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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 July 2004 (08.07.2004)

PCT

(10) International Publication Number
WO 2004/057580 A2

(51) International Patent Classification[7]: G11B

(21) International Application Number:
PCT/US2003/040479

(22) International Filing Date:
17 December 2003 (17.12.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/434,310 17 December 2002 (17.12.2002) US

(71) Applicants and
(72) Inventors: **DRISCOLL, William, J.** [US/US]; 5808 S. Dayton Street, Greenwood Village, CO 80111 (US). **STEVENSON, William, V.** [US/US]; 12515 Washington Lane, Apt. 29D2, Englewood, CO 80112 (US). **LARSEN, Chad, M.** [US/US]; 5377 S. Foresthill Street, Littleton, CO 80120 (US).

(74) Agents: **HENSON, Michael, R.** et al.; Timothy J. Martin, P.C., Suite 200, 9250 W. 5th Avenue, Lakewood, CO 80226 (US).

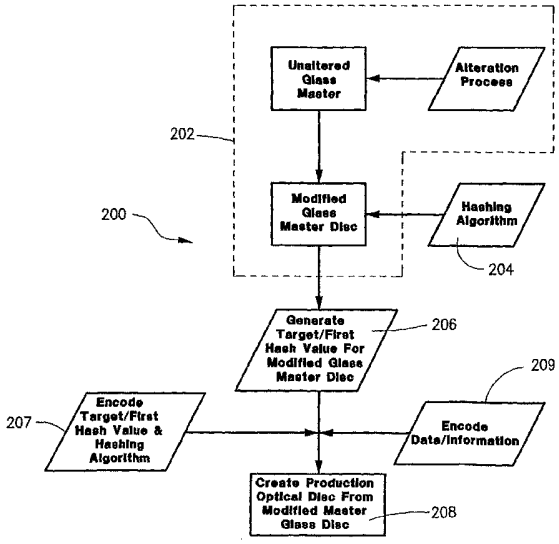
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH,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

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

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: COPY PROTECTED OPTICAL MEDIA STORAGE DEVICE, ALONG WITH METHODOLOGIES FOR MANUFACTURING AND AUTHENTICATING THE SAME



(57) **Abstract:** An optical media storage device comprises a substrate, a metallic reflective layer and a protective layer. The substrate includes an anomaly region configured to generate one or more errors when read by an optical reader, a fingerprint region corresponding to a target hash value obtained when the anomaly region is applied as an input to a hashing algorithm, and a program region corresponding to an executable application program incorporating the hashing algorithm. When the device is read by the optical reader, the hashing algorithm is executed against the anomaly region to generate a test hash value for comparison with the target hash value. Methods for manufacturing a copy protected optical media and for assessing authenticity of the same are also provided.

WO 2004/057580 A2

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.

COPY PROTECTED OPTICAL MEDIA STORAGE DEVICE, ALONG WITH METHODOLGIES FOR MANUFACTURING AND AUTHENTICATING THE SAME

FIELD OF THE INVENTION

The present invention broadly relates to preventing unauthorized access to information residing on a removable storage device, such as optical media. More particularly, the present invention concerns optical disc constructions and methodologies for assessing media authenticity and preventing unauthorized access to stored data in an effort to combat piracy.

BACKGROUND OF THE INVENTION

Removable storage has been around almost as long as the computer itself. Early removable storage was based on magnetic tape like that used by an audio cassette. Prior to that, some computers even used paper punch cards to store information. Technology has progressed exponentially since the days of punch cards. New removable storage devices can store hundreds of megabytes (and even gigabytes) of data on a single disc, cassette, tape or cartridge.

Two widely used types of removable storage technology are magnetic media and optical media. Although, certain types of magnetic media, such as cassette tapes and floppy discs, are rapidly being replaced and phase out by the ever-increasing advances in optical media, magnetic technology still enjoys immense popularity. This is based, in part, on the fact that magnetic tape can be erased and rewritten many times and have an advantage of low cost. As such, magnetic tape is still a highly desirable format for achieving data where rapid access is of less significance.

The optical storage devices most are familiar with are the compact discs (CD) and the digital video disc (DVD), each of which can store enormous amounts of digital information in a manner which is both efficient and inexpensive to manufacture. The compact disc system, itself, is perhaps one of the most remarkable developments in storage technology and embodies many revolutionary steps in design, such as digital signal storage, optical scanning, error correction, and new manufacturing processes. From its inception and development, the CD established a new fidelity standard for the consumer and, today, CD music playback is only one aspect of the many available CD applications. A compact disc system

contains several unique technologies. When combined, they form an unprecedented means of storage. A compact disc contains digitally encoded data that is read by a laser beam. The data encoded on the disc is actually the end product of a coding process accomplished prior to disc mastering, then decoded as the disc is played. Billions of channel bytes of data can be reliably stored on the disc due to EFM modulation and CIRC error correction techniques. Because the laser beam is focused on a reflective layer embedded within the disc, dust and fingerprints on the reading surface do not normally affect reproduction. Moreover, the effect of most errors that normally occur can be minimized by error correction circuitry. Thus, digital storage, error correction, and disc longevity result in a robust digital storage medium.

Figure 1 shows a cross-sectional view of a read-only optical media storage device, such as CD-ROM, which is constructed according to the prior art. Optical media 2 contains pre-recorded data that can be read by an interrogating beam, such as a laser beam in an optical reader. A transparent polycarbonate substrate layer 4, or similar material, permits optical transmission of the interrogating being therethrough. Polycarbonate layer 4 is fabricated with data stored as a surface structure (a "data structure"), as represented by pits 6 and lands 7. A metallic reflective layer 8, which may be aluminum, is disposed over substrate 4. Following metal deposition, a thin plastic protective layer 9 is spin-counted over the metallic layer and cured by ultraviolet radiation.

A conventional prior art technique for manufacturing read-only optical media is well understood in the art and can be summarized as follows. Fabrication of the optical media begins with pre-mastering of the data. A mastering tape is made which contains information to be written on the desk. From this mastering tape a "glass master" is formed. More particularly, a glass plate of appropriate size is lapped a flat and polished. The plate is coated with photoresist. The pre-mastering data from the mastering tape is used to record a laser beam recorder (LBR) which writes the appropriate pattern, coded on the mastering tape according to known specifications, into the photoresist.

The photoresist is developed. A layer of metal, typically silver over a nickel flash, is evaporated over the photoresist. The glass master is then checked for accuracy by playing the disc. The glass master is then subject to an electroforming process during which additional metal is deposited on the silver layer. When the

metal is of appropriate thickness, the metal layer is separated from the glass master. This results in a metal negative impression of the desk, referred to as "father".

The electroplating process is then repeated on the father to generate a plurality of negative impressions called “mothers”. Each mother disc can also be used as a template in another electroplating process to again make a plurality of negative metal impressions called “sons" or "stampers". The stampers are suitable as molds for injection molding. It is also possible to simply use the father disc directly has the stamper. The stamper is used in the injection molding step to create deformations (the “data structure”) representative of the pre-mastering data. Polycarbonate is used to injection mold the CD disc. Following a cool down period, the service of the polycarbonate substrate carrying the deformations is coated with a metallic layer that that has sufficient reflectivity to be optically acceptable, silver and aluminum being the most common metals. Following metal deposition, a thin plastic layer of a protective polymer, typically lacquer, is spin-coated over the metallic layer. The spin-coated layer(s) is cured in UV. Finally, a suitable logo or other information may be silk screened on the top to form a label.

