

TITLE OF THE INVENTION

**SYSTEM FOR SECURELY STORING AND DISTRIBUTING DIGITAL
CONTENT, PROCESSES TO BE IMPLEMENTED IN THE SYSTEM, AND
DATA FORMAT AND STRUCTURE THEREFOR**

5

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a system for securely storing and distributing a digital content, processes to be implemented in the system, and
10 data format and structure therefor, particularly, relates to protecting a digital content such as a document, an audiovisual content and an image and relates to distributing the digital content through a digital content storage medium such as a CD disc, a DVD disc and a USB flash memory by implementing unique biometric information inherent in a particular person such as a
15 fingerprint and an iris as unique personal identification (PID) to identify the particular person as a preferred user from other users.

Description of the Related Art

Currently, there are many data protection systems that can scramble
20 important data on the basis of a password. The scrambled important data can be recorded in a storage medium such as a CD disc and a DVD disc and distributed to a specific person who knows the password. By using a dedicated application, the designated specific person can restore the scrambled or encrypted important data from the CD disc or the DVD disc. Those
25 applications are for sharing or storing all types of sensitive information in an encrypted form and for assigning detailed permission rights. A user of a protection system can decide who is allowed to read, copy, write or share the sensitive information that have been encrypted and stored in a CD disc, a DVD

disc, or other storage media such as audio, video, spreadsheets and presentations.

Accordingly, the user can mail or share encrypted information stored in a CD disc and only an intended recipient of the CD disc can access to the
5 contents of the CD disc.

One typical commercial product has been provided from RICOH Company that is called "EncryptEase" (refer to the homepage of RICOH Company, http://www.ricoh.com/media/cd-r/rr_point.html).

Another product is called "TrueCrypt", which is a free open-source disc
10 encryption software (refer to <http://www.truecrypt.org/>).

In these prior arts, however, there is a problem such that a password is easily forgotten, lost, stolen, or hacked.

Further, if a different password is required for each different CD disc, a user might be in confusion when remembering a plurality of passwords.

15 Furthermore, sometimes, decryption of content in a CD disc may result in long delay when the user tries to view contents of the CD.

More, it is very difficult to transfer ownership or license of a CD disc unless a password of the CD disc is shared with different people. Security-wise, sharing the same password with several people is quite dangerous.

20 In addition thereto, following patents are supposed to be relevant to the present invention:

1. U.S. Patent No. 7,020,057 B2 titled "Apparatus and associated methodology of imparting content protection to optically recorded data for secure reproduction",
- 25 2. U.S. Patent No. 6,738,331 B2 titled "Copy-protected optical disk and protection process for such disk",
3. U.S. Patent No. 6,950,941 B1 titled "Copy protection system for portable storage media",

4. U.S. Patent No. 7,062,686 B2 titled "Data copy protection using reproduction error determination and predetermined pattern recognition",
5. U.S. Patent No. 7,162,642 B2 titled "Digital content distribution and method",
- 5 6. U.S. Patent No. 6,982,110 B2 titled "Information recording medium and manufacturing method thereof",
7. U.S. Patent No. 6,847,948 B1 titled "Method and apparatus for secure distribution of software/data",
8. U.S. Patent No. 6,799,271 B2 titled "Method and system for authenticating user and providing service",
- 10 9. U.S. Patent No. 7,215,771 B1 titled "Secure disk drive comprising a secure drive key a drive ID for implementing secure communication over a public network", and
10. U.S. Patent No. 6,611,812 B2 titled "Secure electronic content distribution on CDs and DVDs".
- 15

SUMMARY OF THE INVENTION

20 Accordingly, in consideration of the above-mentioned problems of the prior arts, an object of the present invention is to provide a system for securely storing and distributing a digital content, processes to be implemented in the system, and data format and structure therefor, which uses unique biometric information inherent in a particular person such as a fingerprint and an iris as

25 unique personal identification (PID) to identify the particular person from other persons as well as generating related security information and the latest storage technologies such as RFID (radio frequency identification) tags, SD memory cards, USB flash memories as a PID storage device to store the unique

PID and security information.

In order to achieve the above object, the present invention provides, according to an aspect thereof, a system for securely storing and distributing a digital content comprising: (a) a personal identification (PID) database and management server including, (1) a local PID register module for registering
5 user's PID information locally, (2) a remote PID register server module for registering user's PID information remotely, (3) a database for securely storing a plurality of user's PID information and for providing network access through its TCP/IP access module, (4) database manager for managing the plurality of
10 user's PID information so as to be inserted or deleted, and (5) a PID reader for scanning user's PID information locally so as to register the user's PID information to the database through the local PID register module; (b) a content protection and distribution server including, (1) a content protector for encrypting a digital content by using an encryption key being generated on the
15 basis of user's PID and PID storage device ID and system generated random user ID, (2) a PID database file for storing user's PID information, (3) a digital content storage writer for writing the encrypted digital content to a digital content storage medium, (4) a PID reader for scanning user's PID information to register or verify the user's PID information, (5) a PID storage reader & writer
20 for writing data to or reading data from an PID storage device to be accompanied by the digital content storage medium, and (6) a local PID register module for registering user's PID information locally; (c) a content playback client for verifying user's PID information and regenerating content and encryption keys and decrypting an encrypted digital content stored in a digital
25 content storage medium, the content playback client including, (1) a digital content storage reader for reading an encrypted digital content from a digital content storage medium to be supplied, (2) a PID reader for scanning user's PID information to register or verify the user's PID information as a preferred

user, (3) a PID storage reader & writer for reading data from or writing data to an PID storage device to be provide together with the digital content storage medium, (4) a remote PID register module for registering the user's PID information remotely, and (5) a content decryption filter driver; and (d) a
5 network for providing network connection among the PID database and management server, the content protection and distribution server and the content playback client, the system for securely storing and distributing a digital content characterized in that a digital content is encrypted and securely stored in a digital content storage medium and distributed to a preferred user
10 through the digital content storage medium, and that the PID database and management server stores and manages a plurality of user's PID information registered locally or remotely, and that the content protection and distribution server encrypts a digital content and writes the encrypted digital content in a digital content storage medium, and that the content protection and
15 distribution server creates security information and stores the security information in an PID storage device, and that unique PID information is used to generate an encryption key, and that the content decryption filter drive is allocated between a file system layer and a digital content storage reader driver layer for passing and interpreting massages and data transferred between a file
20 system and the digital content storage reader, and that the encrypted digital content is decrypted on the fly by the content key on the basis of the user's PID information and the PID storage device ID and the system generated random user ID.

Other object and further features of the present invention will be apparent
25 from the following detailed description when read in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a system for securely storing and distributing a digital content showing system architecture according to an embodiment of
5 the present invention.

FIG. 2 is a flowchart showing a process for securely storing and distributing a digital content according to the embodiment of the present invention.

FIG. 3 is a flowchart showing a process for recovering a protected
10 preferred digital content and viewing the protected preferred digital content by a preferred user according to the embodiment of the present invention.

FIG. 4a is a flowchart showing a process for generating a 128-bit (16-byte) content key according to the embodiment of the present invention.

FIG. 4b shows a data structure of the 16-byte content key.

15 FIG. 5 is a flowchart showing a process for generating a first encryption key for encrypting the 16-byte content key shown in FIG. 4b according to the embodiment of the present invention.

FIG. 6a is a data structure of 16-byte disc ID to be divided into two groups.

20 FIG. 6b is a data structure of the 16-byte disc ID being divided into two groups.

FIG. 7 is a flowchart showing a process for generating a second encryption key for encrypting secret data in 16 bytes according to the embodiment of the present invention.

