G00002

Magnetic disk medium and a fixed magnetic disk drive unit

159159

Technical field of the invention

The present invention relates to a magnetic disk medium and a fixed magnetic disk drive unit that reads and writes digital information by a magnetic head. In particular, the present invention relates to a magnetic disk medium and a fixed magnetic disk drive unit that are given a security function by embedding identification information in the magnetic disk medium.

Background of the invention

A fixed magnetic disk drive unit reads and writes signals while a magnetic head is flying on a magnetic disk rotating at a high speed keeping a gap in an order of submicron. A conventional magnetic disk used in a fixed magnetic disk drive unit has been manufactured by laminating a magnetic layer and a protective layer on a flat substrate of nonmagnetic material, for example, aluminum or glass. In recent years, some of the fixed magnetic disk drive units use a pre-embossed type magnetic disk that records preformatted information such as servo information in the uneven patterns formed on the substrate.

Nikkei Electronics No. 586 (1993.7.19) discloses a fixed magnetic disk drive unit using a pre-embossed medium that carries servo

patterns and recording tracks formed with uneven patterns on a glass substrate. In the servo pattern of the medium, protrusions and dents of the uneven pattern are magnetized in the opposite direction along the track line. A signal pattern of 1/0 is readout by detecting leakage magnetic flux at a boundary of a protrusion and a dent by the magnetic head.

Servo information and recording tracks of the pre-embossed magnetic disk can be formed with high precision because the information and the tracks are manufactured by a method similar to the method in the optical disk production. The pre-embossed systems are expected to be applied to a ROM disk storing programs or data, as well as the application to the servo pattern. In these days, image data, sound data, and various software data (hereinafter, these data are also called "contents") are distributed through networks, such as the internet. Fixed magnetic disk drive units or memory cards are used for temporarily storing the data of these contents that are bought and downloaded.

With increase in the distributing quantity of the digital contents, digital copyright management systems have been introduced for protecting the contents. A digital copyright management system performs a certain operation on the contents bought by a customer and prevents transferring a copy of the contents to a third party and

avoids uploading and delivering to the internet.

Some digital copyright management system provides a scheme that generates a key based on hardware information of the client's PC that playbacks the contents, and that does not permit playback without the key. An example of such a system working jointly with a smart card (a memory card capable of intelligent functions) uses hardware ID information that is embedded in the smart card and unique to the card. This ID information is embedded in an unmanipulatable condition, which brings about high security.

Problem to be solved by the invention

No example of a fixed magnetic disk drive unit exists that has such ID information embedded in the medium. One of the reasons is because the structure of the fixed magnetic disk drive unit allows rather easily rewriting the internal data. Embedding the ID information using a magnetic head by software can hardly prevent manipulating the ID information for a purpose of unfair use.

To solve the problem, a method could be considered, in which the ID information is physically embedded as the above-mentioned pre-embossed type magnetic disk. However, the pre-embossed type magnetic disk formed by a stamper has a problem in that the magnetic disks formed by the same stamper have the same ID

information. That is, uniqueness of ID information can not be obtained. In view of the above, an object of the present invention is to provide a magnetic disk medium that can be embedded with hardly manipulatable and unique ID information. Another object of the invention is to provide a fixed magnetic disk drive unit presenting security by application of such a magnetic disk medium.

Means to solve the problem

To attain the first object, a magnetic disk medium according to the present invention is a magnetic disk medium of a pre-embossed type comprising a recording region having a preformatted region with uneven surface structure, and a non-preformatted region with evenly protruding or evenly recessed surface structure, wherein ID information for uniquely identifying the magnetic disk medium is recorded in the recording region, and the ID information includes a first ID information stored in the preformatted region and a second ID information stored in the non-preformatted region.

The ID information including the first ID information stored in the preformatted region and the second ID information stored in the non-preformatted region are hardly manipulated and yet have uniqueness.

