*150150*

*G00002*

# DESCRIPTION

# RECORDING APPARATUS AND METHOD, REPRODUCING APPARATUS AND METHOD, AND MEMORY MEDIUM

## Technical Field

The invention relates to recording apparatus and method, reproducing apparatus and method, and a memory medium which are suitable for use in a case where when data of contents is recorded/reproduced to/from a disc such as a CD (Compact Disc) 2, the data is encrypted in order to protect the contents data.

## Background Art

In recent years, data of contents can be easily copied owing to the spread of a recordable memory medium such as CD-R (Compact Disc Recordable) or CD-RW (Compact Disc ReWritable). A service such that music data is distributed onto a network has been started to spread owing to the development of the network. Therefore, it is becoming an important issue to protect a copyright holder by restricting copy and reproduction of contents data such as audio data.

Hitherto, an SCMS (Serial Copy Management System) has been used as copyright management information for protecting audio data. In the SCMS, "copy freely"/"copy never" and "copy one generation" can be managed. However, if only the SCMS is used, only simple copyright management

such that an illegal copy is merely prevented can be made.

Therefore, copyright management information in a complicated format such that restriction of the number of copies, restriction of the number of reproducing times, restriction of a reproducing time, charge, or the like can be performed is necessary. If the copyright management information such that the restriction of the number of copies, the restriction of the number of reproducing times, the restriction of a reproducing time, the charge, or the like can be performed is used, a music piece can be reproduced only the predetermined number of times or only for a predetermined period of time in order to be monitored. It is possible to execute services in various forms such that if the music piece is charged for, the music piece can be always listened to, the music piece is charged for in accordance with the number of reproducing times or a reproducing time, and the like.

If such services are started, it is necessary to encrypt the contents data so as to enable desired music pieces among music pieces stored in a memory medium to be listened to the predetermined number of reproducing times or for a predetermined period of time or enable only the user who has been charged to listen to the music pieces. It is also necessary to encrypt the contents data in order to prevent an illegal copy from being frequently performed. For this purpose, key information to decrypt the encryption is necessary.

As mentioned above, in case of selling or distributing the contents data such as audio data, the copyright management information and the key information which is used for decrypting the encryption are necessary. Since the copyright management information or key information has a size of at most about 256 kbits, it hardly becomes a burden on a memory capacity. However, it is necessary to take security into consideration lest the copyright management information or key information leaks to the outside or is easily rewritten.

If the copyright management information and the key information which is used for decrypting the encryption are inserted into a main data area together with the contents data, a data capacity for which the contents data can be recorded is reduced by an amount corresponding thereto, and there is also a possibility that the copyright management information or the encryption information leaks to the outside and is rewritten, so that there is a problem on the security.

In the case where the memory medium is, for example, a CD, there is a method whereby the copyright management information or the encryption information is inserted into a subcode. However, defined information has already been inserted in the subcode. There is also a case where data of the subcode is rewritten each time the disc is edited.

It is, therefore, an object of the invention to provide recording apparatus and method, reproducing

apparatus and method, and a memory medium storage, in which copyright information and key information can be safely stored and they do not become a burden on a data capacity.

## Disclosure of Invention

According to the present invention, there is provided a recording apparatus comprising: input means for inputting encryption data; and recording means for recording the encryption data which is inputted into a data area on a memory medium having the data area, a lead-in area, and a lead-out area and recording additional information corresponding to the encryption data into the lead-out area.

According to the present invention, there is provided a recording apparatus comprising: input means for inputting encryption data; and recording means for recording the encryption data which is inputted into data areas on a memory medium having the plurality of data areas, a plurality of lead-in areas, and a plurality of lead-out areas and recording additional information corresponding to the encryption data into one of the plurality of lead-in areas or one of the plurality of lead-out areas.

According to the present invention, there is provided a reproducing apparatus comprising: reading means for reading out stored encryption data from a data area on a memory medium having the data area, a lead-in area, and a lead-out area and reading out additional information stored in the lead-out area; and reproducing means for reproducing

the encryption data in accordance with the read-out additional information.

