6 thereon. As is well known, these pits extend along a spiral track on the surface of the disc and are separated by lands.

Figure 2 shows a section through a pit 6 and land 8 illustrating how data is encoded on a CD. The pits and lands do not represent binary 0s and 1s, but instead represent transitions from one state to another. The data signal is stored in NRZI form (Non-Return to Zero Inverted), where the signal is inverted every time a 1 is encountered. Figure 2 shows the binary value 00100010.

The data stream always consists of pits and lands of at least 3 bits and at most 11 bits long. This is sometimes referred to as a 3T-11T where T is a 1 bit period. A 3T pit has the highest signal frequency (720khz) and an 11T pit has the lowest signal frequency (196khz). A data signal is derived from the lengths of the pits and lands. The data signal derived forms a square wave known as an EFM signal.

Figure 3 shows schematically the encoding of data onto a CD in the form of pits 6 and lands 8. The data is arranged in sectors and initially, and as indicated, there are 2048 bytes of user data in a sector. This is indicated at 10. Then, as illustrated at 12, a sync block, a header, error detection code (EDC) 14 and error correction code (ECC) 16 are added to those original 2048 bytes.

The data at 12 is then scrambled as shown at 18. The scrambling effectively randomizes the data across a sector to reduce the likelihood of repeating patterns of user data which can cause problems.

As indicated at 20, the data is then passed to the CIRC (Cross Interleaved Reed-Solomon Code) encoder. The CIRC encoder, by means of delays, distributes the data across a number of sectors, which also reduces the likelihood of repeating patterns of user data. The data is then passed to the EFM encoder 22 where it is converted into the pattern of 1's and 0's, that is, a sequence of bits. It is the EFM encoded data, which also incorporates merge bits, which is converted into the series of pits and lands, on the disc.

Figure 4 illustrates schematically a mastering process for a CD in which an authenticating signature is added to the disc. In this respect, during the mastering process, data 40 for the glass master and data 42 for the authenticating signature are provided to an encoder 44 associated with a laser beam controller 46. The controller 46 operates the recording laser 48 to write the data to a glass master 50. Original CDs may then be replicated from the glass master in conventional manner.

The data 40 and the data 42, together with appropriate instructions, define a content file for use in the encoding process illustrated in Figure 4. This content file may be provided, for example, on a single CD-R or may be split across two or more CD-Rs.

Figure 5 illustrates a logical map of the data area of a CD having an authenticating signature as described in WO 98/57413. The data area is sub-divided into addressable sectors from the top at address 00 to the final address MAX. The first area 21 is a Lead-In or pre-gap area. The second area is a system area 22 containing, for a CD-ROM, the primary volume descriptor 27. The remaining parts 23, 25 of the data area are available for user data which may, for example, be arranged in user files 28.

In the arrangement shown in Figure 5, a fourth area 24 comprises a padding area 26 made up of error sectors 11 indicated by X and non-error sectors 12. The error sectors 11 together provide the authenticating signature.

Each of the error sectors 11 contains errors made by altering bits in the bit sequence in the particular sector 11. The number of bit errors is such that they are uncorrectable by error correcting rules. In addition, the originally generated error detection and error correction codes are kept so that the data in the error sector 11 is inconsistent with the error detection and error correction codes. Thus, in applying the authenticating signature to the disc, the user data is processed as shown in Figure 3 until the EFM encoding stage. At EFM encoding the signature file causes the alteration of the generated bits to be encoded on to the disc.

When a disc is to be read, it is subject to decoding by a process which is substantially the reverse of that shown in Figure 3. Thus, the decoded sequence of bits is subject to de-interleaving and de-scrambling and then the error detection codes and error correction codes are used by error detection and error correction routines to correct the user data thereby obtained.

However, the signature method shown in Figure 5 ensures that the error sectors 11 are identified as bad sectors by the playing or reading device.

Generally, the copy protected compact disc will include copy protection software requiring the existence of the error sectors at the known locations to be identified before the playback device is enabled to access to the content of the disc.

Previously, a CD having copy protection by way of an authenticating signature as illustrated in Figure 5 prevented writers available to consumers from making usable copies of the disc. Thus, the writer on reading the user data would discard the error correction and error detection codes. The writer would then write the user data obtained to the copy disc by generating a new bit sequence encoding the user data and including newly generated and inherently correct error correction and error detection bits. Therefore, the pattern of logical errors would be lost and no authenticating signature would appear on the copied disc.

However, the new generation of writers for recordable discs which are now available enable the user to specify the error detection and error correction codes to be used when recording data on to a recordable disc. These new writers can be used legitimately, for example, to enable the user to re-record damaged discs. As the error detection and error correction data could be damaged, as well as the user data on the disc, the new generation of writers provide the facility that error detection and error correction data can be chosen during recording. One choice which can be made is to copy the existing error detection and error correction data.

A number of circumvention techniques now make use of this facility to choose the specific error detection and error correction data to make copies of copy protected discs which can trick copy protection software into identifying a copy disc as an original disc.

Thus, the authenticating signature technique generally provides a corrupt sector with error detecting and error correcting codes which are inconsistent with the sector data. When an attempt is made to retrieve the authenticating signature, a bad sector is flagged. The circumvention technique identifies each such bad sector. The copying software is then used to write data to that sector and then to provide error detection and error correction codes which are inconsistent with the written data so that a bad sector is reported. In this respect, to ensure that the error detection and error correction codes are inconsistent with the data written to the sector, the error detection and error correction codes might be copied from the original disc.

When, therefore, the copy disc made by this circumvention technique is played, errors are reported in the same location as on the original disc. That is, the copy protection software identifies bad sectors in the same locations as on the original disc and therefore identifies the existence of the authentication signature signalling that the disc is authentic. Access to the content of the disc is thereby enabled.