25 FIG. 8 shows a structure of a minor PID (personal identification) flag supporting 4 minor PID according to the embodiment of the present invention.

FIG. 9a shows a structure of the minor PID storing identification (ID) of the 4 minor PID and an IP address and a port number of a server according to

the embodiment of the present invention.

FIG. 9b shows a structure of minor PID storing data length and data of the 4 minor PID according to the embodiment of the present invention.

FIG. 10 is a block diagram of the content decryption filter driver shown in
5 FIG. 1.

DETAILED DESCRIPTION OF THE INVENTION

[Embodiment]

Prior to detailing an embodiment of the present invention, background of
10 the present invention is described first.

It is commonly known that everyone has some unique and immutable biometric information, which is inherent in each person and never stolen by other person. One example of unique biometric information is a fingerprint, which is consist of a series of ridges and furrows on a surface of a finger. Such
15 a fingerprint has been successfully used in numerous applications such as personal identification for criminal investigation and banking.

Further, by virtue of the latest storage technologies, a storage device such as an RFID (radio frequency identification) tag, an SD memory card and a USB flash drive, which are large in memory size but small in physical size, is
20 commonly provided as a personal identification (hereinafter referred to as PID) storage device.

Furthermore, unique PID information and related security information can be stored in such a PID storage device. The PID storage device can be sent to a preferred user together with a digital content storage medium, which
25 contains a preferred digital content, such as a CD disc and a DVD disc to be distributed to the preferred user.

More, basic content information in a PID storage device can be easily viewed by just scanning the PID storage device through a corresponding PID

storage device reader such as an RFID tag reader of which reading speed is much faster than that of a digital content storage medium reader such as a DVD disc drive, which reads a digital content stored in a digital content storage media or a DVD disc.

5 Moreover, in the present invention, security information and license information are stored in a PID storage device that is rewritable, so that license information can be transferred to a new user or can be updated from time to time without issuing a new digital content storage medium.

10 A system according to the present invention can support the strong encryption algorithms such as AES (Advanced Encryption Standard), Blowfish and Triple-DES (Data Encryption Standard).

Further, the system implements a content decryption virtual drive so as to allow a preferred user to directly access encrypted data or an encrypted digital content stored in a digital content storage media.

15 Furthermore, a data writer for a digital content storage medium such as a CD/DVD burner is also integrated in the system.

More, the system provides a real-time decryption process, so that a user is hardly disturbed by decryption delays.

20 Moreover, the system can permit transferring ownership or license of a digital content in a digital content storage medium to another user and also sharing the license among several users without disclosing any secret information.

Accordingly, a digital content is securely protected and distributed in the system according to the embodiment of the present invention.

25 In reference to the accompanying drawings, a preferred embodiment of the present invention is described in detail next.

FIG. 1 is a block diagram of a system for securely storing and distributing a digital content showing system architecture according to an embodiment of

the present invention. In FIG. 1, the system is composed of a "PID database and management server" 1, a "content protection and distribution server" 2, a "content playback client" 3 and a network 4. Each of the "PID database and management server" 1, the "content protection and distribution server" 2 and the "content playback client" 3 uses information-processing devices such as a so-called general-purpose computer, a workstation and a personal computer (PC) as well as a network connectable information-processing device, for instance, a digital home electric appliance and a portable terminal such as a PDA (personal digital assistant) and a cellular phone.

10 Further, in the system according to the embodiment of the present invention, a digital content is encrypted and securely stored in a digital content storage medium such as a CD disc and a DVD disc. The encrypted digital content securely stored in the digital content storage medium is distributed to a preferred user

15 Furthermore, it should be understood that processes to be detailed could be implemented by a software product and that a part of the processes could be carried out in a hardware unit.

Each component of the system is furthermore described in detail next.

20 Firstly, the "PID database and management server" 1 stores and manages preferred user's PID information that is registered locally or remotely. The "PID database and management server" 1 is further composed of a "local PID register module" 1a for registering preferred user's PID information as unique PID information locally through a PID reader 1e, a "remote PID register server module" 1b for registering preferred user's PID information remotely, a database 1c for storing a plurality of preferred user's PID information securely and for providing network access through a TCP/IP access module therein, and a "database manager" 1d for managing the plurality of preferred user's PID information stored in the database 1c so as to be inserted or deleted.

Secondly, the "content protection and distribution server" 2 encrypts a digital content and writes the encrypted digital content into a digital content storage medium such as a DVD disc.

Further, the "content protection and distribution server" 2 creates security
5 information and stores the security information in a PID storage device such as an RFID tag.

The "content protection and distribution server" 2 is further composed of a "PID database (DB) file" 2a for storing preferred user's PID information, a "digital content storage writer" 2b for writing an encrypted digital content into a
10 digital content storage medium, a "PID reader" 2c for scanning user's PID information to register or verify the user's PID information, a "PID storage reader & writer" 2d for writing data into or reading data from a PID storage device that is accompanied by the digital content storage medium storing the encrypted digital content to be distributed, a "local PID register module" 2e for
15 registering user's PID information locally, and a "content protector" 2f for encrypting a digital content together with a second encryption key that is generated on the basis of user's PID information, PID storage device identification (ID), and user ID that is randomly generated by the system.

Thirdly, the "content playback client" 3 verifies user's PID information,
20 regenerates a content key and first and second encryption keys, and decrypts an encrypted digital content stored in a digital content storage medium.

The "content playback client" 3 is further composed of a "digital content storage reader" 3a such as a DVD drive for reading an encrypted digital content out from a digital content storage medium to be distributed, a "PID reader" 3b
25 for scanning user's PID information to register or verify the user's PID information, a "PID storage reader & writer" 3c for reading data out from or write data into a PID storage device that is accompanied by the digital content storage medium storing the encrypted digital content, a "remote PID register

module" 3d for registering user's PID information remotely to the database 1c through the "remote PID register server module" 1b in the "PID database and management server" 1 by way of the network 4, and a "content decryption filter driver" 3e.

5 Hereupon, the "content decryption filter driver" 3e is allocated between a file system layer and a digital content storage reader layer so as to pass and interpret a message and data transferred between a file system and the "digital content storage reader" 3a, wherein an encrypted digital content is decrypted on the fly by a first encryption key that is regenerated by a preferred user based
10 on user's PID information, PID storage device ID and user ID that is randomly generated by the system. The "content decryption filter driver" 3e will be detailed.

 Fourthly, the network 4 such as LAN (Local Area Network) and the Internet provides a network connection among the "PID database and
15 management server" 1, the "content protection and distribution server" 2 and the "content playback client" 3 respectively.

 A digital content described in the embodiment of the present invention can be applicable to any type of digital content such as a JPEG image, a document and a digital audiovisual file.

20 Further, such a digital content can be generated outside the system and imported by an administrator through a digital content storage medium, a network file sharing program or an FTP (File Transfer Protocol) site.

 In the system according to the embodiment of the present invention, it is allowed for an administrator or an authorized personnel in a provider or a
25 distributor of a digital content to define an encryption strategy for initializing the "content protector" 2f in the "content protection and distribution server" 2 for a project of distribution of a digital content. The encryption strategy defines a block cipher algorithm such as the DES, the AES and the Blowfish, a seed for

generating a random key, preferred key length for the block cipher algorithm that accepts variable length keys and preferred plain-text block size such as 64-bit, 128-bit and 256-bit. In case such an encryption strategy is not defined, a default encryption strategy is applied to the system according to the
5 embodiment of the present invention.