According to the present invention, there is provided a reproducing apparatus comprising: reading means for reading out encryption data from one of a plurality of data areas on a memory medium having the plurality of data areas, a plurality of lead-in areas, and a plurality of lead-out areas and reading out additional information corresponding to the encryption data from one of the plurality of lead-in areas or one of the plurality of lead-out areas; and reproducing means for reproducing the encryption data in accordance with the read-out additional information.

According to the present invention, there is provided a recording method comprising the steps of: inputting encryption data; recording the encryption data which is inputted into a data area on a memory medium having the data area, a lead-in area, and a lead-out area; and recording additional information corresponding to the encryption data into the lead-out area.

According to the present invention, there is provided a recording method comprising the steps of: inputting encryption data; recording the encryption data which is inputted into data areas on a memory medium having the plurality of data areas, a plurality of lead-in areas, and a plurality of lead-out areas; and recording additional information corresponding to the encryption data into one of the plurality of lead-in areas or one of the plurality

of lead-out areas.

According to the present invention, there is provided a reproducing method comprising the steps of: reading out stored encryption data from a data area on a memory medium having the data area, a lead-in area, and a lead-out area; reading out additional information stored in the lead-out area; and reproducing the encryption data in accordance with the read-out additional information.

According to the present invention, there is provided a reproducing method comprising the steps of: reading out encryption data from one of a plurality of data areas on a memory medium having the plurality of data areas, a plurality of lead-in areas, and a plurality of lead-out areas; reading out additional information corresponding to the encryption data from one of the plurality of lead-in areas or one of the plurality of lead-out areas; and reproducing the encryption data in accordance with the read-out additional information.

According to the invention, there is provided a memory medium which has a data area, a lead-in area, and a lead-out area and in which encryption data is recorded into the data area and additional information corresponding to the encryption data is recorded into the lead-out area.

According to the invention, there is provided a memory medium which has a plurality of data areas, a plurality of lead-in areas, and a plurality of lead-out areas and in which encryption data which is inputted to the data areas

is recorded and additional information corresponding to the encryption data is recorded into one of the plurality of lead-in areas or one of the plurality of lead-out areas.

When the encryption data is recorded into the data area on the memory medium having the data area, lead-in area, and lead-out area, copyright management information and key information for the encryption data are recorded into the lead-out area.

In case of a memory medium having a plurality of data areas, a plurality of lead-in areas, and a plurality of lead-out areas like CD2, when the encryption data is recorded into the data area, the copyright management information and key information corresponding to the encryption data are recorded into one of the plurality of lead-in areas or lead-out areas.

In a present situation, only information in the Q channel of the subcode has been recorded in the lead-out area and this area is filled with dummy data. The position of the lead-out area is obtained from information of a TOC. The fact that a light spot has entered the lead-out area can be judged from the information in the Q channel. The copyright management information and the key information are recorded by using such a lead-out area. The lead-out area is not rewritten or accessed by an ordinary CD player, so that the copyright management information and the key information can be safely held.

Brief Description of Drawings

Fig. 1 is a schematic diagram of an example of a disc to which the invention is applied; Fig. 2 is a block diagram of an example of a recording apparatus to which the invention is applied; Fig. 3 is a block diagram of an example of a reproducing apparatus to which the invention is applied; Fig. 4 is a schematic diagram of an example of a recording format of copyright management information and key information; Fig. 5 is a flowchart for use in explanation of the reproducing apparatus to which the invention is applied; Figs. 6A to 6D are schematic diagrams for use in explanation of an embodiment of the invention; Figs. 7A to 7D are schematic diagrams for use in explanation of the embodiment of the invention; Fig. 8 is a schematic diagram of another example of a disc to which the invention is applied; and Figs. 9A to 9D are schematic diagrams for use in explanation of the embodiment of the invention.

Best Mode for Carrying Out the Invention

An embodiment of the invention will be described hereinbelow with reference to the drawings. The invention is suitable, for example, when it is used for encrypting data of contents and protecting the data when the contents data is recorded/reproduced to/from CD2.