In WO 02/11136 there is described a method of providing an authenticating signature which, instead of using errors on the disc, encodes the user data using data patterns which are capable of causing DSV problems. In this respect, the digital sum value (DSV) is the running difference between the number of T values where the EFM represents a pit and the number of T values where the EFM represents a land. As each data bit is read, the DSV is incremented or decremented depending upon whether the data bit corresponds to a pit or a land.

As is indicated in Figure 6, the DSV is determined by assigning the value +1 to each land T, and -1 to each pit T. Ideally, the DSV should stray as little as possible from the zero level. If the DSV has a rapid rate of change over a significant period of time, or if the DSV has substantial low frequency components, then the transitions in the EFM signal may be shifted from their ideal values and/or the ability of tracking and focus circuits in CD drives to maintain optimal head positioning may be compromised. This typically causes read failures from the CD.

Original data, in 8 bit bytes, is passed through EFM encoding to produce 14 bit symbols. The set of 14 bit symbols is especially designed:

to level out the number of pits and lands, to help maintain balanced DSV; and

to ensure that there are no symbols which break the EFM coding scheme of 3T-11T.

However, it is still possible to have two 14 bit symbols, which when joined together would compromise the coding scheme. Accordingly, a set of 3 merge bits are added between each 14 bit symbol to ensure that there are no violations of the 3T-11T coding scheme and to ensure that a suitable DSV is maintained.

In order to maintain good DSV characteristics, the encoder often has a choice in the merge bits to insert between the symbols which carry the data. A sophisticated encoder, such as those which control laser beam recorders, may have the foresight, or can be designed, to choose a pattern of merge bits which is not optimal for the immediate locality where this area is followed by one in which the run length limiting rules dictate the merge bits. The result will be that the overall DSV for the two areas will have better properties. The ability to detect upcoming areas where the merge bit choices are limited is called “look-ahead”. Encoders with a larger look-ahead will be able to make more preparations for encoding the troublesome data and hence the overall encoding will be better. CD writers typically have very little ability to look ahead and hence when they lose control of the DSV, it is more likely to result in an unreadable disc.

The applicants identified a number of values which are capable of causing DSV problems because of their EFM pattern at the pits and lands level. When the patterns for these values are processed through the EFM decoder of a CD drive, the DSV accumulates or decrements and this can result in read failures. Of course, and as indicated above, the encoding process for a CD is designed to prevent values capable of causing DSV problems occurring in the EFM pattern as well as providing robust error correction.

To provide an authenticating signature for a CD, data patterns are chosen which are known to cause DSV problems. For example, and as described above, the data patterns may include sectors filled with repeated values. The glass master is created to have the authenticating signature on it by overcoming the effects of the XOR scrambling and the CIRC encoding.

To overcome the effects of scrambling, the data patterns intended to provide an authenticating signature are XOR'd with the same pattern of scrambling data as is used in the scrambling process indicated at 18 in Figure 3. This scrambled data is then subjected to rest of the process indicated in Figure 3. It will be appreciated that when the scrambled data is subjected to the XOR algorithm on encoding, each byte from the sector will be returned to its original value.

The mixing effect of the CIRC encoder, which is indicated at 20, can be partially overcome by writing multiple copies of the sector. For example, sectors N+1, N+2, N+3 and N+4 will contain the same user data as sector N.

The writers for recordable discs which enable a choice of error detection and error correction data on recording, can also be used to circumvent an authentication signature using DSV data patterns as described above. In this respect, it is necessary during the circumvention technique to identify the sectors on the original disc which include the data patterns known to cause DSV problems. Then the data patterns in those sectors are changed to ones which do not cause DSV problems. However, the original error detection and error correction codes of those sectors are kept. The copy disc can then be written without problem, and when this copy disc is read the original data will be output because of the presence of the original error detection and error correction codes.

The present invention provides techniques for defeating the further circumvention techniques described above.

It will be seen in Figure 3, for example, that the sectors 12 containing the user data are provided with error detection and error correction codes 14 and 16. This is an extra level of error correction, over and above that associated with the de-interleaving and de-scrambling routines. This further error correction is required when the data on a disc is computer data, programs, text and the like, where accurate decoding is essential.

The sector 12 illustrated in Figure 3 is a Mode 1 sector. The elements of a Mode 1 sector are shown in more detail in Figure 7. As can be seen in Figure 7, the sector 12 comprises 12 sync bytes. The header is divided into 3 A-time bytes and a single byte identifying the Mode. In this case the Mode is 1. The 2048 bytes of user data are then followed by error detecting data 14 and error correcting data 16.

It will be appreciated that when decoding the data on a CD the C1 and C2 decoders which perform the de-interleaving and de-scrambling provide two levels of error correction. The error detecting and error correcting data in Mode 1 therefore provides a third level of error correction.

As set out above, the Mode 1 format sector is mandatory for computer data. However, it is not needed for data such as audio and video where interpolation can be used instead of error correction. Accordingly, it is possible to format audio and video user data in Mode 2 sectors as illustrated in Figure 8.

In Figure 8, the sector 112 has the sync data and the header divided into A-time and mode as in the Mode 1 format. However, the Mode is set as 2. Thereafter, the sector is filled with 2336 bytes of user data.

To prevent the circumvention techniques as described above from using the error detection and error correction data to simulate original discs, it is proposed that an authenticating signature, as described, should be incorporated in one or more sectors formatted as Mode 2 sectors.

A first example of the invention is shown in Figure 9 in which an authenticating signature, or part thereof, is stored in a Mode 2 format sector 112. This authenticating signature might be identical to that used previously and thus will comprise only 2048 bytes of user data. The sector 112 therefore has 288 bytes of undefined data.