In the system according to the embodiment of the present invention, it is firstly required for a user who wants to be a preferred user to register his PID information such as his fingerprint on the database 1c in the "PID database and management server" 1 or on the "PID DB file" 2a in the "content protection and
10 distribution server" 2 through any of the "local PID register module" 1a in the "PID database and management server" 1, the "local PID register module" 2a in the "content protection and distribution server" 2 and the "remote PID register module" 3d in the "content playback client" 3.

More specifically, in case the user wants to register his PID information
15 locally, his PID information is scanned in through the "PID reader" 1e in the "PID database and management server" 1 and registered on the database 1c by way of the "local PID register module" 1a, or scanned in through the "PID reader" 2c in the "content protection and distribution server" 2 and registered on the "PID DB file" 2a by way of the "local PID register module" 2e.

20 On the other hand, in case the user wants to register his PID information remotely, his PID information is scanned in through the "PID reader" 3b in the "content playback client" 3. In this case, scanned his PID information is transmitted to the database 1c in the "PID database and management server" 1 through the "remote PID register module" 3d in the "content playback client" 3
25 and the "remote PID register server module" 1f in the "PID database and management server" 1 by way of the network 4. The user's PID information is securely protected from any disclosure. Only the administrator has the right to access data in the "database" 1c or the "PID DB file" 2a.

Further, in the system according to the embodiment of the present invention, it is defined that user's PID information is transmitted through a pre-established SSL (Secure Sockets Layer) link from the "remote PID register module" 3d to the "remote PID register server module" 1b and protected by
5 using an asymmetric cipher method or a public-key cryptographic algorithm such as the RSA (Rivest-Shamir-Adelman) public-key cryptography.

Furthermore, in the system according to the embodiment of the present invention, it is allowed for the administrator to create a new project for distributing a preferred digital content to a preferred user who has previously
10 registered his PID information.

In the system according to the embodiment of the present invention, a user's fingerprint functions as unique PID information, wherein unique PID information is used to generate the first encryption key for decrypting the encrypted preferred digital content, an RFID tag functions as a PID storage
15 device, a CD or DVD disc functions as a digital content storage medium, and a DVD writer functions as the "digital content storage writer" 2b.

Further, in the system according to the embodiment of the present invention, an RFID reader functions as the "PID storage reader & writer" 2d and a fingerprint reader functions as the "PID reader" 1c, 2c or 3b.

20 Furthermore, in the system according to the embodiment of the present invention, disc ID, which is a unique GUID (globally unique identifier) that is randomly generated by the system for each digital content storage medium, functions as system content storage ID.

More, in the system according to the embodiment of the present invention,
25 RFID ID, which is a unique ID for each RFID tag, functions as PID storage ID. The PID information is read out securely from the "database" 1e in the "PID database and management server" 1 through the "network" 4 or locally from the "PID DB file" 2a in the "content protection and distribution server" 2.

In reference to FIG. 2, a process for securely storing and distributing a digital content in the system according to the embodiment of the present invention is described in detail next.

FIG. 2 is a flowchart showing a process for securely storing and distributing a digital content according to the embodiment of the present invention. The process is implemented in the system for securely storing and distributing a digital content mentioned above.

In FIG. 2, an administrator or an authorized personnel in a provider or a distributor of a digital content creates a new project and defines an encryption strategy for initializing the "content protector" 2f in the "content protection and distribution server" 2 so as to project distribution of a digital content (step S101). The encryption strategy defines a block cipher algorithm such as the DES, the AES and the Blowfish, seeds for generating random keys, preferred key length for the block cipher algorithm and preferred plaintext block size such as 64-bit, 128-bit and 256-bit.

Further, the administrator adds a digital content to the newly created project (step S102), wherein a digital content can be generated somewhere outside the system and imported through a digital content storage medium, a network file sharing program or an FTP site.

On the other hand, a user who wants to be a preferred user firstly registers his PID information such as a fingerprint on the "database" 1c in the "PID database and management server" 1 or on the "PID DB file" 2a in the "content protection and distribution server" 2 as unique PID information such as a fingerprint template 11 by scanning in his fingerprint through the "PID reader" 1e, 2c or 3b, wherein the fingerprint template is called user's unique PID information or secret data (step S201), and then request his preferred digital content.

The administrator further selects a preferred user from the "database" 1c

in the "PID database and management server" 1 or from the "PID DB file" 2a in the "content protection and distribution server" 2 (step S103).

These information and secret data such as the preferred digital content, the preferred user's information and the fingerprint template 11 are
5 transmitted to the "content protection and distribution server" 2.

In the "content protection and distribution server" 2, a content key 12 for encrypting a preferred digital content is randomly generated (step S104). Length of the content key 12 is defined by the encryption strategy.

Further, a first encryption key 14 for encrypting the content key 12 is
10 generated in the "content protection and distribution server" 2 on the basis of the fingerprint template 11, system content storage ID such as disc ID, which is a unique GUID randomly generated by the "content protection and distribution server" 2 for each digital content storage medium, and the time and date when the new project was created (step S105).

15 Furthermore, in the "content protection and distribution server" 2, a second encryption key 15 for encrypting the fingerprint template 11 or the secret data is randomly generated on the basis of PID storage ID, the disc ID, an owner's name and the time and date when the new project was created (step S106).

20 More, the "content protection and distribution server" 2 encrypts the preferred digital content 13 by using the content key 12 (step S107). Consequently, the preferred digital content 13 is encrypted and securely protected.

Moreover, the "content protection and distribution server" 2 encrypts the
25 content key 12 by using the first encryption key 14 (step S108).

In addition thereto, the "content protection and distribution server" 2 encrypts the secret data (fingerprint template 11) by using the second encryption key 15 (step S109).

Finally, the "digital content storage writer" 2b in the "content protection and distribution server" 2 writes the encrypted preferred digital content 16 to a digital content storage medium 21 (step S110). Consequently, the preferred digital content 13 is securely stored in the digital content storage medium 21.

5 On the other hand, the "PID storage reader & writer" 2d in the "content protection and distribution server" 2 writes the encrypted secret data 18 and the encrypted content key 17 to an PID storage device 22 together with various information such as system ID, the disc ID, a title, the owner's name, a company name, the time and date when the new project was created and a
10 comment (step S111). Hereupon, the system ID is a unique GUID to indicate that the digital content storage medium 21 is created by the system according to the embodiment of the present invention.

As a result, the digital content storage medium 21 securely storing the encrypted preferred digital content 16 can be distributed to the preferred user
15 together with the PID storage device 22 recorded with the secret data by way of mail or courier.

In reference to FIG. 3, a process for recovering the protected preferred digital content 13 stored in the digital content storage medium 21 created as mentioned above and viewing the protected preferred digital content 16 is
20 described in detail next, wherein the process is implemented in the "content playback client" 3.

FIG. 3 is a flowchart showing a process for recovering a protected preferred digital content and viewing the protected preferred digital content by a preferred user according to the embodiment of the present invention.

25 In FIG. 3, in case the preferred user wants to view the protected preferred content 13 securely stored in the digital content storage medium 21 when he received the digital content storage medium 21 together with the PID storage device 22, he must firstly scan in his unique PID information such as a

fingerprint by using the "PID reader" 3b in the "content playback client" 3 (step S301).

Further, the "PID storage reader & writer" 3c in the "content playback client" 3 reads out the encrypted secret data 16, the encrypted content key 17
5 and other information from the PID storage device 22 distributed together with the digital content storage medium 21 storing the encrypted and protected preferred digital content 16 (step S302).