CD2 is an optical disc having a shape similar to that of the ordinary CD and is separated into an area AR1 on the inner rim side and an area AR2 on the outer rim side

as shown in Fig. 1. A mirror portion M1 is provided between the area AR1 on the inner rim side and the area AR2 on the outer rim side. A lead-in area LIN1 is provided in the innermost rim of the area AR1 on the inner rim side and a lead-out area LOUT1 is provided in the outermost rim. A lead-in area LIN2 is provided in the innermost rim of the area AR2 on the outer rim side and a lead-out area LOUT2 is provided in the outermost rim.

For example, music data is recorded as PCM data as it is into the area AR1 on the inner rim side so that it can be reproduced even by an ordinary CD player. In the area AR1 on the inner rim side, usually, encryption is not executed either.

On the other hand, in the area AR2 on the outer rim side, for example, music data is compressed by MP3 (MPEG1 Audio Layer-3) or the like and recorded so that data can be recorded at a double density and affinity with a personal computer can be obtained. By compressing the music data by MP3 or the like and recording it, a recording capacity can be increased and the data can be handled by a file system similar to that of the personal computer. In the area AR2 on the outer rim side, since the data is often taken out to the outside, the data is encrypted and recorded.

As mentioned above, CD2 can be reproduced by the CD player by using the area AR1 on the inner rim side in a manner similar to the ordinary CD. By using the area AR2 on the outer rim side, the data can be handled in an

interlocking relational manner with the personal computer.

In such CD2, particularly, the invention is suitable for use in case of encrypting data of contents when the contents data is encrypted and recorded/reproduced to/from the area AR2 on the outer rim side.

Fig. 2 shows an example of a recording apparatus to which the invention is applied. In Fig. 2, the contents data is supplied to an input terminal 1. For example, the contents data is audio data (music data). A construction such that besides the audio data, various data such as motion image data, still image data, program data of games, data of a Web page, etc. is recorded as contents data is considered. The contents data from the input terminal 1 is supplied to an encrypting circuit 4.

Key information K is supplied to an input terminal 2. The key information K from the input terminal 2 is supplied to the encrypting circuit 4.

The encrypting circuit 4 encrypts the contents data from the input terminal 1 by using the key information K from the input terminal 2.

An output of the encrypting circuit 4 is supplied to an error correction encoding circuit 5. In the error correction encoding circuit 5, an error correction code is added to the contents data encrypted by the encrypting circuit 4.

An output of the error correction encoding circuit 5 is supplied to a modulating circuit 6. In the modulating

circuit 6, the recording data is modulated by a predetermined modulating system. An output of the modulating circuit 6 is supplied to a recording circuit 7.

An output of the recording circuit 7 is supplied to an optical pickup 8. The data is recorded onto a disc 10 by the optical pickup 8. The disc 10 is, for example, a disc of CD2.

The key information K from the input terminal 2 is supplied to a mixing circuit 9. Copyright management information R is supplied to an input terminal 3. The copyright management information R is supplied to the mixing circuit 9 via a rewriting circuit 11. An output of the mixing circuit 9 is supplied to the optical pickup 8 via a recording circuit 12. The key information K and copyright management information R are recorded onto the disc 10 by the optical pickup 8.

The copyright management information R is information for managing, for example, copy inhibition/permission, generation management of the copy, restriction of the number of copies, reproduction inhibition/permission, restriction of the number of reproducing times, restriction of a reproducing time, and the like. In case of performing the generation management of the copy, the restriction of the number of copies, the restriction of the number of reproducing times, or the restriction of the reproducing time, it is necessary to rewrite the copyright management information R each time

the copy or reproduction is performed. The rewriting of the copyright management information R is performed by the rewriting circuit 11.

The key information K and copyright management information R are recorded into the lead-out area on the disc 10. That is, the disc 10 is, for example, a disc of CD2. In case of the disc of CD2, as shown in Fig. 1, the contents data is encrypted and recorded into the area AR2. In this case, the key information K and copyright management information R are recorded into the lead-out LOUT2 in the outer rim of the area AR2.