The circumvention techniques described above are not able to alter the data within the sector 112 as described above because of the omission of the error detection and error correction data. A copy of the sector can still be made but the copy protection will then work as designed. Thus, if the authenticating signature includes data patterns chosen to cause DSV problems, the resultant copy disc will have DSV problems and is likely to be unreadable. If the authenticating signature is a corrupt sector, the C1 and C2 error correction should still flag the existence of the bad sector such that the data therein will not be written to the copy disc in a format identifiable as an authenticating signature.

Figure 10 shows a similar embodiment to that of Figure 9 except that all of the area in sector 112 available for user data has been made available for the authenticating signature or part thereof. This means that the authenticating signature can be made larger, and therefore more effective.

In the embodiment as shown in Figure 11 there is a sector 122 which appears to have the content of a Mode 1 format sector but is specified to be in Mode 2 format. The sector 122 might have been produced, for example, by copying a Mode 1 sector including an authenticating signature and writing it as a Mode 2 format. Thus, the user data in the sector 122 includes the authenticating signature which is followed by its original error detection and error correction codes. However, when trying to circumvent the copy protection on the disc as described, the copying device identifies the error detection and error correction data in sector 122 as user data. Additionally, the copy protection software can be arranged to access this data to perform error correction routines on the authenticating signature. The embodiment shown in Figure 11, therefore, is more robust as it enables the player or reader of the original disc to obtain the authenticating signature even if there are defects on the original disc.

Figure 12 shows a sector 122 having a similar format to that of Figure 11 except that an extra user data area 100 is used to store specific error detection and error correction data to provide error correction for the authenticating signature. The type of error detection and error correction data may be specified as required and may be, for example, Hamming Code as defined in Federal Standard 1037C.

It will be appreciated that variations in and modifications to the invention as described and illustrated may be made within the scope of the appended claims.

CLAIMS

1. A copy protected optical disc carrying an authentication signature, the authentication signature being arranged so that it cannot be accurately copied by a writer of recordable discs, and wherein the authenticating signature is located on the optical disc in a manner which identifies that there is no error detection nor error correction data associated therewith.

2. A copy protected optical disc as claimed in Claim 1, carrying data in sectors, and wherein the authenticating signature is provided in at least one sector on the optical disc which is in Mode 2 format.

3. A copy protected optical disc as claimed in Claim 2, wherein the authenticating signature is accompanied in the or each sector by appropriate error detection and error correction data.

4. A copy protected optical disc as claimed in any preceding claim, carrying a sequence of bits representing data stored on the disc, the sequence of bits being arranged in sectors, and wherein the authenticating signature has been produced by altering selected bits in at least one sector to provide a pattern of erroneous bits which cannot be corrected during playback.

5. A copy protected optical disc as claimed in Claim 4, wherein the sequence of bits comprises bits representing content and error correction and error detection data, and wherein the bits which have been altered are bits representing content.

6. A copy protected optical disc as claimed in any preceding claim, wherein the authenticating signature is made up of data patterns chosen to cause DSV problems for writers of recordable discs.

7. A copy protected optical disc as claimed in Claim 6, wherein the data patterns are chosen to ensure that the DSV has a significant absolute value.

8. A copy protected optical disc as claimed in Claim 6 or Claim 7, wherein the data patterns which are chosen to cause DSV problems are arranged to

have a DSV which has a rapid rate of change.

9. A copy protected optical disc carrying a sequence of bits representing the data stored on the disc, the sequence of bits being arranged in sectors, the optical disc having an authentication signature in at least one sector, the authentication signature having been produced by altering selected bits to provide a pattern of erroneous bits which cannot be corrected during playback, and wherein the authenticating signature is located on the optical disc in a manner which identifies that there is no error detection nor error correction data associated therewith.

10. A copy protected optical disc as claimed in Claim 9, carrying data in sectors and wherein the authenticating signature is provided in at least one sector on the optical disc which is in Mode 2 format.

11. A copy protected optical disc as claimed in Claim 10, wherein the authenticating signature is accompanied in the or each sector by appropriate error detection and error correction data.

12. A copy protected optical disc as claimed in any of Claims 9 to 11, wherein the sequence of bits comprises bits representing content and error correction and error detection data, and wherein the bits which have been altered are bits representing content.

13. A copy protected optical disc carrying data arranged in sectors and having an authenticating signature in at least one sector, wherein the authenticating signature is made up of data patterns chosen to cause DSV problems for writers of recordable discs, and wherein the authenticating signature is located on the optical disc in a manner which identifies that there is no error detection nor error correction data associated therewith.

14. A copy protected optical disc as claimed in Claim 13, carrying data in sectors and wherein the authenticating signature is provided in at least one sector on the optical disc which is in Mode 2 format.

15. A copy protected optical disc as claimed in Claim 14, wherein the

authenticating signature is accompanied in the or each sector by appropriate error detection and error correction data.

16. A copy protected optical disc as claimed in any of Claims 13 or Claim 15, wherein the data patterns are chosen to ensure that the DSV has a significant absolute value.

17. A copy protected optical disc as claimed in any of Claims 13 to 16, wherein the data patterns which are chosen to cause DSV problems are arranged to have a DSV which has a rapid rate of change.

18. A method of copy protecting optical discs, the method comprising adding an authenticating signature to an optical disc during its mastering process, the authenticating signature being arranged so that it cannot be accurately copied by a writer for recordable discs, and the method further comprising locating the authenticating signature on the optical disc in a manner which identifies that there is no error detection nor error correction data associated therewith.

19. A method of copy protecting optical discs as claimed in Claim 18, further comprising arranging data carried by the optical disc in sectors, and providing the authenticating signature in at least one sector on the optical disc which is in Mode 2 format.

20. A method of copy protecting optical discs as claimed in Claim 19, further comprising accompanying the authenticating signature in the or each sector with appropriate error detection and error correction data.