Furthermore, the second encryption key 15 that was used to encrypt the secret data (fingerprint template 11) is regenerated on the basis of the PID
10 storage ID, the disc ID, the owner's name, the time and date when the new project was created (step S303). The regenerated second encryption key 15 decrypts the encrypted secret data 18 (step S304), and then the fingerprint template 11 is recovered.

Succeedingly, the recovered fingerprint template 11 is used to verify the
15 user's unique PID information or the fingerprint that was scanned in previously in the step S301 whether or not the user's fingerprint matches with the fingerprint template 11 (step S305). In case the fingerprint matches with the fingerprint template 11, the user is verified as a legal user or the preferred user. Otherwise, he is defined as an illegal user.

20 In case the user is verified as the legal user, the "content playback client" 3 regenerates the first encryption key 14 that was used to encrypt the content key 12 (step 306). Then, the first encryption key 14 decrypts the encrypted content key 17 (step S307). On the contrary, in case the user is defined as an illegal user, the "content playback client" 3 rejects the user's request.

25 The content key 12 that is decrypted in the step S307 is transferred to the "content decryption filter driver" 3e in the "content playback client" 3. The "content decryption filter driver" 3e is disposed between a file system layer and a digital content storage drive driver layer such as a DVD drive driver layer so

as to pass and interpret messages and data to be transferred between the file system and the digital content storage drive driver.

The content key 12 activates the "content decryption filter driver" 3e to drive the "digital content storage reader" 3e. The encrypted preferred digital
5 content 16 securely stored in the digital content storage medium 21 is decrypted and read out by the "content decryption filter driver" 3e (step S308).

Accordingly, the protected preferred digital content 13 is recovered and viewed by the legal user.

In this connection, the encrypted preferred digital content is decrypted in
10 real-time, so that the legal user can use a normal application software such as MS WORD, MS EXCEL and PDF Viewer for viewing the digital content without any disturbance of decryption delay.

Additionally, in the system according to the embodiment of the present invention, it is basically allowed for the legal user of the digital content storage
15 medium 21 to transfer his ownership or license of the digital content storage medium 21 or the preferred digital content 13 stored in the digital content storage medium 21 to others. In case the legal user has the right to transfer his ownership or license to others, he can request for the ownership or license transfer of the digital content storage medium to others as long as his PID
20 information or his fingerprint is registered in the PID storage device 22 as major PID information or a major fingerprint. In this case, firstly, the legal user or the major user must scan in his PID information or his fingerprint so as to be authenticated. Then another user or a minor user to whom the license or ownership is transferred is required to scan in his PID information or his
25 fingerprint, wherein the minor user's fingerprint is protected as new major PID information or new secret data and saved in the PID storage device 22.

At the same time, a new first encryption key for encrypting the content key 12 is generated on the basis of the minor user's PID information or the minor

user's fingerprint, wherein the content key 12 is re-encrypted by the new first encryption key. All the information stored in the PID storage device 22 are updated in accordance with the minor user.

Further, it is also allowed for the legal user or the major user to share the preferred digital content 13 with several other person to be minor users as long as their PID information or their fingerprints are added into the PID storage device 22 as minor PID information or minor fingerprints. These minor fingerprints are protected by the second encryption key 15 for the secret data.

Furthermore, a minor user must scan his fingerprint first when he wants to view the protected preferred digital content 13. In this case, his fingerprint is verified whether the scanned fingerprint matches with the registered fingerprint in the PID storage device 22 or not. The same is applied to other minor users. In case the minor user is verified as a legal minor user, the "content playback client" 3 makes use of the major fingerprint for recovering the content key 12 and decrypts the preferred digital content 13.

In reference to FIGs. 4a and 4b, generating a content key in 128 bits (16 bytes) for encrypting a digital content is described in detail next.

FIG. 4a is a flowchart showing a process for generating a 128-bit (16-byte) content key according to the embodiment of the present invention, and FIG. 4b shows a data structure of the content key in 16 bytes.

According to the embodiment of the present invention, a 128-bit (16-byte) content key for encrypting a digital content is generated as follows.

1. Set a count number (nCount) of a counter "i" and a loop counter "j" to a byte number of a content key respectively (step S401). In this case, the byte number of the content key is 16, so that "i = j = 16", that is, "nCount = 16".

2. Generate a seed for a random number generator (step S402), wherein the "GetTickCount()" function" can be used to retrieve a number of time in milliseconds, which is elapsed time since the system has been activated.

3. Set the seed in the random number generator (step S403).
4. Generate random number "rNum" that falls in [0, 255], wherein the random number "rNum" can be generated by the "srand() function" for the C++ programming language (step S404).
- 5 5. Set a (16 - nCount)th byte of the content key to be the generated random number (step S405).
6. Set the loop counter "j" to "j - 1". In other words, subtract 1 (one) from "nCount", that is, "nCount - " (step S406).
7. Judge the "nCount" whether it is equal to zero or not (step S407). In
10 case the "nCount" is zero (Yes), a 128-bit (16-byte) content key is obtained. In case the "nCount" is not zero (No), return to the step S404 and repeat the above procedures until the "nCount" becomes zero (j = 0).

Hereupon, an actual configuration of the 16-byte content key is shown in FIG. 4b, wherein "Ckey[15]" and "Ckey[0]" denotes the most significant byte
15 and the least significant byte of the 16-byte content key respectively.

In reference to FIG. 5, a process for generating a first encryption key that encrypts the 16-byte content key is described in detail next.

FIG. 5 is a flowchart showing a process for generating a first encryption key that encrypts the 16-byte content key shown in FIG. 4b according to the
20 embodiment of the present invention.

A first encryption key for encrypting the 16-byte content key shown in FIG. 4b is generated as follows.

1. Assume that system content storage ID such as disc ID is in "L" bytes. Hereinafter the system content storage ID is generically referred to as disc ID.
- 25 2. Divide the L-byte disc ID into two groups such as Group 1 and Group 2 (step S501).

Hereupon, each step of dividing disc ID is described in detail next with reference to FIGs. 6a and 6b.

FIG. 6a is a data structure of 16-byte disc ID to be divided into two groups, and FIG. 6b is a data structure of the 16-byte disc ID being divided into two groups, wherein "L" byte disc ID is defined as 16 byte disc ID.

(a) Two least significant bytes, that is, B[0] and B[1] are always allocated in Group 1, and two most significant bytes, that is, B[L-1] and B[L-2] are always allocated in Group 2. The disc ID is defined as 16 bytes, so that the most significant bytes B[L-1] and B[L-2] are illustrated as B[15] and B[14] respectively in FIG. 6a.

(b) The disc ID is divided into Group 1 and Group 2 on the basis of date (DD MM YYYY) when the project was created, which is one of the system content storage ID. Each byte of the disc ID is allocated as follows:

- (1) In case "DD" is an odd number, then B[2] is allocated in Group 1 and B[3] is in Group 2. In case the "DD" is an even number, then B[3] is allocated in Group 1 and B[2] is in Group 2.
- (2) In case "MM" is an odd number, then B[4] is allocated in Group 1 and B[5] is in Group 2. In case the "MM" is an even number, then B[5] is allocated in Group 1 and B[4] is in Group 2.
- (3) In case "YYYY" is an odd number, then B[6] is allocated in Group 1 and B[7] is in Group 2. In case the "YYYY" is an even number, then B[7] is allocated in Group 1 and B[6] is in Group 2.