Fig. 3 shows a construction of a reproducing system. In Fig. 3, a recording signal on a disc 20 is reproduced by an optical pickup 22. The disc 20 is, for example, a disc of CD2. An output of the optical pickup 22 is supplied to a demodulating circuit 24 via a reproducing amplifier 23. The motion of the optical pickup 22 is controlled by an access control circuit 30 on the basis of a control of a system controller 29.

As mentioned above, the key information K and the copyright management information R have been recorded into the lead-out area on the disc 20. Therefore, in case of decrypting the data recorded on the disc 20, the optical pickup 22 is moved to the lead-out area by the access control circuit 30. The key information K and the copyright management information R are read out from the lead-out area.

An output of the demodulating circuit 24 is

supplied to an error correcting circuit 25. An error correcting process is executed by the error correcting circuit 25. An output of the error correcting circuit 25 is supplied to an encryption decoding circuit 26 and supplied to a key management information reading circuit 27. An output of the key management information reading circuit 27 is supplied to the encryption decoding circuit 26.

The encryption decoding circuit 26 executes a process for decrypting the encryption of the reproduction data by using the key information K read out by the key management information reading circuit 27. The copy or reproduction is restricted by the copyright management information R read out by the key management information reading circuit 27.

An output of the encryption decoding circuit 26 is supplied to a reproducing circuit 28. An output of the reproducing circuit 28 is outputted from an output terminal 31.

As mentioned above, if the discs 10 and 20 are discs of, for example, CD2, the contents data is encrypted and recorded into the recording area AR2 on the outer rim side. The copyright management information R and the key information K at this time are recorded into the lead-out area LOUT2 (Fig. 1) existing in the outer rim of the recording area AR2.

Information indicative of the lead-out has been recorded in the Q channel of the subcode in the lead-out

area LOUT2. That is, with respect to track numbers TNO in the Q channel of the subcode, "00" indicates the lead-in, "01" to "99" denote numbers of movements or the like, and "AA" shows the lead-out. Whether the area is the lead-out area LOUT2 or not can be judged from the track number. When a TOC (Table Of Contents) indicates (POINT = 2), a time when the lead-out starts is shown. The position of the lead-out is known by it.

Usually, only the information in the Q channel of the subcode is stored in the lead-out area LOUT2 and this area is filled with dummy data. The copyright management information R and the key information K are recorded in place of the dummy data. Therefore, a sufficient area for recording the copyright management information R and the key information K can be held in the lead-out area LOUT2.

Fig. 4 shows an example of a format of recording information in case of recording the copyright management information and the key information.

As shown in Fig. 4, a version number of a key is provided at the head. When the encryption is decrypted, the key is updated to a new key and, at this time, the version number is incremented. Subsequently, information indicative of the number of keys is provided and the key information K of the number as many as the number of keys is provided. Subsequently, the number of copyright management information is provided and the copyright management information R of the number as many as the number

of copyright management information is provided. The number of keys or the number of copyright management information corresponds to the number of programs recorded as contents. Lastly, a CRC (Cyclic Redundancy Check) code is added.

An error can be detected by the CRC code and falsification of the copyright management information R or key information K can be prevented. That is, the number of copies and the number of reproducing times are included as copyright management information R. It is presumed that the number of copies or the number of reproducing times is purposely rewritten. If such a rewriting is performed, an error is caused by the CRC code. The falsification of the copyright management information R or the key information K is prevented by this method. A code for authentication can be also recorded in place of the CRC code.

In the ordinary CD player or CD drive for a personal computer, the position of the lead-out area LOUT2 has previously been known from the information of the TOC. The ordinary player does not reproduce the data in the lead-out area LOUT2. Therefore, according to the ordinary CD player or CD drive, the copyright management information R or the key information K of the encryption which have been recorded in the lead-out area LOUT2 is not taken out to the outside. It is considered that even if all of the contents of the disc are copied as they are to another disc by using the ordinary CD player or CD drive, the copyright management

information R and the key information K in the lead-out LOUT2 are not copied.

Fig. 5 is a flowchart showing the reproducing operation in the case where the copyright management information R and the key information K are recorded into the lead-out area LOUT2.