Advantageously, recessed portions of the uneven surface

structure to form the first ID information in the preformatted region is so deep that inversion of magnetization direction is impossible by a magnetic field generated by a gap of a recording head of a fixed magnetic disk drive unit that contains the magnetic disk medium. By this constitution, at least dents cannot be rewritten by the head of the fixed magnetic disk drive unit, and an unfair user hardly change the master ID information to his convenient one.

Advantageously, a pair of the first ID information and the second ID information is recorded on each recording surface of the magnetic disk medium and each pair of the information has different ID information. Since a plurality of ID information can be used, security management becomes more flexible and the magnetic disk medium becomes more useful.

Advantageously, each of the first ID information and the second ID information is information that is encrypted in terms of a prescribed cryptosystem. The encryption prevents the ID information from leaking out by decomposition of the fixed magnetic disk drive unit. Advantageously, each of the first ID information and the second ID information includes a body of ID information that is identifying information and digital signature information for the body of ID information. Because the digital signature information detects unfair manipulation of the ID information, the ID information becomes more

reliable.

To attain the second object mentioned earlier, a fixed magnetic disk drive unit according to the present invention, mounting one or more magnetic disk media of the invention, comprises a readout means for reading out the first ID information and the second ID information on the magnetic disk medium, a decryption means for decrypting the first ID information and the second ID information, a verification means for verifying the first ID information and the second ID information based on digital signature information, and a transfer means for transferring the first ID information and the second ID information to a host apparatus.

Brief description of drawings

Fig. 1(a) illustrates a principle of primary magnetization of an embodiment of a magnetic disk according to the present invention.

Fig. 1(b) illustrates a principle of secondary magnetization of an embodiment of a magnetic disk according to the present invention.

Fig. 2 is a plan view of an embodiment of a magnetic disk according to the present invention.

Fig. 3 is another plan view of an embodiment of a magnetic disk according to the present invention.

Fig. 4 illustrates a method for manufacturing an embodiment of a magnetic disk according to the present invention.

Fig. 5 is an illustration showing a structure of an embodiment of a fixed magnetic disk drive unit according to the present invention.

Fig. 6 illustrates details of a recording plane of an embodiment of a magnetic disk according to the present invention.

Fig. 7 is a diagram showing a structure of a working apparatus for producing a stamper that is used for manufacturing a magnetic disk according to the present invention.

Fig. 8 shows a construction of a control system of an embodiment of a fixed magnetic disk drive unit according to the present invention.

Fig. 9 shows a construction of an apparatus for writing individual medium ID information in a magnetic disk according to the present invention.

Fig. 10 is a flowchart showing a procedure for readout ID information stored in a magnetic disk in an embodiment of a fixed magnetic disk drive unit according to the present invention.

Fig. 11 shows contents of a key table stored in an embodiment of a fixed magnetic disk drive unit according to the present invention.

Aspects of embodiments of the present invention

Some aspects of preferred embodiments of the present invention will be described in detail with reference to the accompanying drawings in the following. Fig. 5 is an illustration of structure of a fixed magnetic disk drive unit of a preferred embodiment of the present invention. The fixed magnetic disk drive unit comprises an

arm 15 supporting a magnetic head 14, a comb-shape carriage 16 fastening the arm 15, a voice-coil motor 17 for driving the carriage, and a magnetic disk 1, which are all mounted on a housing 11. A plurality of stacked magnetic disks is fastened to a spindle 12. The spindle 12 is rotated at a constant angular velocity by a not illustrated spindle motor installed under the housing 11. The carriage 16 is oscillated about a shaft 13 by the voice-coil motor 17. The magnetic head 14 is attached to the tip of the arm 15 and opposes to the disk surface. The magnetic head slides flying on the rotating disk following the movement of the carriage 16.

Fig. 2 is a plan view of a magnetic disk of an embodiment of a magnetic disk medium according to the present invention. The magnetic disk 1 is a pre-embossed type magnetic disk, in which a part of recorded information is formed with uneven surface structure having protrusions and dents. A magnetic film and a protective layer are laminated on a substrate made of plastics, for example. A recording plane of the magnetic disk comprises radially extending servo zones 2 storing control information and concentric tracks for recording data.

