RFID ASSISTED MEDIA PROTECTION, TRACKING AND LIFE CYCLE MANAGEMENT

A data storage apparatus (132), e.g., optical disc, flash memory or hard disk is provided with an RFID tag (136) for controlling its use. The RFID tag stores biometric authentication data (235-255) of a user, in addition to information (210) for decrypting encrypted data on the data storage apparatus. A digital representation (305-320) of a biometric input of the user is obtained, and a message digest function is used to obtain the biometric authentication data. Subsequently, biometric authentication data from a new biometric input is compared to the stored data. If the data matches, the decryption information (210) is read from the RFID tag, and use to decrypt the encrypted data. Only a portion of the data on the data storage apparatus, such as headers (1102) of frames (1100), need be encrypted. The RFID tag may also store purchase validity data (212) added at a point of sale.

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

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
RFID ASSISTED MEDIA PROTECTION, TRACKING AND LIFE CYCLE MANAGEMENT

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. provisional patent application no. 60/670,195, filed April 11, 2005, entitled "RFID assisted media protection, tracking and life cycle management", and incorporated herein by reference.

BACKGROUND

Field of the Invention

[0002] The present invention relates to using RFID technology to control access to data on a data storage media.

Description of the Related Art

[0003] Unauthorized use of data from data storage media such as optical discs has become widespread due to the ease in which digital data can be copied. As a result, content owners are continually seeking viable solutions for safeguarding their copyrighted assets and reigning in the scale of infringement as much as possible. Various techniques have been employed to address this problem but have met with limited success. For example, some systems securely deliver data to the user via the Internet using a digital rights management scheme of the content owner. These systems typically require the user to provide personal information in exchange for access to the data. Other systems take an extreme approach in allowing a user to play an optical disc on only one playing device – the playing device on which the optical disc is first used. Such systems are inconvenient because the protection scheme is tied to one player. For example, if the first player is in the home, the user cannot use a second player at another location in the user’s car, or at a friend’s home, for example. Generally, these existing approaches have been difficult for the content owners to manage, and have drawn the ire of many users because they impose significant restrictions and, in some cases, intrude on the user’s privacy. Further, many of the technologies can be circumvented with minimal effort.
[0004] Improved techniques are needed for controlling access to data.

SUMMARY

[0005] The technology herein, roughly described, provides a data storage apparatus and an apparatus for reading digital data stored on the data storage apparatus.

[0006] A user-friendly, in-situ, copy protection system for digital media is provided using radio frequency identification (RFID) technology for encryption, authentication and verification. RFID tags can be affixed to data storage apparatuses such as optical discs, e.g., media discs such as CDs and DVDs, as well as flash memories and hard disks, for instance. Advantageously, data stored in the RFID tag can be used for both controlling access to the data storage apparatus as well as during the manufacturing, packaging, storage and shipping of the data storage apparatus. The use of RFID tags facilitates a superior inventory control system in stores, libraries and clubs, for instance, as well as facilitating the development of other more accurate business processes such as automated borrowing systems, theft prevention systems and the like. Thus, the existing capabilities which are provided by RFID tags can be expanded to include copy protection functionality. The approach is secure and inexpensive to implement. It provides the genuine user with the liberty to use the data storage apparatus anytime, anywhere, on any RFID and biometric reader enabled device, while at the same time safeguarding the interests of the content copyright owner.

[0007] In one aspect, a data storage apparatus includes a data storage media encoded with digital data, where at least a portion of the digital data is encrypted. Additionally, at least one RFID tag is carried by the data storage media. The RFID tag stores various types of information, including information for decrypting the portion of the digital data which is encrypted, and biometric authentication data of a user. For example, the biometric authentication data may be obtained from a biometric input of the user, such as a fingerprint. To reduce the computational load in the authentication process, the biometric input can be converted to biometric authentication data which consumes much less data than a digital representation of the biometric input itself. The RFID tag can also store other types of information, including information indicating whether the data storage apparatus is being read for the first time, information which authorizes limited reading of the data without
requiring authentication of the user using the biometric authentication data, and a password which is set by the user.