While the CD-audio format (sometimes called CD-Digital-Audio, or CD-DA) was the initial format developed for optical storage mediums, that medium lends itself to other types of data not restricted to audio applications. For example, in CD-ROM computer software or other information can be stored in a read-only format and delivered as a data or video signal rather than an audio signal. The CD-R permits users to record their own data permanently on a disc, and the CD-RW format allows fully erasable recording. Other known formats include the CD-i format which is an interactive, multimedia format and the CD+G format which adds graphics and other types of data. While the interrelationships between these members of the CD family are somewhat complicated, these alternative CD formats demonstrate the remarkable range of applications open to the compact disc.

DVD is the successor to the CD and the technological improvements for this type of optical media provides unparalleled capacity and flexibility of data storage. While the CD was originally designed as an audio storage format and incrementally adapted to other applications, DVD was designed as a universal storage platform and has a much larger data storage capacity due, in part, to the composition of several data storage layers on discs that can be either single-sided or double-sided. As with the CD, various types of DVD formats also exist, including DVD-Rom (Read

Only), DVD-Video, DVD-Audio, DVD-R (Write-Once), DVD-RAM (Random Access Memory) and DVD-RW (Rewriteable). Although based on CD technology, DVD employs new physical specifications and a new file format.

While technological developments in the optical media industry are rapid and diverse, the industry has long been plagued by piracy in the form of illegal misappropriation of software products. Indeed, the misappropriation of software is rampant irrespective of whether the data storage medium is magnetic or optical. The International Planning and Research Corporation (IPR) recently completed an analysis of software piracy for the year 2000 as a part of an ongoing study for the business software alliance (BSA) and its member companies. The study's objective was to review the available data and utilize a systematic methodology to determine the worldwide business software piracy rates and the associated dollar losses. For the first time in the study's history, even with the onset of copy protection technology, the world piracy rate increased in two consecutive years, 2000 and 2001, and the dollar losses attributed to business applications alone was in excess of $10 billion. Numbers released from a leading software development company indicate that 40% of software products worldwide were pirated in 2001, an increase of 1% over 2000. Unless effective prevention techniques are implemented, the software piracy problem will continue to occur at an alarming rate.

Various types of copy protection techniques have been implemented which are both hardware-driven and software-driven, and even hybrids thereof, in an effort to combat both dedicated and casual piracy. An ideal system for combating piracy offers capabilities such as rights management, usage control, authentication, piracy deterrents and tracking. On the hardware side, for example, some manufacturers offer optical media players having de-encryption software for playing encrypted discs. For DVD-video copy protection, in particular, a content scrambling system (CSS) has been developed. Data encryption is used so that the content is self-protecting, but use of the technology is voluntary. Another type of hardware-based approach is described in U.S. Patent Application Publication No. US 2002/0067674 A1, published on June 6, 2002. This publication relates to a method and apparatus for authenticating an optical disc using purposefully induced errors to determine whether the disc has been legitimately manufactured or is an illegitimate copy.

On the software side, it is quite common for products to require validation keys or registration codes, input from a user or otherwise, in order to execute. While

such an interactive validation approach can be effective, there is a fine line between security and usability. As such, end-user resistance to these anti-piracy schemes has been high because they are plagued by one or more limitations, such as an inability to "try before you buy", restrictions on the generation of legitimate back-up copies, and password protection techniques which fail once the password has been divulged of otherwise discovered. Accordingly, the inability of existing copy protection schemes to win end-user acceptance has been so extreme that many publishers have simply abandoned the effort, choosing instead to rely on the integrity of their customers to abide by copyright laws.

Despite people's best efforts at preventing the unauthorized duplication of software, various circumvention techniques are widely available to equip both dedicated software pirates and computer novices with means of circumvention. One approach for circumventing copy protection techniques is known as "raw copying" whereby data is copied bit for bit off the media to another location and subsequently validated to determine if it can be used again. This is one brute force approach which has proven quite successful. Another approach is ISO duplication which is akin to raw copying, except the copied media is stored on another media disc. In the abstract, this is akin to hooking up two VCRs and copying tape to tape. While the different copy protection approaches entail varying levels of sophistication and robustness, they can almost all be circumvented given enough expertise and dedication by a software pirate. Once broken, the word spreads quickly and information soon becomes readily available whereby an end-user, either individually or through the use of third party assistance, is provided with the tools to obtain a pirated copy. While almost any security scheme has its vulnerabilities, it is necessary, particularly in the optical media industry, to develop copy protection schemes which are sufficiently ahead of the state of current circumvention techniques to thwart piracy by making it infeasible, impractical or simply too-time consuming for the technology to be broken.

It has been surprisingly found that these goals can be accomplished by employing existing, proven technology currently utilized for verifying data integrity in different types of message transport applications (such as secured e-mails, instant messaging and the like), as part of an optical media copy protection scheme. It is known, for example, to employ a hashing algorithm in such applications to transform information into a shorter, fixed-length value or key that represents the original string.

The term "hashing algorithm" refers to a function that takes as an input an arbitrary length message and outputs a fixed length string, commonly referred to as the "message digest", the "hashed value" or simply the "digest", that is characteristic of the message.

The hashing algorithm is called a hash function and in the past has been used to encrypt and decrypt digital signatures used to authenticate messages between senders and receivers. The digital signal is transformed with the hash algorithm and then both the message digest and the signature are sent in separate transmissions to the receiver. Using the same hash algorithm as the sender, the receiver derives a message-digest from the signature and compares it with the message-digest it also received. If they are the same, then the receiver knows that the integrity of underlying data's content has not been jeopardized.

The hash algorithm is used to index the original value or key and then used later each time the data associated with the value or key is to be retrieved. Thus, hashing is always one-way operation. The most important property of a hashing algorithm is its irreversibility because it should be extremely difficult, if not practically impossible, to compute a message given its digest. This is true even if the hash algorithm is known. A second important property is that it should be difficult to produce two messages such that they have the same message digest. This property is known as collision resistance.

There are several well-known hash functions which have been used in the past. These include the message-digest algorithms (MD-2, MD-4 and MD-5) used for hashing digital signatures into a shorter value called a message-digest, and the secure hash algorithm (SHA-1), a standard algorithm that makes a larger 60-bit message-digest and is similar to MD-4. In the MD-5 algorithm, a 128-bit message-digest is generated.

To appreciate the robustness of keying technology, RSA Laboratories recently announced that it's RC5-64 project had been solved. Unfortunately for hackers, it took in excess of 300,000 people working nearly five years to decipher the key. One can only imagine the amount of effort that would be entailed to decipher an algorithm, such as the MD-5 hashing algorithm, which involves the creation of a 128-bit message-digest from data input.