Fig. 6 is an illustration showing details of the recording plane of the magnetic disk 1. In the figure, the dotted area is protruding portion; the unpatterned or blank area is recessed portion; and other

area is uneven portion containing small protrusions and dents. The servo zone 2 contains control information formed with uneven pattern; the information including track ID for specifying a track position, lattice patterns 23 for detecting displacement of the head from the track center, and other control information.

The tracks are arranged with interruption by the servo zone 2. Guard bands 28 are formed by grooves between the tracks for avoiding interference from adjacent tracks. There are two types of tracks. One type of track is a protruded region, for example, track 27, and is not preformatted (capable of reading / writing data). Another type of track is an uneven region composed of small protrusions and dents, the track 29 in Fig. 6, and is preformatted (capable of reading only).

Both preformatted and non-preformatted tracks are logically formatted. That is, the tracks are divided into sectors, which are a basic unit of read / write. Each sector consists of a body of the data, header information, and a redundant byte for error correction. The header information includes address information of the sector and synchronization information for generating a clock synchronized with the data. The body of the data is transformed into a code with limited succession of zeros (for example, 2-7RLL code).

The magnetic disk 1 can be manufactured by a method for manufacturing an optical disk. Fig. 4 shows the process of the method. A glass disk 90 is polished and finished to a flawless and flat surface condition. A photosensitive agent (resist) 91 is applied on the disk. Then, laser light is irradiated by a laser cutting apparatus intermittently corresponding to the pattern to be recorded. By developing, the laser irradiated portion dissolves and dents are generated on the surface according to the pattern. The surface is then nickel-plated to a certain thickness to obtain a stamper 94. A substrate 95 is formed by injection-molding resin material using the stamper 94 as a mold. Finally, a magnetic layer and a protective layer are laminated on the surface of the substrate 95 by a sputtering method, for example, and a magnetic disk is completed.

Signal pattern becomes detectable by a magnetic head after conducting magnetization on the magnetic disk. Magnetization is first conducted in one direction on both protrusions and dents using a magnetic head generating a strong magnetic field, as shown in Fig. 1(a) (primary magnetization). Then, secondary magnetization is conducted in the direction opposite to the first magnetization using a magnetic head generating an appropriate magnetic field weaker than in the primary magnetization, as shown in Fig. 1(b). Because the second magnetization does not invert the magnetization direction at the dents, transition of magnetization arises at the boundary between

a protrusion and a dent.

While the magnetic head relatively moves through the uneven portion flying over the disk, a voltage signal arises at the magnetization transition position with a positive or negative peak corresponding to the direction of the transition of magnetization. A signal pattern can be read out by amplifying the voltage signals and detecting peaks. A recording plane of the magnetic disk of the invention stores two type of ID information, master ID information 3 and individual medium ID information 4, on the respective track as shown in Fig. 3. This allows unique identification of a medium.

The master ID information 3, already embedded in the stamper, is transferred to the magnetic disk from the stamper as a pattern of protrusions and dents in the molding step. Accordingly, magnetic disks molded using the same stamper have the same master ID information. The master ID information 3 contains a master ID to uniquely identity a stamper. The master ID can use a serial number of the stamper, for example. When front and back recording planes of a magnetic disk are formed using two stampers embedded with different master ID information, then different recording planes have different ID information.

The master ID information 3 is embedded as an uneven pattern

in the stamper preferably through encryption. The encryption more hinders analysis by disassembling the fixed magnetic disk drive unit. Here, a cryptosystem is not limited to a special one. The master ID information 3 desirably includes digital signature information for the master ID. The digital signature can examine whether the master ID is created by a regular manufacture or not, and whether the master ID has been manipulated or not.