[0008] In another aspect, an apparatus for controlling access to digital data includes a biometric device for receiving a biometric input from a user in a setup procedure of a data storage apparatus. A control is responsive to the biometric device for generating biometric authentication data based on the biometric input, and an RFID tag writer is responsive to the control for writing the biometric authentication data to at least one RFID tag which is carried by a data storage apparatus. The control can generate the biometric authentication data as a message digest which is obtained from a digital representation of the biometric input, for instance. The user is authenticated when the user provides a subsequent biometric input to the biometric input device. To achieve this, the control instructs an RFID tag reader to read the biometric authentication data which was written to the RFID tag, and compares the read biometric authentication data to biometric authentication data which is generated based on the subsequent biometric input. An interface can also be provided for prompting the user to input a password, where the RFID tag writer writes the password to the RFID tag.

[0009] A related method for controlling access to digital data includes receiving a biometric input from a user, generating biometric authentication data based on the biometric input, and writing the biometric authentication data to at least one RFID tag which is carried by a data storage apparatus.

[0010] In yet another aspect, an apparatus for controlling access to digital data includes a biometric device for receiving a biometric input from a user, and a control, responsive to the biometric device, for generating biometric authentication data based on the biometric input. Additionally, an RFID tag reader is responsive to the control for reading biometric authentication data stored in at least one RFID tag which is carried by a data storage apparatus. The control compares the generated biometric authentication data to the read biometric authentication data to determine if there is a match. Upon determining that there is a match, the control instructs the RFID tag reader to read information from the RFID tag for decrypting encrypted digital data encoded on the data storage apparatus. The control
can also authorize reading of the data storage apparatus when a password input by the user matches a password stored in the RFID tag.

[0011] A related method for controlling access to digital data includes receiving a biometric input from a user, generating biometric authentication data based on the biometric input, reading biometric authentication data stored in at least one RFID tag which is carried by a data storage apparatus, and comparing the generated biometric authentication data to the read biometric authentication data to determine if there is a match.

[0012] In yet another embodiment, an apparatus for controlling access to digital data includes a user interface for receiving purchase validity data which is input by a user, an RFID tag reader for reading purchase validity data stored in at least one RFID tag which is carried by a data storage apparatus, and at least one control, responsive to the user interface and the RFID tag reader, for determining whether the user has made a valid purchase of the data storage apparatus based on the input purchase validity data and the stored purchase validity data. For example, the input purchase validity data may be a purchase validity code, and the stored purchase validity data may be a hash of the purchase validity code, in which case the at least one control calculates a hash from the input purchase validity data for comparison with the stored hash to determine if the user has made a valid purchase of the data storage apparatus.

[0013] Or, the input purchase validity data may be a purchase validity code, and the stored purchase validity data may also be a purchase validity code, in which case the at least one control compares the input and stored purchase validity codes to determine if the user has made a valid purchase of the data storage apparatus.

[0014] A related method for controlling access to digital data includes receiving purchase validity data which is input by a user, reading purchase validity data stored in at least one RFID tag which is carried by a data storage apparatus, and responsive to the receiving and the reading, determining whether the user has made a valid purchase of the data storage apparatus based on the input purchase validity data and the stored purchase validity data.
[0015] In yet another embodiment, an apparatus for controlling access to digital data includes a transaction processor at a point of sale location for processing a transaction for delivering a data storage apparatus to a user, and for initiating delivery of purchase validity data to the user, and an RFID writer at the point of sale location, responsive to the transaction processor, for writing purchase validity data to at least one RFID tag which is carried by the data storage apparatus. Only a valid purchase will provide access to the content, thereby dissuading people from stealing.

[0016] A related method for controlling access to digital data includes processing, at a point of sale location, a transaction for delivering a data storage apparatus to a user, responsive to the processing, writing purchase validity data to at least one RFID tag which is carried by the data storage apparatus, and initiating delivery of purchase validity data to the user.