First, the lead-in area LIN2 of the area AR2 is accessed and the TOC information is read out from the lead-in area LIN2 (step S1). The position of the lead-out area LOUT2 is judged from the TOC information (step S2). The lead-out area LOUT2 is accessed and the copyright management information R and the key information K are read out of the lead-out area LOUT2 (step S3). The reproduced contents data is decrypted by using the key information K and the copy or reproduction is restricted by using the copyright management information R (step S4).

Fig. 6 schematically shows the data which is recorded onto the disc in the radial direction of the disc. In this example, in the disc on which the recording area AR1 on the inner rim side and the recording area AR2 on the outer rim side are provided, in case of encrypting the contents data in the recording area AR2 on the outer rim side, as shown in Fig. 6A, copyright management information R2 and key information K2 are recorded into the lead-out area LOUT2 existing in the outer rim of the recording area AR2.

As shown in Fig. 6B, the copyright management

information R2 and the key information K2 can be also recorded into the lead-in area LIN2. The lead-in area LIN2 is used as an area for recording the TOC and, further, there is a possibility that it is used for recording other various kinds of information. However, since each of the copyright management information R2 and the key information K2 has a capacity of at most about 256 kbits, they can be sufficiently recorded into the lead-in area LIN2. If the copyright management information R2 and the key information K2 are recorded into the lead-in area LIN2, there is no need to access the lead-out area LOUT2 and there is an advantage such that an accessing speed can be improved.

Further, as shown in Fig. 6C, the copyright management information R2 and the key information K2 can be also recorded into both of the lead-in area LIN2 and lead-out area LIN2.

Further, as shown in Fig. 6D, for example, it is also possible to construct in a manner such that the copyright management information R2 and the key information K2 of 256 kbits are divided into two copyright management information R2a and R2b and two key information K2a and K2b, the copyright management information R2a and the key information K2a are recorded into the lead-in area LIN2, and the copyright management information R2b and the key information K2b are recorded into the lead-out area LOU2, respectively. It is also possible to separately record the copyright management information R2 and the key information K2 into the lead-in

area LIN2 and lead-out area LOU2, respectively.

In the above description, on the other hand, the contents data is encrypted and recorded into only the area AR2 in the outer rim between the two areas AR1 and AR2 on the disc. However, a case of encrypting and recording the contents data into both of the two areas AR1 and AR2 is presumed.

In such a case, as shown in Fig. 7A, copyright management information R1 and key information K1 for the contents data in the area AR1 are recorded into the lead-out area LOUT1. The copyright management information R2 and the key information K2 for the contents data in the area AR2 are recorded into the lead-out area LOUT2.

As shown in Fig. 7B, it is also possible to record the copyright management information R1 and the key information K1 for the contents data in the area AR1 into the lead-in area LIN1 and record the copyright management information R2 and the key information K2 for the contents data in the area AR2 into the lead-in area LIN2, respectively.

Further, as shown in Fig. 7C, it is also possible to record the copyright management information R1 and the key information K1 for the contents data in the area AR1 into both of the lead-in area LIN1 and the lead-out area LOUT1 and record the copyright management information R2 and the key information K2 for the area AR2 into both of the lead-in area LIN2 and the lead-out area LOUT2, respectively.

Further, as shown in Fig. 7D, for example, it is also possible to construct in a manner such that the copyright management information R1 and the key information K1 for the contents data in the area AR1 are divided into two copyright management information R1a and R1b and two key information K1a and K1b, they are recorded into the lead-in area LIN1 and lead-out area LOUT1, the copyright management information R2 and the key information K2 for the area AR2 are divided into the two copyright management information R2a and R2b and the two key information K2a and K2b, and they are recorded into the lead-in area LIN2 and lead-out area LOUT2, respectively. It is also possible to separately record the copyright management information R1 and the key information K1 and record the copyright management information R2 and the key information K2, respectively.

Further, although the above example has been described with respect to the case of recording the data onto the disc in which the recording area has been divided into two areas like CD2, the invention can be also applied to a case of further dividing the recording area into a plurality of areas. The invention can be also applied to a case of recording the data onto a disc in which the recording area is not divided like an ordinary CD or a double density CD as shown in Fig. 8.