The digital signature can be produced by transforming the master ID to a fixed length data (hash code) by a hash function, and then encrypting the hash code using a secret key in a public key cryptosystem. To examine this digital signature, first the master ID and the digital signature are read out of the magnetic disk, and the digital signature is decrypted using a public key that pairs with the above-mentioned secret key to obtain a hash code. Comparing this hash code with a hash code obtained from the master ID by a hash function, judgment is made on coincidence of the two. If the coincidence is confirmed, the master ID may be presumed to be created by a regular manufacturer, and not manipulated.

The master ID information is embedded in an uneven and preformatted track (read only track 29) in Fig. 6. This read only track 29 may locate at any track position in the magnetic disk 1. In the uneven structure with protrusions and dents on the read only

track 29, the dent is preferably so deep that the recording field generated at the gap by the recording head of the fixed magnetic disk drive unit cannot reach the bottom of the dent. The optimum depth of the dent varies depending on characteristics of the head and flying gap length. Consequently, the optimum depth of the dent is selected according to the hardware specification of the fixed magnetic disk drive unit.

Fig. 7 is a diagram showing the structure of a working apparatus 31 used in a process for manufacturing a stamper embedding a master ID. This apparatus is used for writing a pattern corresponding to protrusions and dents on a surface of a glass substrate coated with resist. Operation of this working apparatus will be described below.

A master ID generator 32 generates a unique ID number, say 10572972. An encryptor 33 encrypts the ID number using a common key 96 that is input from outside. A hash function operator 34 transforms the encrypted master ID into a fixed length hash code with 128 bytes, for example, by a prescribed hash function operation. An encryptor 35 encrypts this hash code using a secret key 97 input from outside, to generate a digital signature 36.

The encrypted master ID 37 and the digital signature 36 are

combined and input to a format transformer 38. The format transformer 38 transforms the input data with a byte format to a serial bit string, and executes format transformation according to a logical format of the track, and further conducts transformation to a prescribed code. The mapping operator 39 executes mapping of the output data from the format transformer 38 in a two dimensional region according to the track position to which master ID information is recorded. Consequently, information for a pattern of protrusions and dents are generated corresponding to the master ID information.

A laser cutting apparatus 40 receives a master data 41 storing information of uneven patterns for servo zones and recording tracks, and uneven pattern information 39a generated by a mapping operator 39. While rotating a glass substrate 90 having a surface coated with photosensitive material, the laser 42 is shot on and off based on this information. After developing the glass substrate 90, the resulted uneven surface with protrusions and dents is nickel-plated, to complete a stamper.

The master ID information is hardly changed to different information by a magnetic head as described above. That means outstanding tamper resistant ability of the magnetic disk. On the other hand, there is a drawback that uniqueness cannot be held because the magnetic disks manufactured using the same stamper

have the same ID information. To make up for this drawback, a magnetic disk of the invention uses individual medium ID information as second ID information. The individual medium ID information contains ID number that uniquely identifies a magnetic disk.

Different individual medium ID information can be recorded on front and back recording planes of a magnetic disk. Since a sheet of magnetic disk can use a plurality of ID information, security management can be made more flexible. Like master ID information, this individual medium ID information is also preferably encrypted at the time of writing in a magnetic disk. A cryptosystem in this case is also not limited to any special one. The individual medium ID information, like master ID information, favorably contains digital signature information.

The individual medium ID information is recorded by a magnetic head on one of the tracks excepting the read only track 29 in Fig. 6, that is, on a non-preformatted track (track 27 etc.). Track position is not specially limited. The step for recording this individual medium ID information in the manufacturing process is conducted after completion of assembling the fixed magnetic disk drive unit.

Fig. 9 shows a construction of an apparatus for writing individual

medium ID information on a magnetic disk 1 installed in a fixed magnetic disk drive unit. In writing on the magnetic disk, the fixed magnetic disk drive unit 5 is connected to an ID writing apparatus 70 with a bus 62, as shown in Fig. 9. In the ID writing apparatus 70, ID number 71a that is unique to the medium is generated by an individual medium ID generator 71 and encrypted by an encryptor 72 to produce encrypted data 79. Digital signature 78 of the individual medium ID is generated by a hash function operator 73 and encryptor 74. Write data 82 is produced by adding the encrypted ID data and the digital signature. The write data 82 together with a track number and a head number 77 is sent to the fixed magnetic disk drive unit 5 as a write instruction, and individual medium ID information 4 is written on a specified track and in a specified recording plane of the magnetic disk 1.