21. A method of copy protecting optical discs as claimed in any of Claims 18 to 20, the method comprising representing data on the optical disc by a sequence of bits encoded onto the disc, and arranging the bits of the sequence in sectors, and producing the authenticating signature by altering selected bits to provide a pattern of erroneous bits which cannot be corrected during playback.

22. A method of copy protecting optical discs as claimed in any of Claims 18 to 21, the method comprising making up the authenticating signature from data

patterns chosen to cause DSV problems for writers of recordable discs, arranging data carried by the disc in sectors, and locating the authenticating signature in at least one sector.

23. A content file for use in manufacturing a copy protected optical disc carrying an authentication signature, the authentication signature being arranged so that it cannot be accurately copied by a writer of recordable discs, the content file comprising data to be stored on the optical disc, the data being arranged in sectors and being provided with appropriate error detection and error correction data, and the data including the authentication signature which is arranged in at least one sector, the or each sector containing the authentication signature being formatted in a manner which identifies that there is no error detection nor error correction data associated with the authenticating signature.

24. A content file for use in manufacturing a copy protected optical disc carrying an authentication signature as claimed in Claim 23, wherein the or each sector in which the authenticating signature is arranged is in Mode 2 format.

25. A content file for use in manufacturing a copy protected optical disc carrying an authentication signature as claimed in Claim 24, wherein the or each sector containing the authenticating signature also contains appropriate error detection and error correction data.

26. A content file for use in manufacturing a copy protected optical disc carrying an authentication signature as claimed in any of Claims 23 to 25, wherein the data is to be encoded to form a sequence of bits to be stored on the optical disc, and wherein the content file includes means for altering selected bits of the sequence of bits during encoding to provide a pattern of erroneous bits defining the authenticating signature.

27. A content file for use in manufacturing a copy protected optical disc carrying an authentication signature as claimed in any of Claims 23 to 26, wherein the authenticating signature is made up of data patterns chosen to cause DSV problems for writers of recordable discs.

28. A content file for use in manufacturing a copy protected optical disc carrying an authentication signature as claimed in Claim 27, wherein the data patterns are chosen to ensure that the DSV has a significant absolute value.

29. A content file for use in manufacturing a copy protected optical disc carrying an authentication signature as claimed in Claim 27 or Claim 28, wherein the data patterns which are chosen to cause DSV problems are arranged to have a DSV which has a rapid rate of change.

30. A copy protected optical disc carrying an authentication signature substantially as hereinbefore described with reference to the accompanying drawings.

31. A method of copy protecting optical discs substantially as hereinbefore described with reference to the accompanying drawings.

32. A content file for use in manufacturing a copy protected optical disc substantially as hereinbefore described with reference to the accompanying drawings.