It is the transformation of existing hashing techniques, or other algorithms akin thereto, for use in an optical media environment which has resulted in the evolution

of a very robust copy protection scheme which, for all intents purposes, is impossible to defeat with known circumvention approaches, such as those discussed above. The present invention is particularly directed to meeting these needs.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a removable storage device, such as an optical media disc, which is constructed in a manner that prevents unauthorized copying.

Another object of the present invention is to provide such a new and useful optical media storage device which is relatively easy to manufacture without substantial increases in costs.

A further object of the present invention is the translation of known hashing techniques into an optical media environment to prevent unauthorized duplication of the optical media.

Yet another object of the present invention is to provide a new and useful methodology for creating such an optical media storage device.

Still a further object of the present invention is to provide a new and useful methodology of assessing the authenticity of optical media.

In accordance with these objectives, the present invention in one sense relates to an optical media storage device of a selected format that is adapted to be read by an optical reader. The optical media storage device comprises a substrate, such as polycarbonate, having a first surface and an opposite second surface, with the first surface having a data structure formed thereon. The metallic reflective layer is disposed over the data structure, and a protective layer, such as a polymeric film, is disposed over the metallic layer. To this end, the storage device may be a CD-ROM.

The data structure which is formed on the substrate includes an anomaly region, a fingerprint region and a program region. The anomaly region is configured to generate one or more errors when read by the optical reader. The fingerprint region has associated informational pits and lands corresponding to a target hash value obtained when the anomaly region is applied as an input to hashing algorithm. The program region has associated informational pits and lands corresponding to an executable application program which incorporates the hashing algorithm. This application program is coded such that, when the optical media storage device is read by the optical reader, the hashing algorithm is executed against the anomaly

region to generate the test hash value. In the preferred embodiment, the application program executes improperly if the test hash value and the target hash value are not the same. An improvement to a multi-layer optical media storage device of a selected format is also provided, wherein the improvement comprises a data structure such as discussed herein.

The hashing algorithm can be selected from a variety of known algorithms, such as MD-2, 4, or 5, or SHA-1, to name a few. Preferably, the MD-5 algorithm is employed to generate a 128-bit hash value, with the hashing algorithm being obscured within an executable version of the application program so that it is difficult to detect. In the illustrated embodiment of the optical media storage device, the anomaly region comprises a plurality of physical defects formed on the substrate. These physical defects are in the form of a plurality of anomalies on the substrate which have characteristics falling outside normal operating specifications for the selected format. The defects for the anomaly region may be contiguous on the substrate or dispersed throughout. The same is true for the informational pits and lands associated with fingerprint region.

A method of manufacturing a copy protected optical media storage device is also provided. According to this method, a mastering tape is created having information corresponding to a data structure as discussed above that is to be formed on a substrate. A glass master is generated from the mastering tape, and at least one stamper suitable for injection molding is fabricated from the glass master. A polycarbonate substrate is molded from the stamper and coded with a metallic reflective layer. A protective layer is then formed over the metallic reflective layer.

Another advantageous embodiment of the present invention relates to a method of assessing authentication of optical media. According to this methodology, an optical media storage device as described above is provided. The storage device is read by an optical reader whereby the hashing algorithm is executed against the anomaly region thereby to generate the test hash value. The optical media is authenticated only if the test hash value matches the target hash value. Otherwise, it is preferred to abort normal operation of the application program.

These and other objects of the present invention will become more readily appreciated and understood from a consideration of the following detailed description of the exemplary embodiments of the present invention when taken together with the accompanying drawings, in which:

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an enlarged cross-sectional view (not to scale) of a conventional read-only optical media storage device constructed according to the prior art;

Figure 2(a) is a representative perspective view (not to scale) which diagrammatically depicts a substrate with imbedded errors to form an altered production blank for use during the manufacture of an optical media disc according to the invention;

Figure 2(b) is a representative plan view (not to scale) which diagrammatically depicts features of a copy protected version of an optical media disc for use with the present invention, at the completion of its manufacture;

Figure 3 is a flowchart broadly illustrating a first exemplary embodiment of a methodology for creating a copy protected optical media disc according to the present invention;

Figure 4 is a flowchart of a more detailed rendition of the methodology diagrammatically shown in Figure 2;

Figure 5 is a flowchart illustrating how the broad methodology steps of Figures 3 & 4 can be performed by different entities/persons to create the copy protected optical media disc of the present invention; and

Figure 6 is a flowchart illustrating the operations performed when a user attempts to access stored information on a copy protected optical media disc that has been manufactured according to the teachings of the present invention.

DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS

In accordance with these objectives, the present invention in one sense concerns an optical media storage device, such as a compact disc (CD), which has been copy protected during its manufacture in such a manner that unauthorized access to data on the disc is exceedingly difficult, if not virtually impossible. The copy protected optical media disc is preferably in the form of a CD-ROM capable of storing computer software or other information in a read-only format. However, while the present invention will be described in the context of this particular type of optical media, it is contemplated that the teachings described herein can be extended to other CD formats, as well as other types of optical media such as DVDs, magnetic media and the like. Moreover, the teachings can also be adapted for use with various optical media formats, including read-only, write-once read-many, and erasable or re-writable

With this in mind, initial reference is made to Figures 2(a) and 2(b) to illustrate the evolution of various characteristics of the CD for achieving this copy protected state. It should be appreciated that Figures 2(a) and 2(b) are merely representative diagrammatic views and are neither drawn to scale or actual representations of the media itself. Figure 2(a) illustrates, according to one advantageous embodiment of the present invention, an early stage of an optical disc's manufacture prior to incorporation of the copy protectable data. At this stage, it can be characterized as an "altered production blank". The term "altered production blank" can refer to optical media having the characteristics discussed above with reference to Figure 2(a) such that it has defects imbedded thereon, corresponding to least some inconsequential data in the anomaly region, but has not yet evolve to the point in the manufacturing process where it has software or other data encoded on it. For instance, that the altered production blank could actually be a glass master having anomalies written on it by the LBR, either before or concurrently with, the writing of application data, so that the anomalies are translated onto the master's progeny and the production discs. Alternatively, the altered production blank could be generated from an off-the-shelf blank media disc which has been physically altered to generate the anomaly region that can be hashed.

In any event, altered production blank 10 has a representative area or region 12 which has been embedded with a plurality of physical defects 14. Defects 14 have been purposefully introduced during the initial stages of the disc's production. These physical defects 14 can assume a variety of different forms and the enlarged portion of Figure 2(a) is provided simply to illustrate that different varieties of physical defects could be employed.

For example, during the process of mastering conventional optical media, such as a CD, digital or analog source signals are converted to code for subsequent translation into a digital pattern of pits and lands by a laser beam recorder (LBR). The source signal themselves are derived by a suitable interface, which converts ISO source files, for example executables, into the appropriate signal stream used by the LBR. Thus, software developers can simply provide the appropriate ISO files to the mastering company which handles the remainder of the fabrication process. For developers desiring more control over how the data is written onto the media, some mastering companies provide toolkits so developers can write programming modules to accomplish this in accordance with the manufacturer's specifications.