[0017] In yet another embodiment, a data storage apparatus includes a data storage media encoded with digital data, and at least one RFID tag carried by the data storage media, the at least one RFID tag storing purchase validity data which is written at a point of sale of the data storage apparatus.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] FIG. 1 depicts an apparatus for controlling access to digital data on a data storage apparatus.

[0019] FIG. 2a depicts a data structure of an RFID tag.

[0020] FIG. 2b depicts a process for obtain a seed hash value which is stored in the data structure of FIG. 2a.

[0021] FIG. 3 depicts a data structure with digital representations of biometric inputs.

[0022] FIG. 4 depicts a process for authorizing use of the data on a data storage apparatus, including a setup procedure.
FIG. 5 depicts a biometric authentication process.

FIG. 6 depicts an alternative biometric authentication process.

FIG. 7 depicts an alternative setup procedure.

FIG. 8 depicts a password setup procedure to allow sharing of a data processing apparatus without requiring biometric authentication of a user.

FIG. 9 depicts a process for reading data from a data storage apparatus.

FIG. 10 depicts an alternative process for reading data from a data storage apparatus.

FIG. 11 depicts a frame of data on a data storage apparatus.

FIG. 12 depicts bytes of data in sectors and frames of a data storage apparatus.

FIG. 13 depicts the encoding of purchase validity data on a data storage apparatus at a point of sale.

FIG. 14 depicts a process for providing purchase validity data on a data storage apparatus at a point of sale.

FIG. 15 depicts a process for verifying purchase validity data on a data storage apparatus at a reading apparatus.

DETAILED DESCRIPTION

FIG. 1 depicts an apparatus for controlling access to digital data on a data storage apparatus. Various types of data storage apparatuses which may be used include optical discs, including CDs and DVD, as well as flash memories and hard disks. The example reading apparatus 100 is a player for a data storage apparatus 131 which includes a data storage media 132 in the form of an optical disc. However, the concepts disclosed herein are applicable as well to other types of data storage media. The player can be a standalone device or a general purpose computer, e.g., a PC or laptop, for instance.
Moreover, the data carried by the data storage apparatus 132 can be of any type, including audio, video, computer software or other data. Various encoding techniques are well known for such data storage apparatuses. For example, audio data is commonly encoded in the Red Book or MP3 format, while video data is commonly encoded in the MPEG-2 format. Other data such as computer software, including multimedia applications and databases, can be stored in a data CD such as a CD-ROM, for instance, using a data format which includes sectors, frames and bytes of data.

[0035] The data storage apparatus 131, which is removably received in a holder 130, includes a central hole 134 about which an RFID tag 136 is affixed. The RFID tag may use high frequency technology based on the ISO 15693 protocol, for example. RFID tags are desirable because they store data permanently yet require no battery power. In one possible approach, an RFID tag is provided as an adhesive inlay which is affixed to a surface of an optical disc. However, various other configurations are possible. For example, the RFID tag can be secured within the interior of the optical disc. The RFID tag should be positioned in a location which does not interfere with the normal use of the data storage apparatus. For example, for an optical disc, the RFID tag should not interfere with the movement of a laser which is used to read and/or write to the disc. For a flash memory or hard disk, the RFID tag can be positioned within the circuitry or packaging in an unobtrusive manner. Additionally, it is possible to use more than one RFID tag to store the different types of data mentioned in connection with FIG. 2a. For instance, two RFID tags may be used, one on each side of the data storage apparatus.

[0036] A data storage media reader 120 includes a laser that is positioned to read the microscopic pits in a spiral track in the data storage media 132. An RFID tag reader/writer 146, or transceiver, is positioned to read data from, and write data to, the RFID tag 136. For example, the RFID tag reader/writer 146 can be embedded in the reading apparatus 100, positioned just above the RFID tag 136 as indicated. The RFID tag 136 and the hole 134 are shown with dashed lines to indicate they are below the RFID tag reader/writer 146. The RFID tag reader/writer 146 may use a protocol for reading and writing which satisfies the byte/block writing requirements of the tag air interface protocol. This protocol can cover the command structure and the structure of the payload for each command, that is, the
position of the memory block in the tag memory, the number of bits/words/bytes (unit memory), and the order of units.