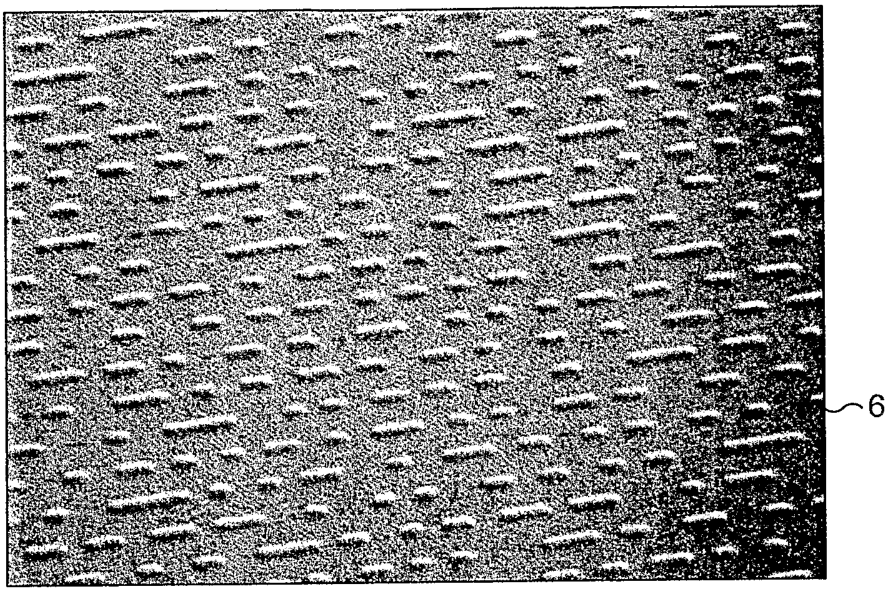


FIG. 1

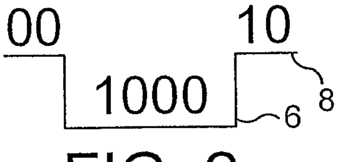


FIG. 2

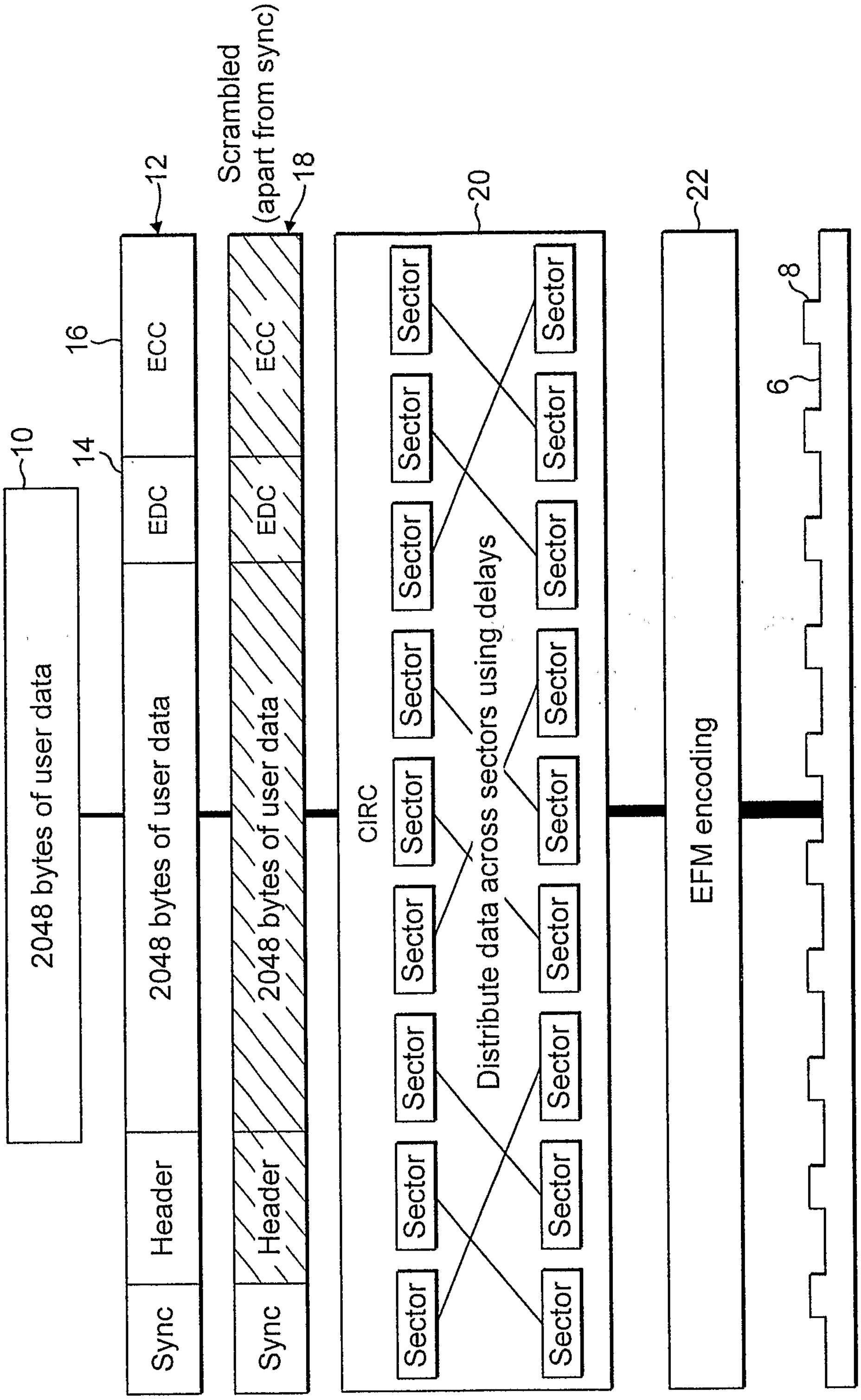

10
2048 bytes of user data
12
14
16
Sync
Header
2048 bytes of user data
EDC
ECC
Scrambled
(apart from sync)
18
Sync
Header
2048 bytes of user data
EDC
ECC
20
CIRC
Sector
Sector
Sector
Sector
Sector
Sector
Sector
Sector
Sector
Sector
Sector
Sector
Sector
Sector
Sector
Sector
Distribute data across sectors using delays
22
EFM encoding
6
8