(c) The disc ID is also divided into Group 1 and Group 2 on the basis of time (HH MM SS) when the project was created, which is one of the system content storage ID. Each byte of the disc ID is allocated as follows:

- (1) In case "HH" is an odd number, then B[8] is allocated in Group 1 and B[9] is in Group 2. In case the "HH" is an even number, then B[9] is allocated in Group 1 and B[8] is in Group 2.
- (2) In case "MM" is an odd number, then B[10] is allocated in Group 1 and B[11] is in Group 2. In case the "MM" is an even number, then B[11] is

allocated in Group 1 and B[10] is in Group 2.

(3) In case "SS" is an odd number, then B[12] is allocated in Group 1 and B[13] is in Group 2. In case the "SS" is an even number, then B[13] is allocated in Group 1 and B[12] is in Group 2.

5 (d) The steps (b) and (c) are repeated until all the bytes of the disc ID are divided into either Group 1 or Group 2.

3. Calculate a hash code for each disc ID byte group such that getting H1 for Group 1 and H2 for Group 2 (step S502). Configurations of H1 and H2 are shown in FIG. 6b.

10 4. Append H1 to major PID such as a fingerprint template to construct a new block of data and calculate its hash code of H3 (step S503).

5. Use the Blowfish algorithm to encrypt H3 by H2 so as to be a first encryption key (step S504). Then, the first encryption key for the content key is obtained.

15 In reference to FIG. 7, a process for generating a second encryption key that encrypts secret data is described in detail next.

FIG. 7 is a flowchart showing a process for generating a second encryption key that encrypts secret data in 16 bytes according to the embodiment of the present invention.

20 A second encryption key for encrypting 16-byte secret data is generated as follows.

1. Assume that system content storage ID such as disc ID is in "L" bytes.

2. Divide the L-byte disc ID into two groups such as Group 1 and Group 2 (step S601).

25 Hereupon, each step of dividing disc ID is described in detail next with reference to FIGs. 6a and 6b.

FIG. 6a is a data structure of 16-byte disc ID to be divided into two groups, and FIG. 6b is a data structure of the 16-byte disc ID being divided into two

groups, wherein "L" byte disc ID is defined as 16 byte disc ID.

(a) Two least significant bytes, that is, B[0] and B[1] are always allocated in Group 1, and two most significant bytes, that is, B[L-1] and B[L-2] are always allocated in Group 2. In FIG. 6a, the disc ID is in 16 bytes. Consequently, two
5 most significant bytes B[L-1] and B[L-2] are illustrated as B[14] and B[15] respectively in FIG. 6a.

(b) The disc ID is divided into Group 1 and Group 2 on the basis of date (DD MM YYYY) when the project was created, which is one of the system content storage ID. As shown in FIG. 6b, each byte of the disc ID is allocated as
10 follows:

(4) In case "DD" is an odd number, then B[2] is allocated in Group 1 and B[3] is in Group 2. In case the "DD" is an even number, then B[3] is allocated in Group 1 and B[2] is in Group 2.

(5) In case "MM" is an odd number, then B[4] is allocated in Group 1 and B[5] is in Group 2. In case the "MM" is an even number, then B[5] is allocated in Group 1 and B[4] is in Group 2.
15

(6) In case "YYYY" is an odd number, then B[6] is allocated in Group 1 and B[7] is in Group 2. In case the "YYYY" is an even number, then B[7] is allocated in Group 1 and B[6] is in Group 2.

(c) The disc ID is also divided into Group 1 and Group 2 on the basis of time (HH MM SS) when the project was created, which is one of the system content storage ID. Each byte of the disc ID is allocated as follows:

(4) In case "HH" is an odd number, then B[8] is allocated in Group 1 and B[9] is in Group 2. In case the "HH" is an even number, then B[9] is allocated in Group 1 and B[8] is in Group 2.
25

(5) In case "MM" is an odd number, then B[10] is allocated in Group 1 and B[11] is in Group 2. In case the "MM" is an even number, then B[11] is allocated in Group 1 and B[10] is in Group 2.

(6) In case "SS" is an odd number, then B[12] is allocated in Group 1 and B[13] is in Group 2. In case the "SS" is an even number, then B[13] is allocated in Group 1 and B[12] is in Group 2.

(d) The steps (b) and (c) are repeated until all the bytes of the disc ID are
5 divided into either Group 1 or Group 2.

3. Calculate a hash code for each disc ID byte group such that getting H1 for Group 1 and H2 for Group 2 (step S602). Configurations of H1 and H2 are shown in FIG. 6b.

4. Append H1 to PID storage ID such as RFID ID to construct a new block
10 of data and append the new block of data to the disc ID (step S603). In case RFID ID is not available, append H1 directly to the disc ID.

5. Calculate a hash code of the new block of data so as to obtain H3 (step S604).

6. Set a number of value to the time (HH MM SS), that is, "nVal = HH +
15 MM + SS". If an owner's name is in "k" bytes, then do $Name[i] = (Name[i] + nVal) \% 256$, where "i" = 0, 1, ..., (k-1) (step S605).

7. Append H3 to the new name data constructed as mentioned above, and then calculate its hash code of H4 (step S606).

8. Use the Blowfish algorithm to encrypt H4 by H2 so as to obtain the
20 second encryption key (step S607).

9. The second encryption key for the secret data is obtained.

A data format of secret data to be stored in a PID storage device is described in detail next.

The secret data contains following fields:

- 25
1. System ID: This is a unique ID code to indicate that data following the system ID field is generated by the system according to the present invention and conforms to the data format.
 2. System content storage ID such as disc ID: This is a unique GUID,

which is randomly generated by the system according to the present invention for each digital content storage medium such as a CD disc and a DVD disc.

3. Title: This is assigned for the digital content storage medium while
5 creating the project. It is non-secure information and able to be shown
 upon scanning through a PID storage reader such as an RFID reader.
4. Owner's name: This is assigned while creating the project. It is
 non-secure information and able to be shown upon scanning through
 the PID storage reader. This is a field must be filled by either the user
10 or the system, wherein the system obtains the data from the database
 1c in the "PID database and management server" 1.
5. Date: This is a date when the digital content storage medium was
 created. It is non-secure information and able to be shown upon
 scanning through the PID storage reader. A format of the date is
15 "DDMMYY".
6. Time: This is approximate time when the project was created. A format
 of the time is "HHMMSS".
7. Comment: This is added while creating the digital content storage
 medium. It is non-secure information and able to be shown upon
20 scanning through the PID storage reader.
8. Content key (protected): This is encrypted by a first encryption key that
 is derived from information of user's PID such as a fingerprint template,
 the system content storage ID and the date & time when the project
 was created.
- 25 9. Major PID data length such as a major fingerprint data length: This is
 a field of showing data length of the major fingerprint.
10. Major PID information such as major fingerprint template: This is
 data of the major fingerprint template.

11. Minor PID flag such as minor fingerprint flag: This is a flag for showing how many minor PID such as minor fingerprints are supported and how to support the minor PID locally or remotely.

12. Minor PID ID (minor fingerprint ID) or ID of minor PID (minor fingerprint template): If the minor PID is stored in the database 1c of the "PID database and management server" 1, there exists corresponding minor PID ID in 16 bytes or 128 bits that is a hash code of the minor PID. If the minor PID is stored locally, there exists minor PID data length being followed by the corresponding minor PID data.

10 In reference to FIGs. 8 – 9b, a data structure of the minor PID flag being stored in a PID storage device and a data structure of storing minor PID ID and minor PID data are described in detail next.

FIG. 8 shows a data structure of a minor PID flag supporting four minor PID, that is, four minor user's PID according to the embodiment of the present invention.