As well understood by those skilled in the field, transitions between the pits and lands on the master disc are translatable into readable data on an optical disc generated therefrom during the production process. When created according to known specifications, these pits and lands have physical characteristics which fall within specified parameters. For example, on a CD having a single spiral track of data, 1.6 microns may separate radially adjacent track segments and the "pits" or "bumps" that make up the track are intended to be 0.5 microns wide, a minimum of 0.83 microns long and 125 nanometers high when viewed through the polycarbonate layer of the CD.

One aspect of the present invention relates to the creation of anomalies or defects, such as physical defects represented in Figure 2(a), for the purpose of generating structures which fall outside known specifications such that the defects are interpreted as errors when the CD is read by an optical reader. For representative purposes only, various types of such defects which can be created are shown in Figure 2(a), such as a ripple 16 in the surface, a scratch 18, as well as a variety of bumps 20, each of which has one or more geometric characteristics which deviates from conventional data parameters so that an optical reader cannot effectively interpolate whether they are intended to represent binary "1s" or "0s" during a reading interval. While the present invention describes such geometries as physical defects or anomalies, this terminology should not be unduly restricted. That is to say, the present invention contemplates any type of irregularity, discontinuity, ripple, defect, disruption, or other type of alteration, whether implemented in hardware (i.e. a physical defect) or software, which causes an optical reader to predictably interpret the anomaly, or a patterned array of them, as error(s) on the disc, or to erroneously misinterpret a binary "1" as a "0", and vice-versa. Further, while Figure 2(a) shows the array of defects 14 presented/embedded on a contiguous region 12, it is contemplated that one or more physical defects could be dispersed in such a manner that they span a single track, multiple track segments, are distributed in a plurality of confined regions, are interleaved amongst other accurate data on the manufactured disc, or distributed sporadically. In fact, it is contemplated that the defects can be presented in any desired patterned arrangement sufficient to accomplish the goals of the present invention. Accordingly, term "region" is used herein, whether in the context of the anomalies 14 or other aspects of the media, to broadly encompass each of these manners of distribution.

It is currently believed that the anomaly region on the finished disc (i.e. the copy protected production optical disc) will need to be in the form of a file or file(s) in order to be hashed, but it is also contemplated that this might not necessarily be required in all cases.

The generation of such physical defects can also be accomplished in a variety of known ways adequate to create the desired effects. These might include, for example, laser etching, burning, drilling, cutting, slicing, punching, etc. Approaches to creating such types of physical defects are discussed in U.S. Publication No. US 2002/0067674 A1, published June 6, 2002, and entitled "Method and System For Authenticating An Optical Disc Using Purposefully Provided Data Errors", and the ordinarily skilled artisan could readily adapt the teachings of this reference as one manner of generating anomalies on optical media for use with the present invention. The present invention, however, improves upon the technique(s) taught in the referenced publication, and other known technique for creating physical defects, to create a more robust copy protected production optical disc.

Generating the anomalies can also be implemented in software and translatable onto a glass master, and its progeny, during disc production. That is, a programming module can be written in accordance with the mastering company's interface specifications or requirements, which causes the LBR to create one or more anomalies on the glass master which have physical characteristics falling outside of operating specifications for the particular media format. A pertinently skilled artisan in the field who is familiar with such specifications would recognize that various type of anomalies could be created which would predictably cause an optical reader to generate one or more errors or misinterpretations during a read cycle of the finished disc.

With the above in mind, a first exemplary embodiment of a methodology for achieving a copy protected optical media is illustrated in the diagrammatic flowchart of Figure 3. According to this broad methodology, an altered production blank is provided at 102. A hashing algorithm 104 is applied to the altered production blank to generate, at 106, a hash value for the disc blank. As discussed in the background of the present application, hashing is a proven technology which up to this point has been utilized primarily for verifying data integrity in different types message transport applications and the like, where it is important to ensure that context has not been modified. Accordingly, it is not known by the inventors to utilize hashing in

connection with the production of optical media discs for the purpose of preventing or dissuading optical media piracy.

As used in herein, the term "hashing algorithm" broadly refers to any suitable function for implementation in the context of the present invention, whether implemented in software, hardware, or by other means, which receives an arbitrary length message, in the form of an input data string, and generates an output data stream that is characteristic of the message, wherein the hashing function has the characteristics of irreversibility and collision-resistance. The terms "message digest", "fingerprint" and "hash value" are used interchangeably herein to refer to the output data produced by the hashing algorithm. A variety of different hashing algorithms, such as MD2, MD4, MD5 and the secure hash algorithm (SHA) have been employed in the past in other contexts to generate a message digest having a selected bit length, such as 32-bit, 60-bit, 64-bit or even 128-bit. The preferred hashing algorithm employed with the present invention in its context utilizes the MD5 function to generate a 128-bit "fingerprint" or "message-digest" from the input.

In one advantageous embodiment, the hashing algorithm 104 which is applied to the error embedded optical disc blank 102 in methodology 100 scans only the physical defects as the input data for the hashing algorithm. Of course, the ordinarily skilled artisan would appreciate that the hashing algorithm could be applied to one or more of the actual physical defects embedded on the production blank, as well as other data which might be provided on the disc in order to generate the unique 128-bit hash value at step 106. Once the hash value has been generated, subsequent manufacturing processes accomplish encoding of the hash value, as well as a hashing algorithm, during the eventual creation of a finished product from the production blank, as represented at step 108 in Figure 3.

Accordingly, a production grade/commercially prepared optical disc 110 is produced, as diagrammatically represented in Figure 2(b). Such a disc 110 includes the anomaly region 12 as discussed above, a region 112 encoded with data corresponding to the hash value generated by the hashing algorithm, as well as another region 114 having encoded data corresponding to an executable form of the hashing algorithm. As discussed more thoroughly below, when a copy of disc 110 is made and one attempts to access valid data stored thereon, such as a software program or other information, the encoded hashing algorithm executes to generate a second hash value correlated to the copied disc 110.

With this construction in mind, and with an appreciation of conventional disc mastering as discussed above in the background section, reference is now made to Figure 4 which illustrates a preferred implementation of disc manufacture the according to the present invention. According to methodology 200, some type of physical alteration process may applied to an unaltered mastered glass disc to generate an altered glass master having an anomaly region. This step 202 illustrates various sub-routines which can be employed to generate the physically modified glass master disc, otherwise referred to as the altered optical disc blank 102 in Figure 3. After application of the hashing algorithm 204, the hash value or unique fingerprint for the modified glass master disc is generated at 206. At this point, the modified glass master disc is encoded at 207 with the hash value data as well as the hashing algorithm. The modified glass master disc is also encoded at 209 with the data/information correlated to the software to be provided on the disc. This might be, for example, any of a variety of software applications, produced by software developers. Of course, the encoding of the modified glass master disc at steps 207 and 209 would be accomplished by known techniques. In its preferred form, the hashing algorithm or checking mechanism is embedded into the executable version of the software program's source code which is subsequently translated into a digital pattern of pits and lands during the mastering process. It is moreover preferred that the hashing algorithm be embedded in such a manner that it is obscured and difficult to detect. The ordinarily skilled artisan would recognize that obfuscation can be accomplished in a variety manners, for example through encryption, opaque predicate modification (a set of multiple instructions which, when evaluated, always return the same result), lexical transformations, or compiler de-optimization, to name a few representative examples.