In case of a disc having one recording area, as shown in Fig. 9A, the copyright management information R and the key information K for the contents data in the area

AR are recorded into the lead-out area LOUT.

As shown in Fig. 9B, the copyright management information R and the key information K for the contents data in the area AR can be also recorded into the lead-in area LIN.

Further, as shown in Fig. 9C, the copyright management information R and the key information K for the contents data in the area AR can be also recorded into both of the lead-in area LIN and lead-out area LOUT.

Further, as shown in Fig. 9D, the copyright management information R and the key information K for the contents data in the area AR can be also divided into two Ra and Rb and two Ka and Kb and recorded into the lead-in area LIN and lead-out area LOUT, respectively. It is also possible to separately record the copyright management information R and the key information K into the lead-in area LIN and lead-out area LOU, respectively.

According to the invention, when the encryption data is recorded into the data area of the memory medium having the data area, lead-in area, and lead-out area, the copyright management information and the key information for the encryption data are recorded into the lead-out area.

In case of the memory medium having a plurality of data areas, a plurality of lead-in areas, and a plurality of lead-out areas like CD2, when the encryption data is recorded into the data area, the copyright management information and the key information corresponding to the

encryption data are recorded into one of the plurality of lead-in areas or one of the plurality of lead-out areas.

In the present situation, only information in the Q channel of the subcode has been recorded in the lead-out area and this area is filled with dummy data. The position of the lead-out is obtained from the information of the TOC. The fact that the light spot has entered the lead-out area can be judged from the information in the Q channel. The copyright management information and the key information are recorded by using such a lead-out area. The lead-out area is not rewritten or accessed by the ordinary CD player, so that the copyright management information and the key information can be safely held.

## Industrial Applicability

The invention is suitable for use in a case where when contents data is recorded/reproduced to/from the disc like CD2, the data is encrypted in order to protect the contents data.

CLAIMS

1. A recording apparatus comprising:

input means for inputting encryption data; and

recording means for recording said encryption data which is inputted into a data area on a memory medium having the data area, a lead-in area, and a lead-out area and recording additional information corresponding to said encryption data into said lead-out area.

2. A recording apparatus according to claim 1, wherein

said recording means records the additional information as copyright management information for restricting reproduction/copy of said encryption data into said lead-out area.

3. A recording apparatus according to claim 1, wherein

said recording means records the additional information as a decrypting key for decrypting said encryption data into said lead-out area.

4. A recording apparatus according to claim 1, wherein

as said additional information, said recording means records a version number of a decrypting key for decrypting said encryption data, the number of said decrypting keys, the decrypting keys of the number as many as said decrypting keys, the number of copyright management

information for restricting reproduction/copy of said encryption data, the copyright management information of the number as many as said copyright management information, and a CRC code.

5. A recording apparatus comprising:

input means for inputting encryption data; and recording means for recording said encryption data which is inputted into data areas on a memory medium having the plurality of data areas, a plurality of lead-in areas, and a plurality of lead-out areas and recording additional information corresponding to said encryption data into one of said plurality of lead-in areas or one of said plurality of lead-out areas.

6. A recording apparatus according to claim 5, wherein

said memory medium has a first data area and a second data area on the inner rim side and, further, has a first lead-in area on the inner rim side of said first data area, a first lead-out area on the outer rim side of said first data area, a second lead-in area on the inner rim side of said second data area, and a second lead-out area on the outer rim side of said second data area, and

said recording means records said encryption data into said second data area and records said additional information into at least one of said second lead-in area and said second lead-out area.

7. A recording apparatus according to claim 6,

wherein

said recording means records the additional information as copyright management information for restricting reproduction/copy of said encryption data into at least one of said second lead-in area and said second lead-out area.

8. A recording apparatus according to claim 7, wherein

said recording means records the additional information as a decrypting key for decrypting said encryption data into at least one of said second lead-in area and said second lead-out area.

9. A recording apparatus according to claim 8, wherein

said recording means records said copyright management information and said decrypting key into said second lead-out area.