As mentioned above, the minor PID flag is a flag for showing how many minor PID are supported and how to support the minor PID locally or remotely. In other words, the minor PID flag shows that the PID storage device can support how many minor users.

20 In FIG. 8, one byte of minor PID flag is divided into two areas, that is, "minor PID enabling bits" and "minor PID location bits". They support four minor PID: "PID0"; "PID1"; "PID2" and "PID3" respectively. In the following description, each of the four minor PID is generically referred to as "PIDi".

With respect to the minor PID enabling bits, in case "PIDi" is equal to "1" (one), the minor PID is enabled. In other words, the minor user is allowed to access a protected digital content. On the contrary, in case the "PIDi" is equal to "0" (zero), the minor PID is disabled. In other words, the minor user is not allowed to access the protected digital content.

With respect to the minor PID location bits, in case "PIDI" is equal to "1" (one), the minor PID is remotely stored. In other words, the minor PID is stored in a PID database provided in the "PID database and management server" 1 in case the minor PID is enabled.

5 On the contrary, in case the "PIDI" is equal to "0" (zero), the minor PID is locally stored. In other words, the minor PID is stored locally in a PID storage device provided in the "content playback client" 3 in case the minor PID is enabled.

FIG. 9a shows a structure of the minor PID storing identification (ID) of the 4 minor PID and an IP address and a port number of a server according to the embodiment of the present invention, and FIG. 9b shows a structure of minor PID storing data length and data of the 4 minor PID according to the embodiment of the present invention.

In FIG. 9a, each ID of four minor PID is composed of 128 bits if the minor PID is enabled, and headed by 4 bytes of server IP and 2 bytes of port number of the "PID database and management server" 1.

As shown in FIG. 9b, each of the four minor PID data is headed by 2 bytes of minor PID data length in case the minor PID is stored locally.

In reference to FIG. 10, a content decryption filter driver is described in details next.

FIG. 10 is a block diagram showing a configuration of the content decryption filter driver according to the embodiment of the present invention.

The "content decryption filter driver" 3e in the "content playback client" 3 provides kernel layer decryption of a protected digital content or encrypted digital content stored in a digital content storage medium such as a CD disc and a DVD disc. Consequently, a user can directly access to the protected digital content as a normal file. The kernel layer is a layer placed on the top of a file system driver stack, that is, a "digital content storage medium file system

device stack" 31 and decrypts data packets passing through the layer.

The "content decryption filter driver" 3e is designed to be loaded when an OS (operating system) is booted up. As shown in FIG. 10, the "content decryption filter driver" 3e is composed of three device objects, that is, a "control
5 device object (CDO)" 3e1, a "monitoring filter device object (Monitoring FDO)" 3e2 and a decrypting filter device object (Decrypting FDO)" 3e3. Each of the CDO 3e1, the "Monitoring FDO" 3e2 and the "Decrypting FDO" 3e3 is detailed next.

The CDO 3e1 is a permanent module of the "content decryption filter
10 driver" 3e and exists whenever the "content decryption filter driver" 3e is loaded. Major tasks of the CDO 3e1 are to communicate with the "content playback client" 3, to listen for a signal from the "Monitoring FDO" 3e2 and to control loading of the "Decrypting FDO" 3e3.

Further, the CDO 3e1 is only one communication channel between the
15 "content decryption filter driver" 3e and the "content playback client" 3. The "content playback client" 3 sends control information to the CDO 3e1, wherein the control information is a content key for decrypting a encrypted digital content, a command for cleaning the system cache and memory mapped files.

On the other hand, the content playback client" 3 registers signal events
20 at the CDO 3e1 so as to receive information coming from the "content decryption filter driver" 3e such as a mount notification.

Furthermore, the CDO 3e1 is also responsible for cleaning the system cache when the CDO 3e1 is informed of that a "digital content storage medium volume device" is unmounted.

25 The "Monitoring FDO" 3e2 is also a permanent module of the "content decryption filter driver" 3e and connected with the "digital content storage medium file system device stack" 31 when the "content decryption filter drive" 3e initiates the "Monitoring FDO" 3e2.

Further, the "Monitoring FDO" 3e2 acts as a hook for a mounting IRP (I/O Request Packet). The mounting IRP is generated when the "digital content storage medium volume device" is mounted and mostly when a CD or DVD disc is inserted into the "digital content storage reader" 3a. The "Monitoring FDO" 3e2 notifies the CDO 3e1 immediately after intercepting the mounting IRP being successfully returned. Then, the CDO 3e1 request the "content playback client" 3 for the content key for decrypting the encrypted digital content. When the CDO 3e1 receives the content key from the "content playback client" 3, the CDO 3e1 creates the "Decrypting FDO" 3e3 and attaches the mounting IRP to a newly mounted "digital content storage medium file system device stack" 31.

Similarly, when the CD or DVD disc is unmounted, the "Monitoring FDO" 3e2 signals an event to the CDO 3e1 to clear the system cache and deletes the memory mapped files.

The "Decrypting FDO" 3e3 recovers the encrypted digital content by using the content key. The content key is loaded on-demand basis by the CDO 3e1. Once the content key is loaded, the "Decrypting FDO" 3e3 intercepts packets, which are created whenever the user wants to read data such as a file and directory from a file system. When the "Decrypting FDO" 3e3 receives a reading IRP, the "Decrypting FDO" 3e3 checks a type of reading operation. In other words, the "Decrypting FDO" 3e3 checks whether the reading IRP is file content reading or directory list reading. In case the reading IRP is a file content reading IRP, the data to be read are decrypted. The decrypted data are passed through higher layers to a corresponding user's application.

Further, the "Decrypting FDO" 3e3 is detached from a "digital content storage medium volume device object stack" 32 and destroyed when the "digital content storage medium volume device" is unmounted.

As mentioned above, according to the present invention, the system

according to the embodiment of the present invention uses unique biometric information inherent in a particular person such as a fingerprint and an iris as unique personal identification (PID) to identify the particular person from other persons as well as generating related security information and the latest
5 storage technologies such as RFID tags, SD memory cards, USB flash memories as a PID storage device to store the unique PID and security information.

Further, according to another aspect of the present invention, the system can realize protection over a digital content such as document, an audiovisual
10 content and an image, while the digital content is distributed through a digital contents storage medium such as a CD disc, a DVD disc and a USB flash memory by implementing unique biometric information inherent in a particular person such as a fingerprint and an iris as unique personal identification (PID) to identify the particular person from other persons.

15 While the invention has been described above with reference to a specific embodiment thereof, it is apparent that many changes, modifications and variations in configuration, materials and the arrangement of equipment and devices can be made without departing from the invention concept disclosed herein.

20 In addition thereto, it will be apparent to those skilled in the art that various modifications and variations could be made in the method field in the present invention without departing from the scope of the invention.