The unique hash value for the modified glass master disc preferably resides in another region of the CD separate from the executable and is also converted into corresponding pits and lands through known conversion techniques during mastering. Upon completion of the mastering process -- which as known might necessarily involve various sub-processing steps, as discussed above, a production optical disc is ultimately created from the modified master glass disc at 208.

A somewhat different rendition of the invention's methodology is shown in Figure 5. Methodology 300 contemplates that generation of the unique hash value 306 from an error embedded production blank, such as an optical disc blank 302, to

which has been applied the hashing routine 304, can be performed by a first party company or individual, while creation of the software program 303 would be accomplished by a second party company or individual. The software program would be initially created in source code and the software developer could be provided with a hashing toolkit 305 from the first party company/individual. This hashing toolkit, which may be in the form of a CD ROM, a downloadable executable file or the like, creates an executable version of the software program at 306 with the executable version having embedded therein the hashing routine 304 applied by the first party company/individual. The first party would also provide to the software developer as part of the hashing toolkit 305 the unique hash value for the error embedded optical disc blank so that the software developer could provide all of this information in an appropriate format to a third party mastering company responsible for creating the copy protected production optical disc at step 308.

With the above in mind, reference is now made to the flowchart of Figure 6 in order to appreciate the robustness of a copy protected storage device, such as a CD-ROM manufactured according to the teachings discussed above. According to the flowchart 400, the copy protected optical disc is inserted into a disc player at 402 and a copy of the disc is created at 404 through any of a variety of known techniques. At 406, the user attempts to access the stored program on the copied optical disc, at which point 408 the hashing algorithm embedded in the program's executable is run whereby a second hash value, referred to as "hash value (2)", is generated of the copied optical disc. The hashing algorithm makes an inquiry at 410 as to whether the second hash value for the copied optical disc matches the first hash value 411, referred to as "hash value (1)", which was encoded on the original protected disc and translated to the copied optical disc at step 404. As discussed above, there must be a match at inquiry 410 between the respective hash values in order for normal operation of the program to continue at 412.

However, the inventors have verified that the second hash value corresponding to the copied optical disc which is generated at step 408 will not match the first hash value for the copy protected optical disc. This is because, regardless of how the copying occurs at step 404 (such as through raw copying, ISO duplication or the like) the representation of the physical errors present on the original optical disc, which are created when it is copied at step 404, is different than the actual physical errors themselves. Thus, there will only be a match between the

target and test hash values when the optical media in the reader is the original optical media produced in accordance with the teachings herein, and not an attempted duplication.

Accordingly, when the copied optical disc is hashed at step 408 it generates a second fingerprint which is always different than the first fingerprint since the hashing algorithm is applied to representative errors and not the actual physical errors themselves. As such, the inquiry at 410 will, for all practical purposes, find that the first and second hash values do not match each other such that normal operation of the stored program is aborted at 414. As such, while a user might believe he/she has made a valid copy of the original disc at step 404, this copied version will not execute.

Accordingly, the present invention has been described with some degree of particularity directed to the exemplary embodiments of the present invention. It should be appreciated though that the present invention is defined by the following claims construed in light of the prior art so that modifications or changes may be made to the exemplary embodiments of the present invention without departing from the inventive concepts contained herein.

What is claimed is:

1. An optical media storage device of a selected format that is adapted to be read by and optical reader, comprising:

(a) a substrate having a first surface and an opposite second surface, said first surface having a data structure formed thereon which includes:

an anomaly region configured to generate one or more errors when read by the optical reader;

a fingerprint region having associated informational pits and lands corresponding to a target hash value obtained when said anomaly region is applied as an input to a hashing algorithm; and

a program region having informational pits and lands corresponding to an executable application program which incorporates said hashing algorithm, said application program being coded such that, when said optical media storage device is read by the optical reader, said hashing algorithm is executed against said anomaly region to generate a test hash value;

(b) a metallic reflective layer disposed over said data structure; and

(c) a protective layer disposed over said metallic reflective layer.

2. An optical media storage device according to claim 1 wherein said application program is operative to execute improperly if said test hash value is different than the target hash value.

3. And optical media storage device according to claim 1 wherein said hashing algorithm is MD-5.

4. An optical media storage device according to claim 3 wherein said target hash value is a 128-bit key.

5. An optical media storage device according to claim 1 wherein said hashing algorithm is obscured within said application program.

6. An optical media storage device according to claim 1 wherein said anomaly region, said fingerprint region and said executable region reside at separate locations on said substrate.

7. An optical media storage device according to claim 1 wherein optical media device is of a CD-ROM format.

8. An optical media storage device according to claim 1 wherein said substrate comprises polycarbonate and said protective layer is a polymeric film.

9. An optical media storage device according to claim 1 wherein said anomaly region comprises a plurality of contiguous physical defects formed on said substrate.

10. An optical media storage device according to claim 1 wherein said anomaly region comprises a plurality of anomalies formed on said substrate which have characteristics falling outside of normal operating specifications for the selected format.

11. An optical media storage device according to claim 1 wherein the informational pits and lands associated with said fingerprint region are contiguous.

12. In a multi-layer optical media storage device of a selected format that is adapted to be read by an optical reader, wherein optical media storage device comprises a polycarbonate substrate, a metallic reflective layer disposed over said substrate, and a polymeric film disposed over said metallic reflective layer, the improvement comprising a data structure formed on said substrate which includes:

an anomaly region configured to generate one or more predictable errors when read by the optical reader;

a fingerprint region having associated informational pits and lands corresponding to a target hash value obtained when said anomaly region is applied as an input to a hashing algorithm; and

a program region having associated informational pits and lands corresponding to an application program which incorporates said hashing algorithm.

13. The improvement of claim 12 wherein said application program is coded to scan said anomaly region and apply results obtained from said scan as an input to said hashing algorithm in order to generate a test hash value, said application program being further coded to execute improperly if said test hash value is different than the target hash value.

14. The improvement of claim in 12 wherein said hashing algorithm is selected from a group consisting of MD-2, MD-4, MD-5 and SHA-1.

15. The improvement of claim 14 wherein said hashing algorithm is obscured within an executable form of said application program.

17. The improvement of claim 12 wherein each of said anomaly region, said fingerprint region and said executable region resides at an unique location on said substrate.

18. The improvement of claim 12 wherein said anomaly region comprises a plurality of contiguous physical defects formed on said substrate.

19. An optical media storage device according to claim 12 wherein said anomaly region comprises a plurality of anomalies formed on said substrate which have characteristics falling outside of normal operating specifications for the selected format.