FIG. 3

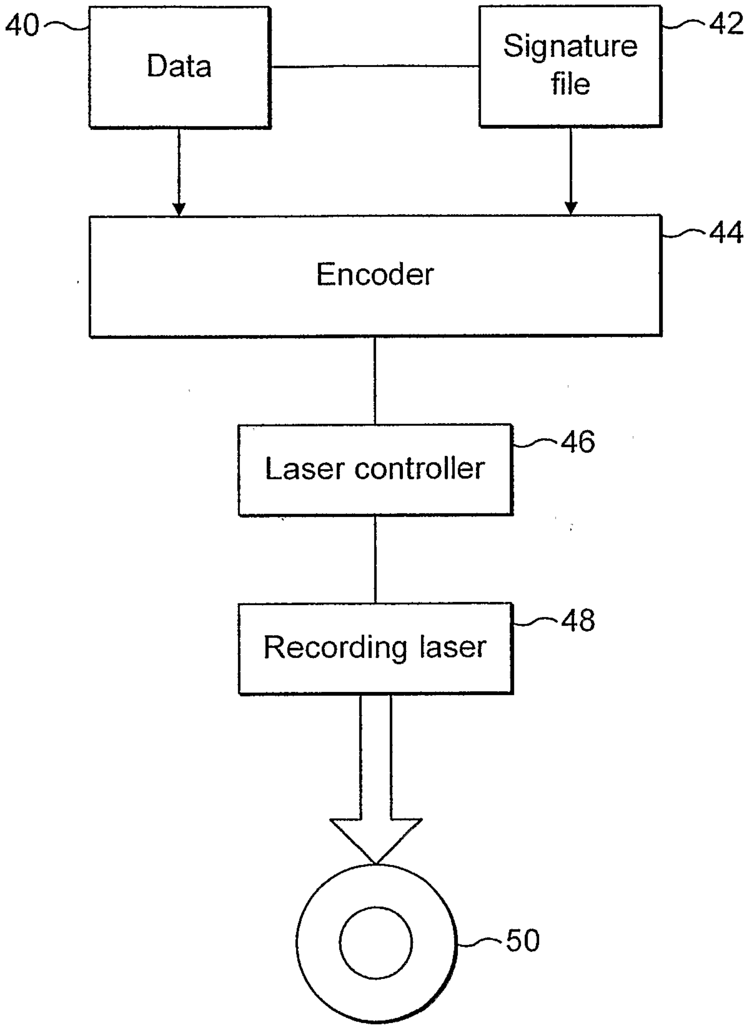

40
Data
Signature file
42
Encoder
44
Laser controller
46
Recording laser
48
50

FIG. 4

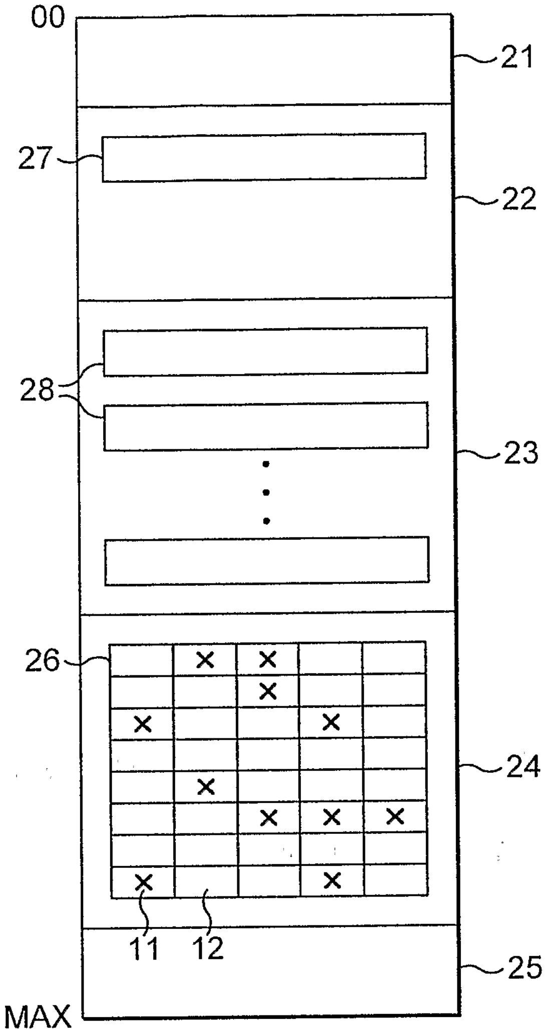

00
21
27
22
28
23
26
24
11
12
25
MAX

FIG. 5

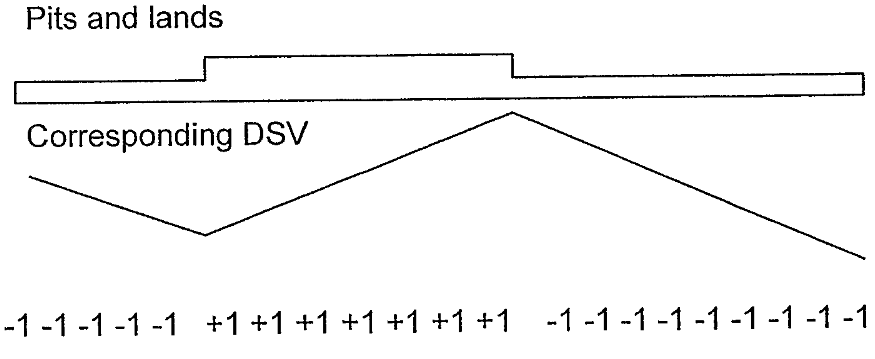

Pits and lands
Corresponding DSV
-1 -1 -1 -1 -1
+1 +1 +1 +1 +1 +1 +1
-1 -1 -1 -1 -1 -1 -1 -1 -1

FIG. 6

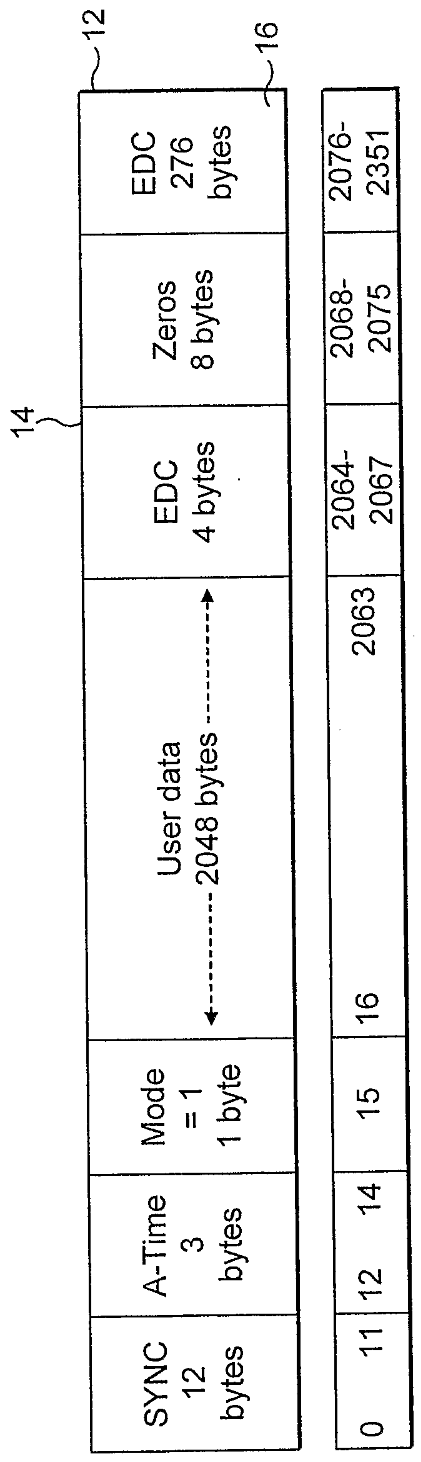

12
14
16
SYNC 12 bytes
A-Time 3 bytes
Mode = 1 1 byte
User data 2048 bytes
EDC 4 bytes
Zeros 8 bytes
EDC 276 bytes
0
11
12
14
15
16
2063
2064-2067
2068-2075
2076-2351