WHAT IS CLAIMED IS

1. A system for securely storing and distributing a digital content comprising:
 - (a) a personal identification (PID) database and management server including,
 - (1) a local PID register module for registering user's PID information locally,
 - (2) a remote PID register server module for registering user's PID information remotely,
 - (3) a database for securely storing a plurality of user's PID information and for providing network access through its TCP/IP access module,
 - (4) a database manager for managing the plurality of user's PID information so as to be inserted or deleted, and
 - (5) a PID reader for scanning user's PID information locally so as to register the user's PID information to the database through the local PID register module;
 - (b) a content protection and distribution server including,
 - (1) a content protector for encrypting a digital content by using a content key being generated on the basis of user's PID and PID storage device ID and system generated random user ID,
 - (2) a PID database file for storing user's PID information,
 - (3) a digital content storage writer for writing the encrypted digital content to a digital content storage medium,
 - (4) a PID reader for scanning user's PID information to register or verify the user's PID information,
 - (5) a PID storage reader & writer for writing data to or reading data from an PID storage device to be accompanied by the digital

content storage medium, and

(6) a local PID register module for registering user's PID information locally;

(c) a content playback client for verifying user's PID information and regenerating the content key and encryption keys and decrypting the encrypted digital content stored in the digital content storage medium, the content playback client including,

(1) a digital content storage reader for reading the encrypted digital content from the digital content storage medium to be supplied,

(2) a PID reader for scanning user's PID information to register or verify the user's PID information as a preferred user,

(3) a PID storage reader & writer for reading data from or writing data to the PID storage device to be provide together with the digital content storage medium,

(4) a remote PID register module for registering the user's PID information remotely, and

(5) a content decryption filter driver; and

(d) a network for providing network connection among the PID database and management server, the content protection and distribution server and the content playback client,

the system for securely storing and distributing a digital content further characterized in that a digital content is encrypted and securely stored in a digital content storage medium and distributed to a preferred user through the digital content storage medium, and

that the PID database and management server stores and manages a plurality of user's PID information registered locally or remotely, and

that the content protection and distribution server encrypts a digital content and writes the encrypted digital content in a digital content storage

medium, and

that the content protection and distribution server creates security information and stores the security information in an PID storage device, and

that the content decryption filter driver is allocated between a file system layer and a digital content storage reader driver layer for passing and interpreting messages and data transferred between a file system and the digital content storage reader, and

that the encrypted digital content is decrypted on the fly by the content key being regenerated on the basis of the user's PID information and the PID storage device ID and the system generated random user ID.

2. A process for securely storing and distributing a digital content to be implemented in the system for securely storing and distributing a digital content as claimed in claim 1,

the process comprising the steps of:

creating a new project

defining an encryption strategy for initializing the content protector in the content protection and distribution server so as to project distribution of a digital content;

adding a digital content to the newly created project as a preferred digital content, wherein the digital content enables to be imported through a digital content storage medium, network file sharing or FTP (file transfer protocol);

selecting a preferred user from the database in the PID database and management server or the PID database file in the content protection and distribution server;

generating randomly a content key for encrypting the preferred digital content by the content protection and distribution server;

generating a first encryption key for encrypting the content key by the

content protection and distribution server on the basis of the preferred user's PID information, a unique GUID (globally unique identifier) and related other information;

generating a second encryption key for encrypting the secret data by the content protection and distribution server on the basis of PID storage device ID, the unique GUID and related other information;

encrypting the preferred digital content by the content key in the content protection and distribution server;

encrypting the content key by the first encryption key in the content protection and distribution server;

encrypting the secret data by the content protection and distribution server;

writing the encrypted preferred digital content to a digital content storage medium by using the digital content storage writer in the content protection and distribution server;

writing the encrypted content key and the encrypted secret data to the PID storage device together with the unique GUID, related other information by using the PID storage reader & writer in the content protection and distribution server; and

distributing the digital content storage medium and the PID storage device to the preferred user,

the process further characterized in that user's PID information of the preferred user is previously registered into the database or the PID database file by the preferred user through either the local PID register modules in the PID database and management server and in the content protection and distribution server or the remote PID register module in the content playback client, and

that the user's PID information is transmitted from the remote PID register

module in the content playback client to the remote PID register server module in the PID database and management server through a pre-established SSL (secure socket layer) link, and

that the preferred user's PID information is read out as secret data from the database or the PID database file.

3. A process for recovering and viewing a preferred digital content in a distributed digital content storage medium storing the preferred digital content in a content playback client to be implemented in the system for securely storing and distributing a digital content as claimed in claim 1,

the process comprising the steps of:

registering PID information of a user to be a preferred user by scanning his PID information through an PID reader in the content playback client when receiving a distributed digital content storage medium;

reading encrypted secret data, an encrypted content key and other information from a distributed PID storage device by using a PID storage reader & writer to in the content playback client;

regenerating the second encryption key for encrypting the secret data on the basis of PID storage device ID, the unique GUID and related other information;

decrypting the encrypted secret data to recover the preferred user's PID information stored in the distributed PID storage device;

verifying the user's PID information registered by scanning in the step of registering PID information whether or not the use's PID information matches with the preferred user's PID information;

regenerating the first encryption key for encrypting the content key in case the user is verified as the preferred user or a legal user, wherein the content playback client rejects the user in case the user is judged as an illegal user;

decrypting the encrypted content key and passing the decrypted content key to the content decryption filter driver in the content playback client; and

reading the preferred digital content by decrypting the encrypted digital content in real-time through the content decryption filter driver.

4. A process for sharing an encrypted preferred digital content stored in a distributed digital content storage medium to be implemented in the system for securely storing and distributing a digital content as claimed in claim 1, wherein a preferred user or a legal user defined as a major user can share a preferred digital content with another user to be defined as a minor user,

the process comprising the steps of:

adding PID information of another user to be defined as a minor user to the distributed PID storage device so as to be minor PID information by the legal user defined as a major user in accordance with a predefined data format, wherein user's PID of the major user is defined as major PID information, and

wherein the minor PID information is protected by a content key for secret data;

scanning in essentially the minor user's PID information;

verifying the minor user's PID information scanned in the step of scanning in the minor user's PID information whether or not the minor user's PID information matches with the minor PID information added to the PID storage device in the step of adding PID information of the minor user;

recovering the content key by using the major PID information in case the user is verified as the added minor user or a legal minor user, wherein the content playback client rejects the user in case the user is judged as an illegal user;

decrypting the encrypted content key by using the major PID information; and

decrypting the preferred digital content by the content decryption filter driver.

5. A process for transferring ownership or license of a distributed digital content storage medium to be implemented in the system for securely storing and distributing a digital content as claimed in claim 1, wherein a legal user whose PID information is stored in a distributed PID storage device as major PID information can request to transfer ownership or license of a distributed digital content storage medium to another user as a minor user in case the legal user has a right to transfer the ownership or license,

the process comprising the steps of:

scanning in essentially major user's PID information to be authenticated;

scanning in PID information of a minor user so as to be protected as new secret data or new major PID information and to be stored in a distributed PID storage device;

generating a new encryption key for encrypting a content key on the basis of the new major PID information, wherein the content key is re-encrypted by the new encryption key; and

updating all information in the distributed PID storage device on the basis of the new major PID information of the minor user.

6. A process for generating a content key to be implemented in the system for securely storing and distributing a digital content as claimed in claim 1 and the process for securely storing and distributing a digital content as claimed in claim 2,

the process comprising the steps of:

setting a counter "i" to be equal to a byte number of a key length of a content key;

setting a loop counter "j" to "i";
generating a seed for a random number generator;
setting the seed in the random number generator;
generating a random number that falls in [0, 255];
setting an (i - j)th byte of the content key to be the generated random number;
setting "j = (j - 1)"; and
repeating the above steps until "j = (j - 1)" becomes 0 (zero).