20. A method of manufacturing a copy protected optical media storage device, comprising:

(a) creating a mastering tape having information corresponding to a data structure to be formed on a substrate, wherein said data structure is to include:

an anomaly region configured to generate one or more predictable errors when read by an optical reader;

a fingerprint region having associated informational pits and lands corresponding to a target hash value obtained when said anomaly region is applied as an input to a selected hashing algorithm; and

a program region having associated informational pits and lands corresponding to an application program which is coded to execute said hashing algorithm against said anomaly region to generate a test hash value, and to abort normal program operation if said test hash value does not match said target hash value;

(b) generating a glass master from said mastering tape;

(c) fabricating at least one stamper suitable for injection molding from said glass master;

(d) molding a polycarbonate substrate from said stamper;

(e) coating said polycarbonate substrate with a metallic reflective layer; and

(f) forming a protective layer over said metallic reflective layer.

21. A method of assessing authenticity of optical media, comprising:

(a) providing an optical media storage device comprising:

(i) a substrate formed to include a data structure having:

an anomaly region configured to generate one or more predictable errors when read by an optical reader;

a fingerprint region having associated informational pits and lands corresponding to a target hash value obtained when said anomaly region is applied as an input to a hashing algorithm; and

a program region having informational pits and lands corresponding to an application program which incorporates said hashing algorithm, said application program being coded such that, when said optical media storage device is read by the optical reader, said hashing algorithm is executed against said anomaly region to generate a test hash value;

(ii) a metallic reflective layer disposed over said data structure; and

(iii) a protective layer disposed over said metallic reflective layer;

(b) reading said optical media storage device with an optical reader whereby said hashing algorithm is executed against said anomaly region thereby to generate said test hash value; and

(c) authenticating said optical media only if said test hash value matches said target hash value.

22. A method according to claim 21 whereby normal operation of said application program is aborted if the test hash value does not match the target hash value.

23. A method according to claim 21 said hashing algorithm obscured within said application program and is selected from a group of algorithm's consisting of MD-2, MD-4, MD-5 and SHA-1.

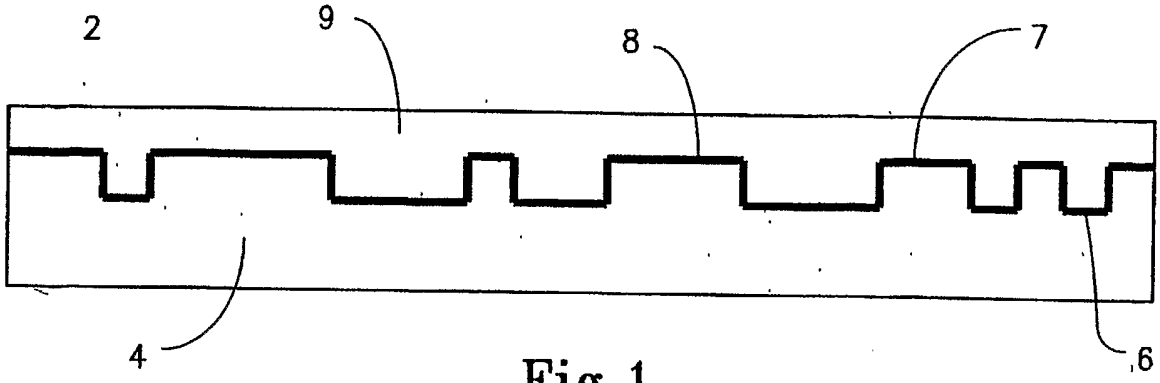


Fig.1
(Prior Art)