Fig. 8 shows a construction of a control system 50 of the fixed magnetic disk drive unit of an embodiment according to the present invention. A head amplifier 51 of the control system 50 comprises a read amplifier for amplifying head readout signal (not shown), a driver circuit for switching recording current of the magnetic head 14 (not shown), and a head selection circuit (not shown). Output signals from the head amplifier 51 is lead to readout controller 53, in which the data is reproduced. The readout controller 53 comprises a peak detection circuit 53a for detecting peaks of readout signals, and a

demodulation circuit 53b for decrypting channel-coded data. A format controller 56 performs format transformation of read/write data based on a prescribed sector format, verification of readout data by error correction code, and correction of occurred errors. A buffer memory 63 is a temporary storage memory for read/write data.

The fixed magnetic disk drive unit connects to a host system 61 (PC, for example,) through a bus 62. CPU 58 analyses commands sent from the host system 61 and processes each command.

ROM 58a is a read only memory storing firmware of this disk drive unit. ROM 58a further stores a key table 101 keeping several key data that are necessary on reading out ID information. Fig. 11 shows the contents of the key table 101. A common key 101a for master ID is the same key as the common key 96 that is input to the encryptor 33 in the working apparatus 31 for manufacturing a stamper shown in Fig. 7. A public key 101b for master ID is a public key pairing with the secret key 97 that is input to the encryptor 35. A common key 101c for individual medium ID is the same key as the common key 98 that is input to the encryptor 72 in the ID writing apparatus 70 in Fig. 9. A public key 101d for individual medium ID is a public key pairing with the secret key 99 that is input to the encryptor 74.

Fig. 10 is a flowchart showing a procedure for readout ID information stored in the magnetic disk in the fixed magnetic disk drive unit. Here, the fixed magnetic disk drive unit 5 is assumed in a state where initialization process after power turn on is completed and the unit is waiting for a command from a host apparatus 61. The procedure for reading ID information will be described according to this flowchart and referring to Fig. 8, Fig. 11 etc.

When a command to readout ID information of a specified head number is sent from a host apparatus 61 through the bus 62, the CPU 58 issues a command to the positioning controller 54 for the head 14 to seek for the read only track that stores the master ID information, in the step S1.

In the step S2, the CPU 58 gives the head amplifier 51 a command to select the head designated by the host apparatus 61 out of a plurality of heads. Readout signals from the recording plane of the appropriate head are amplified by the head amplifier 51 and the output from the amplifier is lead through a peak detection circuit 53a to a demodulation circuit 53b, and the data from the read only track are readout from the demodulation circuit 53b as a NRZ (non-return-to-zero) data string.

In the step S3, the CPU 58 gives the format controller 56 a

command to readout master ID information. According to the command, the NRZ data string is input to the format controller 56, where only the data in the sector storing the master ID information is extracted. The format controller 56 further executes error detection of the sector data and error correction, if necessary. After that, the sector data is stored in the buffer memory 63 through the transfer control circuit 57.

In the step S4, the CPU 58 first accesses the buffer memory 63 and decrypts the digital signature data in the sector data using a public key 101b for master ID stored in the key table 101. Then, the CPU 58 computes a hash code of the master ID data in the sector data by a prescribed hash function. The prescribed hash function here is the same as the function applied in the hash function operator 34 in the working apparatus for producing a stamper in Fig. 7.

In the step S5, the CPU 58 compares the hash code computed from the master ID with the digital signature code decrypted in the preceding step. If the two codes are not identical, the medium is judged to have some abnormality, and the occurrence of abnormality is notified to the host apparatus (S14). The processing is suspended and returns to a state waiting for a command (S13).