10. A recording apparatus according to claim 8, wherein

said recording means records said copyright management information and said decrypting key into said second lead-out area.

11. A recording apparatus according to claim 8, wherein

said recording means records said copyright management information and said decrypting key into each of said second lead-in area and said second lead-out area.

12. A recording apparatus according to claim 8, wherein

said recording means records a part of said copyright management information and said decrypting key into said second lead-in area and records the other part into said second lead-out area.

13. A recording apparatus according to claim 12, wherein

said recording means records one of said copyright management information and said decrypting key into said second lead-in area and records the other into said second lead-out area.

14. A recording apparatus according to claim 8, wherein

said recording means records said encryption data into said first data area and records said additional information into at least one of said first lead-in area and said first lead-out area.

15. A recording apparatus according to claim 14, wherein

said recording means records said copyright management information and said decrypting key into said first lead-out area.

16. A recording apparatus according to claim 14, wherein

said recording means records said copyright management information and said decrypting key into said

first lead-out area.

17. A recording apparatus according to claim 14, wherein

said recording means records said copyright management information and said decrypting key into each of said first lead-in area and said first lead-out area.

18. A recording apparatus according to claim 14, wherein

said recording means records a part of said copyright management information and said decrypting key into said first lead-in area and records the other part into said first lead-out area.

19. A recording apparatus according to claim 18, wherein

said recording means records one of said copyright management information and said decrypting key into said first lead-in area and records the other into said first lead-out area.

20. A reproducing apparatus comprising:

reading means for reading out said stored encryption data from a data area on a memory medium having the data area, a lead-in area, and a lead-out area and reading out additional information stored in said lead-out area; and

reproducing means for reproducing said encryption data in accordance with said read-out additional information.

21. A reproducing apparatus according to claim 20, wherein

said reproducing means has reproduction restricting means for restricting reproduction/copy of said encryption data in accordance with copyright management information as said additional information.

22. A reproducing apparatus according to claim 20, wherein

said reproducing means further has decrypting means for decrypting said encryption data in accordance with a decrypting key for decrypting said encryption data as said additional information and reproduces said decrypted data.

23. A reproducing apparatus according to claim 20, wherein

as said additional information, said reproducing means reproduces a version number of a decrypting key for decrypting said encryption data, the number of said decrypting keys, the decrypting keys of the number as many as said decrypting keys, the number of copyright management information for restricting reproduction/copy of said encryption data, the copyright management information of the number as many as said copyright management information, and a CRC code.

24. A reproducing apparatus comprising:

reading means for reading out encryption data from one of a plurality of data areas on a memory medium having the plurality of data areas, a plurality of lead-in areas,

and a plurality of lead-out areas and reading out additional information corresponding to said encryption data from one of said plurality of lead-in areas or one of said plurality of lead-out areas; and

reproducing means for reproducing said encryption data in accordance with said read-out additional information.

25. A reproducing apparatus according to claim 24, wherein

said memory medium has a first data area and a second data area on the inner rim side and, further, has a first lead-in area on the inner rim side of said first data area, a first lead-out area on the outer rim side of said first data area, a second lead-in area on the inner rim side of said second data area, and a second lead-out area on the outer rim side of said second data area,

said reading means reads out said additional information from at least one of said second lead-in area and said second lead-out area, and

said reproducing means reproduces said encryption data which is recorded in said second data area in accordance with said additional information.

26. A reproducing apparatus according to claim 25, wherein

said reading means reads out the additional information as copyright management information for restricting reproduction/copy of said encryption data from

at least one of said second lead-in area and said second lead-out area.

27. A reproducing apparatus according to claim 26, wherein

said reading means reads out the additional information as a decrypting key for decrypting said encryption data from at least one of said second lead-in area and said second lead-out area.

28. A reproducing apparatus according to claim 27, wherein

said reading means reads out said copyright management information and said decrypting key from said second lead-out area.

29. A reproducing apparatus according to claim 27, wherein

said reading means reads out said copyright management information and said decrypting key from said second lead-out area.

30. A reproducing apparatus according to claim 27, wherein

said reading means reads out said copyright management information and said decrypting key from each of said second lead-in area and said second lead-out area.