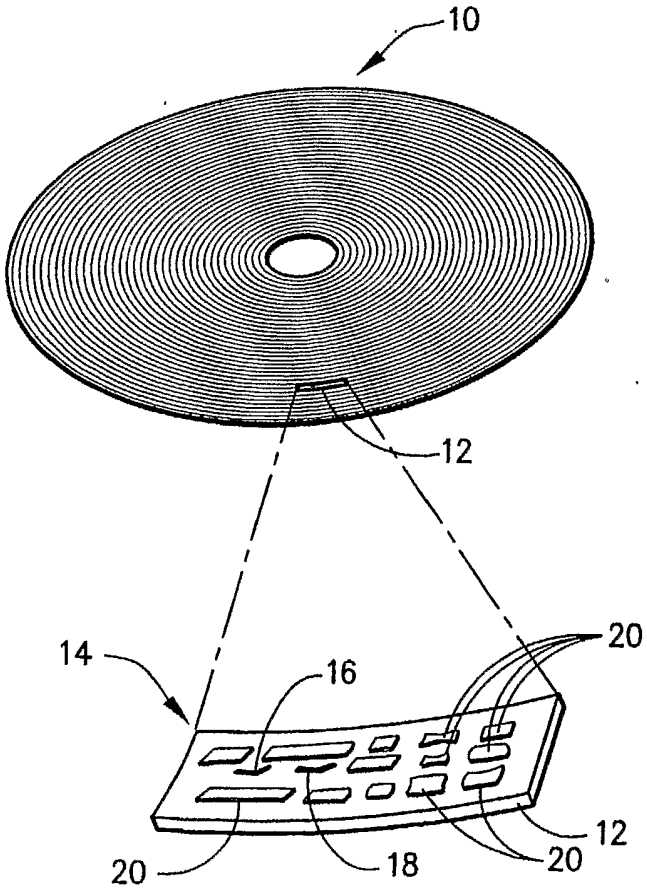


Fig.2a

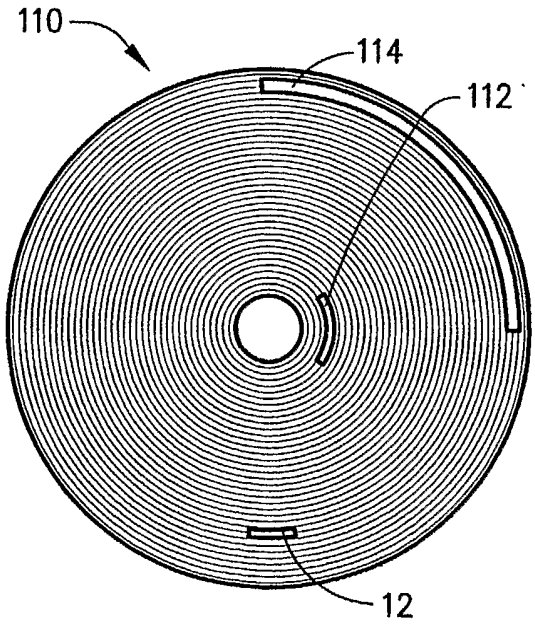


Fig.2b

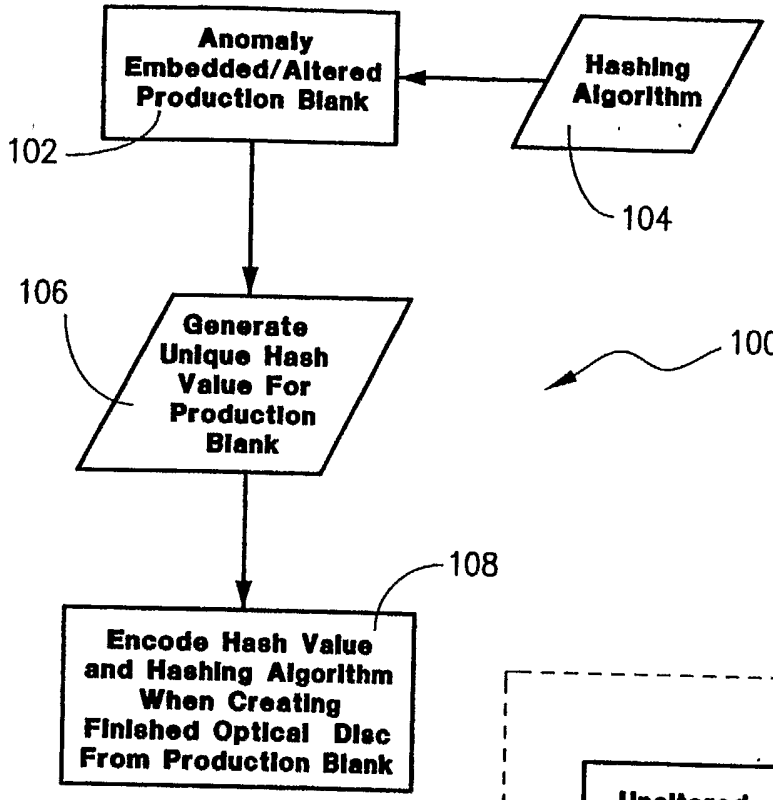

Anomaly Embedded/Altered Production Blank
Hashing Algorithm
102
104
106
Generate Unique Hash Value For Production Blank
100
108
Encode Hash Value and Hashing Algorithm When Creating Finished Optical Disc From Production Blank

Fig.3

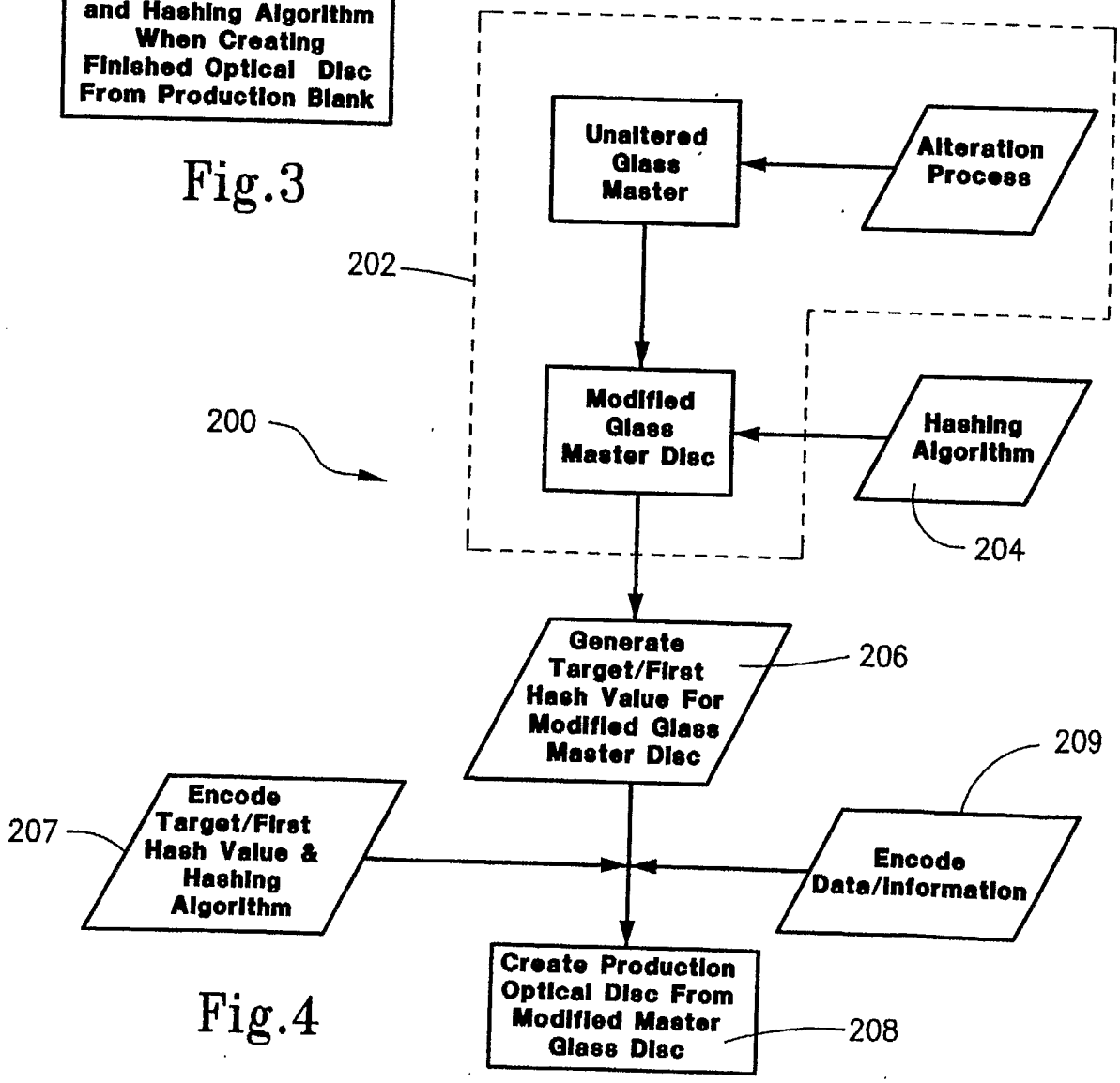

Unaltered Glass Master
Alteration Process
202
Modified Glass Master Disc
Hashing Algorithm
200
204
Generate Target/First Hash Value For Modified Glass Master Disc
206
209
Encode Target/First Hash Value & Hashing Algorithm
207
Encode Data/Information
Create Production Optical Disc From Modified Master Glass Disc
208