If coincidence is verified, the processing proceeds to the next step

S6. In the step S6, the CPU 58 decrypts the encrypted master ID using the common key 101a for master ID, to obtain a master ID (16 bits) in a clear text.

In the next step S7, the CPU 58 let the magnetic head 14 seek for the track storing the individual medium ID information.

In the next step S8, the ID information recorded on this track is readout and the sector data including individual medium ID information is written in to the buffer memory 63.

In the next step S9, the CPU 58 first decrypts the digital signature data in the sector data using the public key 101d for individual medium ID. Then, the CPU 58 computes a hash code of the individual medium ID data in the sector data by a prescribed hash function. The prescribed hash function here is the same as the function applied in the hash function operator 73 in the ID writing apparatus in Fig. 9.

In the next step S10, the CPU 58 compares the hash code computed from the individual medium ID with the digital signature code decrypted in the preceding step. If the two codes are not identical, the medium is judged to have some abnormality, and the occurrence of abnormality is notified to the host apparatus in the step

S14. The processing is suspended and returns to a state waiting for a command.

If coincidence is verified, the processing proceeds to the next step S11. In the step S11, the CPU 58 decrypts the encrypted individual medium ID using the common key 101c for individual medium ID, to obtain an individual medium ID (32 bits) in a clear text. Finally, in the step 12, the CPU 58 combines the master ID (16 bits) and the individual medium ID (32 bits) to produce an ID with 48 bits, which is sent to the host apparatus 61 through the bus 62. Then, the procedure returns to a state waiting for a command from the host apparatus 61 in the step 13.

After that, the host apparatus 61 sends a command to readout ID to another head in the similar manner, if necessary. Based on the obtained ID for each head, encryption key etc. is generated.

Advantageous Effect of the invention

As described so far, in a magnetic disk medium according to the present invention, ID information for uniquely identifying a medium is recorded separately in a preformatted region and non-preformatted region of a pre-embossed magnetic disk. Consequently, the present invention provides a magnetic disk medium that inhibits manipulation and yet holds unique ID information.

A fixed magnetic disk drive unit according to the present invention comprises one or more such magnetic disk media and can read ID information out of the magnetic disk media and send the information to a host apparatus. Consequently, a fixed magnetic disk drive unit of the invention can be applied to a wide variety of security systems.

Claims

1. A magnetic disk medium of a pre-embossed type comprising a recording region having a preformatted region with uneven surface structure, and a non-preformatted region with evenly protruding or evenly recessed surface structure, wherein ID information for uniquely identifying the magnetic disk medium is recorded in the recording region, and the ID information includes first ID information stored in the preformatted region and second ID information stored in the non-preformatted region.

2. A magnetic disk medium according to claim 1, wherein recessed portions of the uneven surface structure to form the first ID information in the preformatted region have so deep that inversion of magnetization direction is impossible by a magnetic field generated by a gap of a recording head of a fixed magnetic disk drive unit that contains the magnetic disk medium.

3. A magnetic disk medium according to claim 1, wherein a pair of the first ID information and the second ID information is recorded on each recording surface of the magnetic disk medium and each pair has different ID information.

4. A magnetic disk medium according to claim 1, wherein each of the first ID information and the second ID information is information that is encrypted in terms of a prescribed cryptosystem.

5. A magnetic disk medium according to claim 1, wherein each of the first ID information and the second ID information includes a

body of ID information that is identifying information and digital signature information for the body of ID information.

6. A fixed magnetic disk drive unit mounting one or more magnetic disk media that are defined by claim 1, the fixed magnetic disk drive unit comprising:

a readout means for reading out the first ID information and the second ID information on the magnetic disk medium,

a decryption means for decrypting the first ID information and the second ID information,

a verification means for verifying the first ID information and the second ID information based on digital signature information, and

a transfer means for transferring a pair of the first ID information and the second ID information to a host apparatus.