31. A reproducing apparatus according to claim 27, wherein

said reading means reads out a part of said copyright management information and said decrypting key

from each of said second lead-in area and reads out the other part from said second lead-out area.

32. A reproducing apparatus according to claim 31, wherein

said reading means reads out one of said copyright management information and said decrypting key from said second lead-in area and reads out the other from said second lead-out area.

33. A reproducing apparatus according to claim 27, wherein

said reading means reads out said additional information from at least one of said first lead-in area and said first lead-out area, and

said reproducing means reproduces said encryption data which is recorded into said first data area in accordance with said additional information.

34. A reproducing apparatus according to claim 33, wherein

said reading means reads out said copyright management information and said decrypting key from said first lead-out area.

35. A reproducing apparatus according to claim 33, wherein

said reading means reads out said copyright management information and said decrypting key from said first lead-out area.

36. A reproducing apparatus according to claim 33,

wherein

said reading means reads out said copyright management information and said decrypting key from each of said first lead-in area and said first lead-out area.

37. A reproducing apparatus according to claim 33, wherein

said reading means reads out a part of said copyright management information and said decrypting key from said first lead-in area and reads out the other part from said first lead-out area.

38. A reproducing apparatus according to claim 37, wherein

said reading means reads out one of said copyright management information and said decrypting key from said first lead-in area and reads out the other from said first lead-out area.

39. A recording method comprising the steps of:

inputting encryption data;

recording said encryption data which is inputted into a data area on a memory medium having the data area, a lead-in area, and a lead-out area; and

recording additional information corresponding to said encryption data into said lead-out area.

40. A recording method comprising the steps of:

inputting encryption data;

recording said encryption data which is inputted into data areas on a memory medium having the plurality of

data areas, a plurality of lead-in areas, and a plurality of lead-out areas; and

recording additional information corresponding to said encryption data into one of said plurality of lead-in areas or one of said plurality of lead-out areas.

41. A reproducing method comprising the steps of:

reading out said stored encryption data from a data area on a memory medium having the data area, a lead-in area, and a lead-out area;

reading out additional information stored in said lead-out area; and

reproducing said encryption data in accordance with said read-out additional information.

42. A reproducing method according to claim 41, wherein

reproduction of said encryption data is restricted in accordance with said read-out additional information.

43. A reproducing method according to claim 41, wherein

said encryption data is decrypted in accordance with said read-out additional information, and

said decrypted data is reproduced.

44. A reproducing method comprising the steps of:

reading out encryption data from one of a plurality of data areas on a memory medium having the plurality of data areas, a plurality of lead-in areas, and a plurality

of lead-out areas;

reading out additional information corresponding to said encryption data from one of said plurality of lead-in areas or one of said plurality of lead-out areas; and

reproducing said encryption data in accordance with said read-out additional information.

45. A reproducing method according to claim 44, wherein

reproduction of said encryption data is restricted in accordance with said read-out additional information.

46. A reproducing method according to claim 44, wherein

said encryption data is decrypted in accordance with said read-out additional information, and

said decrypted data is reproduced.

47. A memory medium

which has a data area, a lead-in area, and a lead-out area and

in which encryption data is recorded into said data area and

additional information corresponding to said encryption data is recorded into said lead-out area.

48. A memory medium according to claim 47, wherein

said additional information is copyright management information for restricting reproduction/copy of said encryption data.

49. A memory medium according to claim 47, wherein as said additional information, additional information as a decrypting key for decrypting said encryption data is recorded into said lead-out area.

50. A memory medium which has a plurality of data areas, a plurality of lead-in areas, and a plurality of lead-out areas and in which said encryption data which is inputted into said data areas is recorded and additional information corresponding to said encryption data is recorded into one of said plurality of lead-in areas or one of said plurality of lead-out areas.

51. A memory medium according to claim 50, wherein said additional information is copyright management information for restricting reproduction/copy of said encryption data.

52. A memory medium according to claim 50, wherein as said additional information, additional information as a decrypting key for decrypting said encryption data is recorded into said lead-out area.