7. A process for generating a first encryption key for the content key to be implemented in the system, the processes and the methods as claimed in claims 1 through 5, wherein the unique GUID is assumed as "L" bytes,

the method comprising the steps of:

(a) dividing the unique GUID in "L" bytes into two groups, wherein two least significant bytes (B[0] and B[1]) are always allocated in a group 1, and

wherein two most significant bytes (B[L-1] and B[L-2]) are always allocated in a group 2, and

wherein (L-4) bytes of the unique GUID are allocated in accordance with a date (DD MM YYYY) when the project is created as follows,

(1) allocating a third byte B[2] in the group 1 and a fourth byte B[3] in the group 2 in case the "DD" is an odd number,

(2) allocating the fourth byte B[3] in the group 1 and the third byte B[2] in the group 2 in case the "DD" is an even number,

(3) allocating a fifth byte B[4] in the group 1 and a sixth byte B[5] in the group 2 in case the "MM" is an odd number,

(4) allocating the sixth byte B[5] in the group 1 and the fifth byte B[4] in the group 2 in case the "MM" is an even number,

(5) allocating a seventh byte B[6] in the group 1 and a eighth byte B[7]

in the group 2 in case the "YYYY" is an odd number, and

- (6) allocating the eighth byte B[7] in the group 1 and the seventh byte B[6] in the group 2 in case the "YYYY" is an even number, and

further wherein remaining 6 bytes of the unique GUID are allocated in accordance with time (HH MM SS) when the project is created as follows,

- (1) allocating a ninth byte B[8] in the group 1 and a tenth byte B[9] in the group 2 in case the "HH" is an odd number,
- (2) allocating the tenth byte B[9] in the group 1 and the ninth byte B[8] in the group 2 in case the "HH" is an even number,
- (3) allocating an eleventh byte B[10] in the group 1 and a twelfth byte B[11] in the group 2 in case the "MM" is an odd number,
- (4) allocating the twelfth byte B[11] in the group 1 and the eleventh byte B[10] in the group 2 in case the "MM" is an even number,
- (5) allocating a thirteenth byte B[12] in the group 1 and a fourteenth byte B[13] in the group 2 in case the "SS" is an odd number, and
- (6) allocating the fourteenth byte B[13] in the group 1 and the thirteenth byte B[12] in the group 2 in case the "SS" is an even number;

(b) repeating the above step (a) until all the bytes in the system content ID are divided into either group1 or group 2;

(c) calculating a hash code for each group and obtaining H1 for the group 1 and H2 for the group 2;

(d) appending the H1 to a master PID information so as to construct a new block of data and to calculate its hash code of H3;

(e) encrypting the H3 by the H2 so as to be the first encryption key by using the Blowfish algorithm; and

(f) obtaining the encryption key for encrypting the content key.

8. A process for generating the second encryption key for encrypting secret data to be implemented in the system, the processes as claimed in claims 1 through 5, wherein the unique GUID is assumed to be in "L" bytes,

the process comprising the steps of:

(a) dividing the unique GUID in "L" bytes into two groups, wherein two least significant bytes (B[0] and B[1]) are always allocated in a group 1, and

wherein two most significant bytes (B[L-1] and B[L-2]) are always allocated in a group 2, and

wherein 12 bytes of the unique GUID are allocated in accordance with a date (DD MM YYYY) when the project is created as follows,

(1) allocating a third byte B[2] in the group 1 and a fourth byte B[3] in the group 2 in case the "DD" is an odd number,

(2) allocating the fourth byte B[3] in the group 1 and the third byte B[2] in the group 2 in case the "DD" is an even number,

(3) allocating a fifth byte B[4] in the group 1 and a sixth byte B[5] in the group 2 in case the "MM" is an odd number,

(4) allocating the sixth byte B[5] in the group 1 and the fifth byte B[4] in the group 2 in case the "MM" is an even number,

(5) allocating a seventh byte B[6] in the group 1 and a eighth byte B[7] in the group 2 in case the "YYYY" is an odd number, and

(6) allocating the eighth byte B[7] in the group 1 and the seventh byte B[6] in the group 2 in case the "YYYY" is an even number, and

further wherein remaining 6 bytes of the unique GUID are allocated in accordance with time (HH MM SS) when the project is created as follows,

(1) allocating a ninth byte B[8] in the group 1 and a tenth byte B[9] in the group 2 in case the "HH" is an odd number,

(2) allocating the tenth byte B[9] in the group 1 and the ninth byte B[8] in the group 2 in case the "HH" is an even number,

- (3) allocating an eleventh byte B[10] in the group 1 and a twelfth byte B[11] in the group 2 in case the "MM" is an odd number,
 - (4) allocating the twelfth byte B[11] in the group 1 and the eleventh byte B[10] in the group 2 in case the "MM" is an even number,
 - (5) allocating a thirteenth byte B[12] in the group 1 and a fourteenth byte B[13] in the group 2 in case the "SS" is an odd number, and
 - (6) allocating the fourteenth byte B[13] in the group 1 and the thirteenth byte B[12] in the group 2 in case the "SS" is an even number;
- (b) repeating the above step (a) until all the bytes in the system content ID are divided into either group1 or group 2;
- (c) calculating a hash code for each group and obtaining H1 for the group 1 and H2 for the group 2;
- (d) appending the H1 to PID storage device ID so as to construct a new block of data and appending the new block of data to the unique GUID;
- (e) calculating a hash code for the new block of data as H3;
- (f) setting "nVal = HH + MM + SS", and then in case an owner's name is in "k" bytes, performing "Name[i] = (Name[1] + nVal)%256", wherein i = 1, 2, ..., and (k-1);
- (g) appending the H3 to new name data and calculating its hash code of H4;
- (h) encrypting the H4 by the H2 so as to be the second encryption key by using the Blowfish algorithm; and
- (i) obtaining "K" as the second encryption key for encrypting secret data.

9. A data format of secret data being stored in a PID storage device to be implemented in the system and the processes as claimed in claims 1 through 5, the data format comprising:

system ID that is a unique ID code to be generated by the system;

system content storage ID that is a unique GUID to be randomly generated by the system for each digital content storage medium;

a title that is a title of a digital content storage medium;

an owner's name assigned during creation of the project, wherein the owner's name must be filled by either a user or the system by obtaining data from a database;

a date that is a date when the digital content storage medium is created, wherein the date is formatted in "DDMMYYYY";

time that is time when the digital content storage medium is created, wherein the time is formatted in "HHMMSS";

a comment added while creating the digital content storage medium, wherein the comment is non-secure information and shown by scanning through a PID storage reader;

a content key that is encrypted by another key;

major PID data length showing a data length of major PID information;

major PID information that is data of major PID;

a minor PID flag indicating how many minor PID information are supported and how to support the minor PID information locally or remotely; and

minor PID ID, wherein the minor PID ID is a hash code of the minor PID information or the minor PID data in case the minor PID information is stored in the database of the PID database and management server.

10. A data structure of the minor PID flag as claimed in claim 9, wherein the data structure comprises 4 bits of minor PID enabling bits and 4 bits of minor PID location bits.

11. A data structure for storing minor PID ID and minor PID data as claimed in claim 9, the data structure comprising:

server IP address in 4 bytes;

port number in 2 bytes; and

PID ID in 128 bits, wherein each PID ID exists in case each PID is enabled.

12. A content decryption filter driver to be implemented in the system for securely storing and distributing a digital content as claimed in claim 1, wherein the content decryption filter driver is an upper layer placed at the top of a file system driver stack and decrypts a data packet passing through the content decryption filter driver, and

wherein the content decryption filter driver provides kernel layer decryption of an encrypted digital content stored in a digital content storage medium, so that a user can directly access the encrypted digital content as a normal file, and

wherein the content decryption filter driver is designed to be loaded when an OS (operating system) is booted up,

the content decryption filter driver comprising:

a control device object (CDO) for communicating with the content playback client;

a monitoring filter device object (monitoring FDO), wherein the monitoring FDO is a permanent module of the content decryption filter driver; and

a decrypting filter device object (decrypting FDO) for decrypting an encrypted digital content.