Fig.4

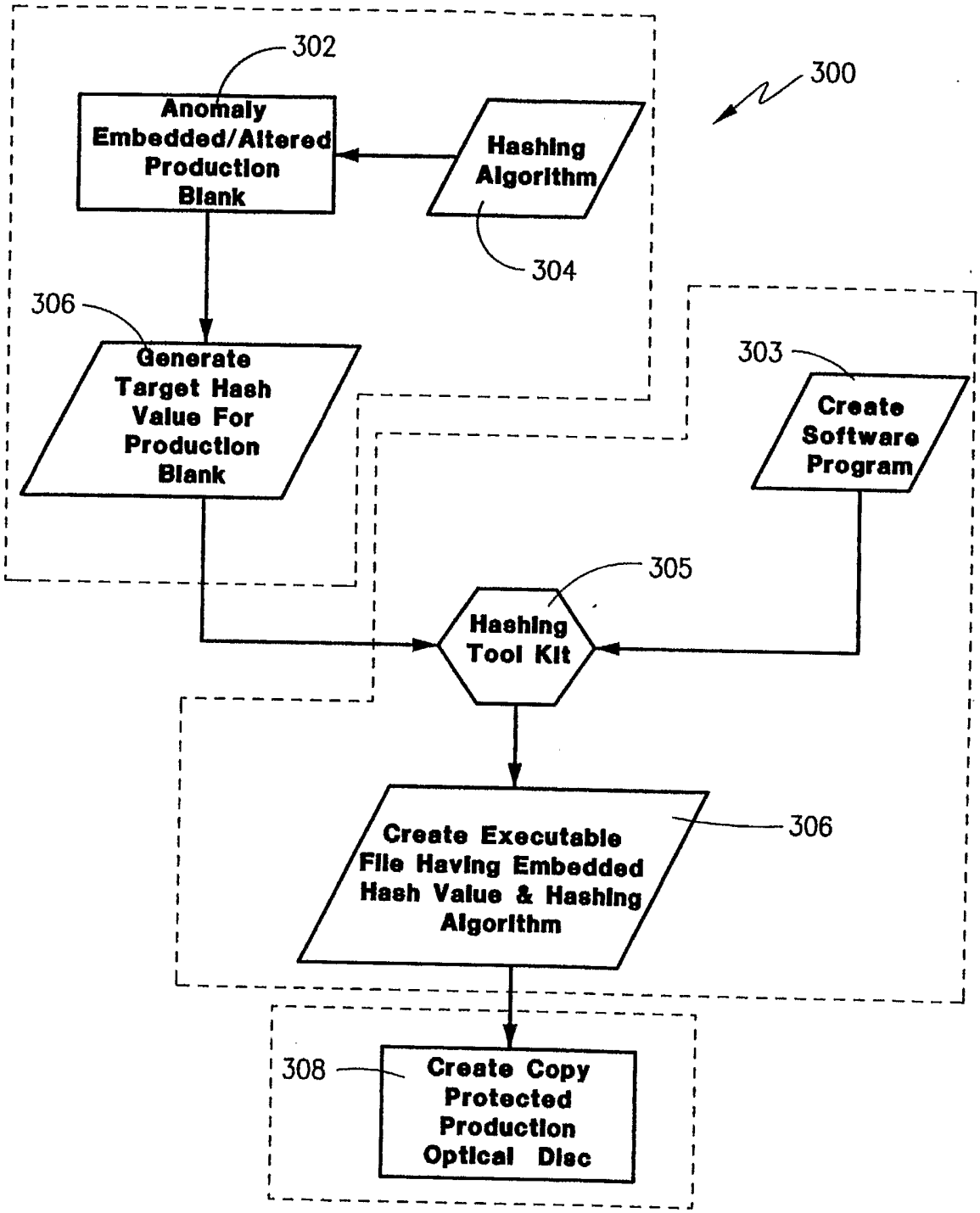

300
302
Anomaly Embedded/Altered Production Blank
Hashing Algorithm
304
306
Generate Target Hash Value For Production Blank
303
Create Software Program
305
Hashing Tool Kit
Create Executable File Having Embedded Hash Value & Hashing Algorithm
306
308
Create Copy Protected Production Optical Disc

Fig.5

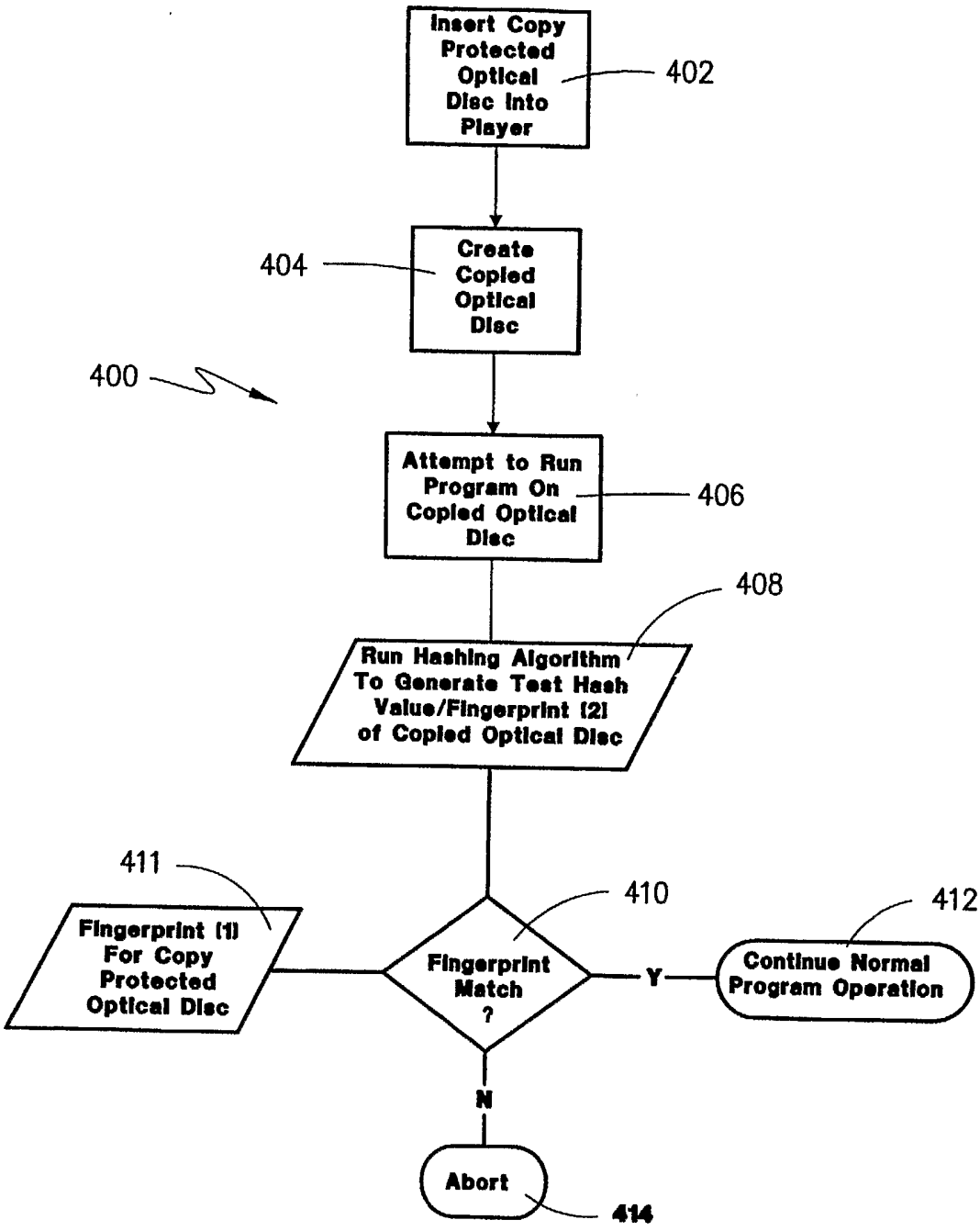

Insert Copy Protected Optical Disc into Player
402
Create Copied Optical Disc
404
400
Attempt to Run Program On Copied Optical Disc
406
408
Run Hashing Algorithm To Generate Test Hash Value/Fingerprint (2) of Copied Optical Disc
411
Fingerprint (1) For Copy Protected Optical Disc
410
Fingerprint Match ?
412
Y
Continue Normal Program Operation
N
Abort
414

Fig.6