[0037] The data storage media reader 120 and the RFID tag reader/writer 146 communicate with a control 142 which runs client software 144 to provide the desired functionality. The client software 144 can be an embedded software module in the reading apparatus 100 which supervises the chain of events dealing with the authentication, verification and decryption of the content on the data storage apparatus 131 using biometric authentication data and hash values which are stored in the RFID tag, as described further below. In one possible approach, the control 142 and associated non-volatile memory 148 and volatile or working memory 149, are provided on a daughterboard 140, while a data decoder 150, which provides an output signal to one or more output ports 160, is provided on a motherboard. By embedding the RFID tag reader/writer 146 and the biometric reader 105 along with the supplementary memory 106 and client software 144 into the reading apparatus 100, the additional functionality can be economically added to existing devices without requiring extensive redesign. It is feasible to add these modules into any standard media player, such as a CD or DVD player, with some modifications. For example, it is possible to incorporate the new components on the same circuit board on which the existing decoder 150 is provided, and/or to incorporate the functionality of the control 142 into a common control which is also used by the decoder 150. A further option is to provide multiple controls, such as a control for handling the data storage media reader 120 and a control for handling the RFID tag reader/writer 146.

[0038] A user interface 110 includes switches/keypad 112 and a display/touch screen 114, in one possible design. The display 114 can be an economical two- or four-line LCD display, for instance, or a touch screen (e.g., 3.5” x 2.5”). A keypad is not needed if a touch screen is used, as the touch screen can provide a virtual keypad. The user interface 110 can be used to provide information to the user, such as a message indicating that access to the data storage apparatus 131 has been granted or denied, as well as receiving information from the user, such as a password, or a command to activate a loan feature, as described further below. A biometric reader 105 is used to obtain a biometric input from the user, such as a fingerprint, palm print, eye scan, voice sample or the like. Fingerprint readers, for
example, are advantageous because they are compact and economical, and the technology is relatively mature, reliable and user-friendly. The biometric reader 105 provides a biometric input from the user to the control 142 where it is used to control access to the data storage apparatus 131, as discussed further below. The biometric reader 105 can include its own onboard non-volatile memory 106, such as flash/EEPROM, to store the biometric input. The biometric input can be stored additionally, or alternatively, in the non-volatile memory 148.

[0039] FIG. 2a depicts a data structure of an RFID tag. Standard RFID tags which store 256 bytes of data can be used, in one approach. The RFID tag can be partitioned into a format similar to that shown. In one approach, 128-bit slots may be reserved for each of the data entries. The example data structure 200 includes a tag identifier 205 which can be a unique 16, 24 or 64-bit identifier that is assigned to the RFID tag at the time it is manufactured, based on the type of RFID tag that is used. The tag identifier can be used for tracking, inventory management and the like. During the media preparation stage, a seed hash value 210 is generated based on a secret key, the unique tag identifier, and/or descriptive text of the content.

[0040] FIG. 2b depicts a process for obtain a seed hash value which is stored in the data structure of FIG. 2a. At step 260, the unique RFID tag identifier is read from the RFID tag. Additionally, descriptive text of the media content can be read from the data storage apparatus. For instance, the descriptive text can be a title, such as a CD album title, an artist's name, a movie name or the like. At step 265, a one way hash function is applied to a concatenation of the tag identifier, the descriptive text and a secret key to obtain the seed hash value 210, in one possible approach. In another approach, the one way hash function can be applied to one or more of the RFID tag identifier, the descriptive text, and the secret key. The secret key can be randomized while generating the seed hash value. At step 270, the seed hash value is written to the data structure of the RFID tag and locked, thereby rendering it tamper proof. At step 275, the content to be stored on the data storage apparatus is at least partly encrypted using the seed hash value and, at step 280, the encrypted and unencrypted content is written to the data storage apparatus.
Referring again to FIG. 2a, at entry 212, a purchase validity hash may be used to verify that the data storage apparatus was purchased legitimately and not stolen, as discussed below in connection with FIGs. 13-15. A first use flag 215 indicates whether the data storage apparatus is being played or otherwise accessed for the first time, e.g., by the end user. A loan flag 220 indicates whether the user has entered a command to allow the data storage apparatus to be used in a limited manner by another user without requiring the other user to be authenticated. For example, when set, the loan flag 220 can authorize a one time use by another user. This allows the genuine user and owner of the data storage apparatus to loan it after selecting the loan flag. This process will add the valid biometric authentication data from the stored biometric authentication data on the RFID tag to the loan flag area on the RFID tag, thereby allowing the borrower to use the data storage apparatus for one time, for example. In another approach, the loan flag can store additional information to allow multiple uses. The flag is then decremented after each use until no further uses are allowed. A password flag/password 225 can be provided to allow an authenticated user to select a password by which access to the data storage apparatus is granted to other users. For example, a teacher may grant access to a number of students via the password. The number of accesses which each student is granted via the password can be limited.