FIG. 7

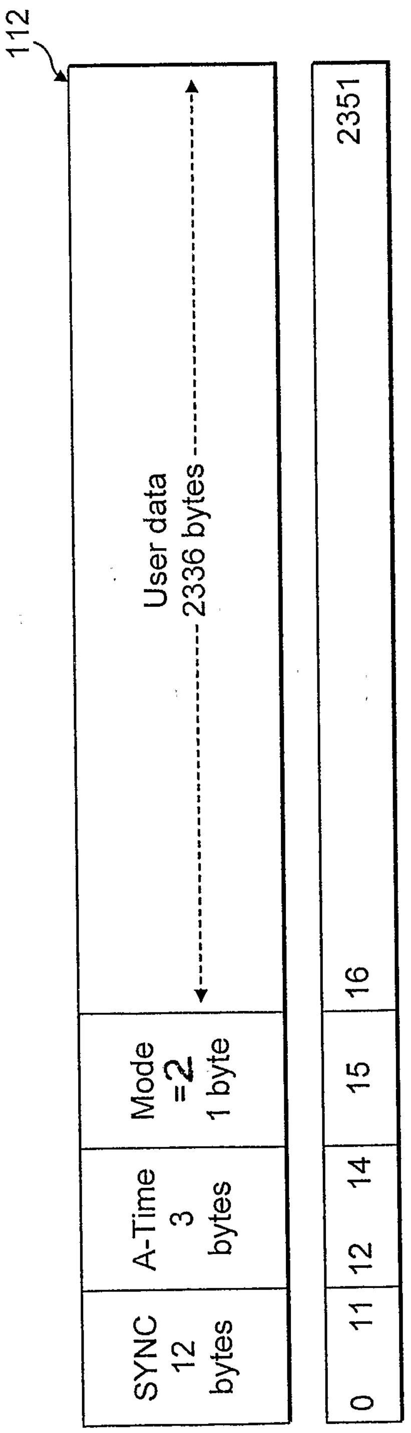

112
SYNC 12 bytes
A-Time 3 bytes
Mode =2 1 byte
User data 2336 bytes
0
11
12
14
15
16
2351

FIG. 8

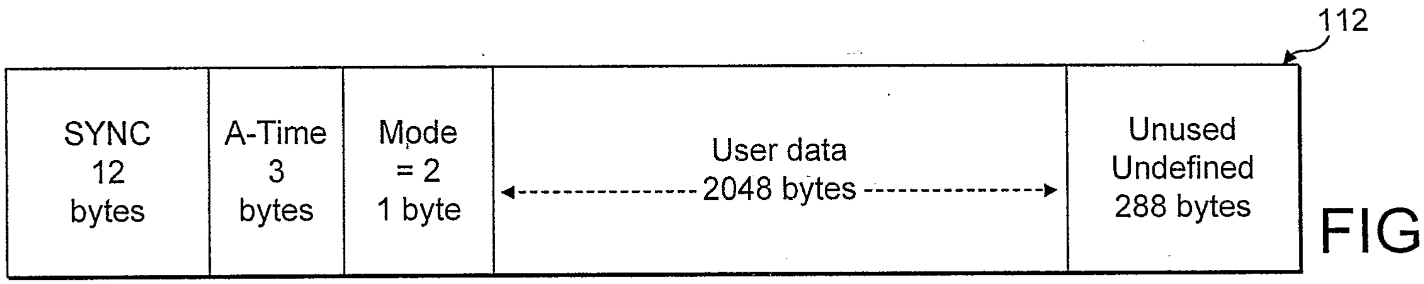


FIG. 9

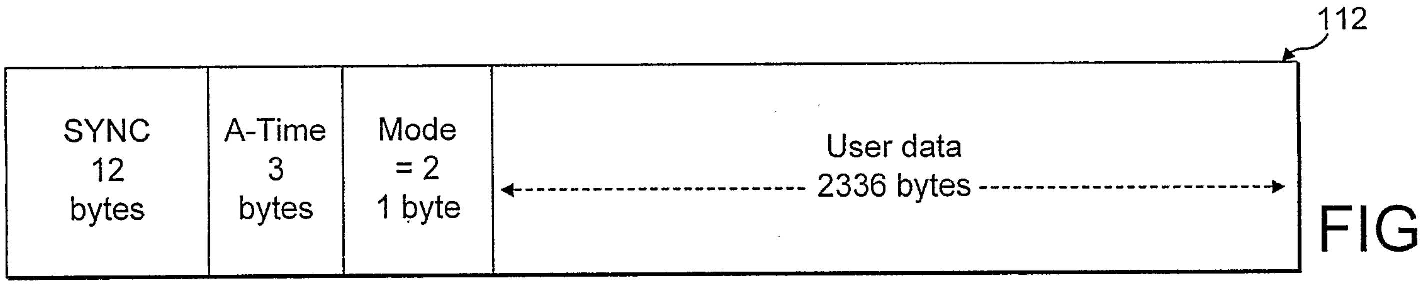


FIG. 10

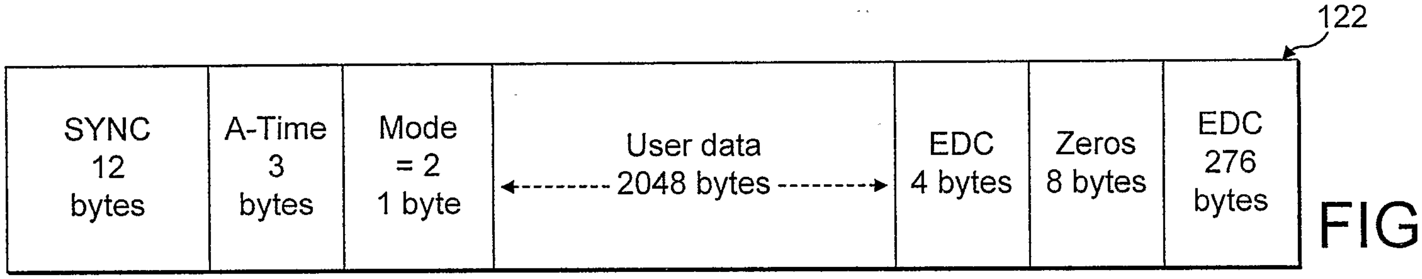


FIG. 11

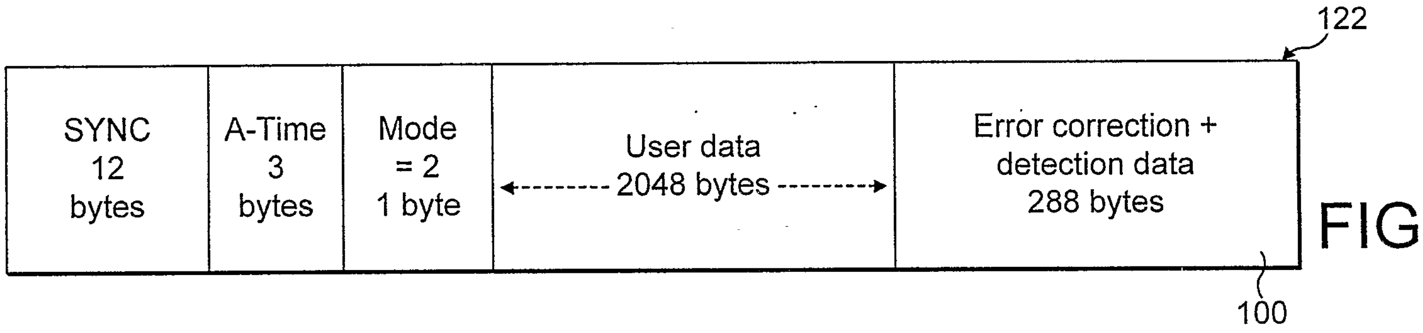


FIG. 12

INTERNATIONAL SEARCH REPORT

onal application No
GB2005/004910

A. CLASSIFICATION OF SUBJECT MATTER
G11B20/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G11B

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

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

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 104 679 A (SOLLISH ET AL) 15 August 2000 (2000-08-15) column 4, line 67 - column 5, line 52 column 6, line 63 - column 7, line 29 column 7, line 55 - column 8, line 21	1,18, 30-32
Y	column 10, line 32 - line 37	4-9,12, 13,16, 17, 21-23, 26-29

Y	WO 02/11136 A (MACROVISION EUROPE LIMITED; HEYLEN, RICHARD, A., A) 7 February 2002 (2002-02-07) cited in the application page 4, line 1 - line 12	6-8,13, 16,17, 22,27-29

	-/--	

☒ 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 document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 21 March 2006	Date of mailing of the international search report 28/03/2006
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Ogor, M

INTERNATIONAL SEARCH REPORT

tional application No
/GB2005/004910

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 98/54713 A (C-DILLA LIMITED) 3 December 1998 (1998-12-03) cited in the application abstract page 9, line 14 - page 10, line 12	4,5,9, 12,21, 23,26
A	EP 1 204 111 A (MITSUBISHI CHEMICAL CORPORATION) 8 May 2002 (2002-05-08) paragraphs [0030], [0032], [0033]	1,9,13, 18,23, 30-32