Entries 230, 235, 240 and 245 in the data structure 200 store biometric authentication data of different users. The number of biometric authentication data entries can be one or more. The maximum number can be set based on the storage capacity of the RFID tag or other criteria. In one approach, by providing space for four biometric authentication data entries, four different users, such as members of a family, can access the data storage apparatus. Biometric authentication data can be obtained in different ways. In one approach, the biometric authentication data entries are obtained by calculating a message digest of a digital representation of a biometric input using a one-way hash function. See steps 425-435 in Fig. 4. In another possible approach, the biometric authentication data entries provide a digital representation, encrypted or not, of a biometric input. The digital representation can be a fingerprint image, for example, when the biometric input is a fingerprint. This approach is feasible if space permits in the RFID tag. It is also possible to store the biometric authentication data in one or more separate RFID
tags. As described further below, the biometric authentication data can be used to authenticate a user and control access to a data storage apparatus. In authenticating a user, a comparison based on message digests requires a small computational load because a comparison of relatively short bit strings is performed. A comparison based on digital representations of biometric inputs requires a larger computational load, such as when pattern matching techniques are used.

[0043] FIG. 3 depicts a data structure with digital representations of biometric inputs. The data structure 300 may store one or more digital representations of biometric inputs, such as fingerprint images. The data structure in this case is essentially a memory map of fingerprints of the authorized users of the data storage apparatus. In the example provided, four images are stored in data locations 305, 310, 315 and 320. As mentioned, the digital representations can be stored in non-volatile memories 106 and/or 148 (FIG. 1). A fingerprint image can be compressed using Wavelet Scalar Quantization, for example, as it provides good compression and is machine readable. Generally, when multiple digital representations are stored, the same amount of data can be allocated for each. Design factors include determining whether lossy or lossless image storage is used, whether monochrome or color images are stored, and the size of the biometric reader. The digital representations provide biometric authentication data that can be used in a secondary or additional authentication procedure, for instance.

[0044] FIG. 4 depicts a process for authorizing use of the data on a data storage apparatus, including a setup procedure. At step 400, a user attempts to access a data storage apparatus using a reading apparatus such as a CD/DVD player, portable flash memory device player, such as an MP3 player, portable computing device such as a PDA or cell phone, or a general purpose computer such as a laptop or workstation. For example, the user may load a CD or DVD into a player, or power on a device with a flash memory or hard disk. At step 405, the reading apparatus reads the one or more RFID tags on the data storage apparatus. Based on the first use flag 215, the client software 144 in the reading apparatus determines if the data storage apparatus is being read for the first time, at step 410. In this case, a setup procedure is started, at step 415. Note that the setup procedure can be entered at other times. For example, a setup procedure may be started for the first n
uses where, e.g., n=4 or some other number of allowed authorized users. A purchase validity procedure can also be carried out, at step 412, as described in FIG. 15, before the setup procedure. If the purchase validity procedure passes, the setup procedure begins, at step 415. If the purchase validity procedure fails, after one or more attempts, reading of the data storage apparatus is not authorized, at step 490.

[0045] In the setup procedure, at step 420, the user is prompted to provide a biometric input via the biometric reader 105. For example, the user may simply place his or her fingertip on a fingerprint reader. At step 425, a digital representation of the biometric input is generated. For example, this may be image data of a fingerprint. The image data can be provided in any desired format. Optionally, the digital representations of biometric inputs of one or more users can be stored in non-volatile memory 106 and/or 148. At step 430, a message digest is calculated from the digital representation. A message digest function is an algorithm, such as a one-way hash function, that converts variable messages to a unique fixed length value, which is the message digest. For example, the MD5 algorithm reduces a message to a 128-bit digest. SHA1 is another one-way hash function which may be used. The same input always produces the same output from any particular algorithm. Thus, the message digest can be obtained by applying a one-way hash function to the digital representation. At step 435, the message digest is used as the biometric authentication data. Alternatively, the message digest could be processed in further steps, such as one or more encryption steps, to obtain the biometric authentication data.

[0046] At step 440, the biometric authentication data is written to, and locked on, the RFID tag. The first use flag, entry 215 in FIG. 2a, can be set, at step 442. This flag will be used to signal a reading apparatus to inquire for a fingerprint scan or other biometric input every time a subsequent play attempt is made. At step 445, the client software authorizes the reading of data from the data storage apparatus and, at step 450, displays an authorization message on the user interface 110, such as the display 114, to inform the user that he or she is now able to proceed and access the data storage apparatus. Or, the reading apparatus may simply enter a play mode. For example, a CD or DVD player can read and play an optical disc to provide an audio/video output. The security feature here is that authorized persons will be allowed to use the data storage apparatus at anytime on any
RFID and biometric enabled reading apparatus. The data storage apparatus will play only when the scanned fingerprint matches the ones stored, for instance, as determined by the biometric authentication data.

[0047] At block 455, the user interface may prompt the user to enter a password setup procedure, if so desired, described further in connection with FIG. 8. The password setup procedure allows the authenticated user to enable other users to access the data storage apparatus by entering a password, without the need to be biometrically authenticated, as discussed in connection with the password flag/password 225 of FIG. 2a.

[0048] At step 410, if the first use flag 215 indicates that the data storage apparatus is not being used for the first time, and the loan flag 220 is set at step 460, limited reading of the data storage apparatus can be authorized (step 465). For example, as discussed in connection with FIG. 2a, the loan flag 220 can indicate whether the user has entered a command to allow the data storage apparatus to be used in a limited manner by another user without requiring the other user to be authenticated. The loan flag can indicate, e.g., that one use is allowed. In this way, an authorized user can allow a friend or family member to access a data storage apparatus once, such as to play a movie on a DVD. After the allowed access, further attempts to access the data storage apparatus require the user to be biometrically authenticated. Thus, at step 445, reading of the data storage apparatus is authorized, and, at step 450, an authorization message is displayed.

[0049] At step 460, if the loan flag is not set, and at decision step 470, the password flag (entry 225 in FIG. 2a) is set, the user is prompted to enter a password at step 475. At step 480, the password stored in the RFID tag is read, and the two passwords are compared at step 485. If they match, reading of the data storage apparatus is authorized at step 445, and an authorization message is displayed at step 450. If the passwords do not match, reading of the data storage apparatus is not authorized at step 490, and a non-authorization message is displayed on the user interface at step 495. For example, the user may be informed that the password is incorrect and given one or two additional chances to enter the correct password.
[0050] If the password flag is not set at decision step 470, a biometric authentication process is initiated at step 498 as discussed in connection with FIG. 5 and 6. The biometric authentication process can be the default process for accessing the data storage apparatus after the setup process has occurred, and in the absence of a loan or password authorization process being configured.