A	US 6 718 501 B1 (BRODY MOSHE ET AL) 6 April 2004 (2004-04-06) column 17, line 26 - line 40 column 26, line 48 - line 57	1,9,13, 18,23, 30-32
A	US 6 215 750 B1 (SAKO YOICHIRO ET AL) 10 April 2001 (2001-04-10) column 6, line 8 - column 7, line 4 figures 7,8	
A	POHLMANN ED - POHLMANN K C: "THE COMPACT DISC HANDBOOK" COMPACT DISC HANDBOOK, OXFORD, OUP, GB, 1992, pages 213-221, XP002033060 the whole document	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2005/004910

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6104679 A	15-08-2000	NONE	
WO 0211136 A	07-02-2002	AU 7570901 A	13-02-2002
		BR 0112805 A	01-07-2003
		CA 2416314 A1	07-02-2002
		CN 1466755 A	07-01-2004
		EP 1305799 A1	02-05-2003
		GB 2369718 A	05-06-2002
		JP 2004505403 T	19-02-2004
		MX PA03000851 A	13-12-2004
		NZ 523625 A	30-07-2004
		PL 363776 A1	29-11-2004
		US 2002076046 A1	20-06-2002
WO 9854713 A	03-12-1998	AT 302462 T	15-09-2005
		AU 7228298 A	30-12-1998
		BR 9804931 A	08-09-1999
		CA 2261899 A1	03-12-1998
		CN 1516155 A	28-07-2004
		CN 1236468 A	24-11-1999
		CN 1606085 A	13-04-2005
		DE 69831275 D1	22-09-2005
		DK 1227482 T3	02-01-2006
		ES 2247261 T3	01-03-2006
		HK 1024086 A1	21-10-2005
		JP 2001507849 T	12-06-2001
		KR 2000029683 A	25-05-2000
		TW 399200 B	21-07-2000
		US 6353890 B1	05-03-2002
EP 1204111 A	08-05-2002	WO 0079532 A1	28-12-2000
		US 2002080960 A1	27-06-2002
US 6718501 B1	06-04-2004	AU 1727701 A	12-06-2001
		BR 0016182 A	27-08-2002
		DE 10084721 B4	25-11-2004
		DE 10084721 T0	21-08-2003
		EP 1245025 A2	02-10-2002
		GB 2371916 A	07-08-2002
		WO 0141130 A2	07-06-2001
		JP 2003535420 T	25-11-2003
		MX PA02005360 A	05-05-2004
US 6215750 B1	10-04-2001	US 5966359 A	12-10-1999