[0051] FIG. 5 depicts a biometric authentication process. In this approach, a user is biometrically authenticated by comparing biometric authentication data. At step 500, the biometric authentication process begins. At step 505, the user is prompted to provide a biometric input. At step 510, a digital representation of the biometric input is generated, at step 515, a message digest is calculated from the digital representation. At step 520, the message digest is used as the biometric authentication data. At step 525, the biometric authentication data which was previously stored in the RFID during the setup procedure is read and compared to the generated biometric authentication data, at step 530, to determine if there is a match. If there is a match, reading of the data storage apparatus is authorized at step 545, and an authorization message is displayed at step 550. Optionally, the user can be prompted to enter the password setup procedure at this time, at step 555. If the biometric authentication data do not match, at step 530, reading of the data storage apparatus is not authorized at step 535, and a non-authorization message is displayed on the user interface at step 540.

[0052] FIG. 6 depicts an alternative biometric authentication process. In this approach, a user is biometrically authenticated by comparing digital representations of biometric inputs. At step 600, the alternative biometric authentication process begins. At step 605, the user is prompted to provide a biometric input. At step 610, a digital representation of the biometric input is generated, and at step 615, the digital representation which was previously stored in the RFID during the setup procedure is read and compared to the generated digital representation, at step 620, to determine if there is a match. If there is a match, reading of the data storage apparatus is authorized at step 635, and an authorization message is displayed at step 640. Optionally, the user can be prompted to enter the password setup procedure at this time, at step 645. If the digital representations do not
match, at step 620, reading of the data storage apparatus is not authorized at step 630, and a non-authorization message is displayed on the user interface at step 630.

[0053] FIG. 7 depicts an alternative setup procedure. In this approach, the biometric authentication data includes a digital representation of a biometric input. Thus, a user can subsequently be authorized to access the data storage apparatus based on a comparison of digital representations of biometric inputs. Appropriate matching algorithms, such as pattern matching algorithms, can be used to determine when two digital representations are sufficiently close so as to indicate, with a given degree of confidence, that they came from the same user. As mentioned, this approach, requires a higher computational load than the matching of message digests, but is a feasible alternative. The alternative setup procedure begins at step 700. At step 705, the user is prompted to provide a biometric input. At step 710, a digital representation of the biometric input is generated. At step 715, the digital representation is written to, and locked on, the RFID tag. The first use flag, entry 215 in FIG. 2a, can be set, at step 720. Reading of the data storage apparatus is then authorized at step 725, and an authorization message is displayed at step 730. At block 735, the user interface may prompt the user to enter a password setup procedure, if so desired, described further in connection with FIG. 8.

[0054] FIG. 8 depicts a password setup procedure to allow sharing of a data processing apparatus without requiring biometric authentication of a user. As mentioned previously, the RFID tag on the data storage apparatus can be configured to allow access with a password. This can be useful in various scenarios, such as where a teacher provides instructional materials on multiple copies of a data storage apparatus, such as an instructional video, and provides a password to students to allow access to the content. At step 800, a user command is received via the user interface to enter the password setup procedure and, at step 805, the password setup procedure begins. The password setup procedure can be entered in any convenient way. For example, the user interface can prompt the user to provide a command to enter the password setup procedure. The user interface can use a touch screen display, e.g., display 114, or keypad 112 for this purpose. At step 810, the user is prompted to enter the password and, at step 815, a password flag and
the password are written to the RFID tag. See, e.g., entry 225 in FIG. 2a. The password flag can indicate that a password is in effect.

[0055] FIG. 9 depicts a process for reading data from a data storage apparatus. Once a user has been authorized to access a data storage apparatus, reading of the data storage apparatus can begin, at step 900. As mentioned, all or a portion of the data on the data storage apparatus can be encrypted using the seed hash value. In particular, for audio and/or video data on a CD or DVD, the loss of several frames of data may result in dropouts in the reproduced signal, but the loss usually does not render the data useless. In such cases, it is advantageous to encrypt specific portions of the data which are necessary for decoding other portions. For instance, the encrypted portions can include meta data such as frame headers which are needed to decode the payload data, e.g., audio and/or video samples, in the frames. Similar sections from different popular file formats can be chosen. Selective encryption of data such as digital media files on the data storage apparatus avoids taxing the reading apparatus / playback system 100 compared to a case where all of the data on the data storage apparatus is encrypted and therefore needs to be decrypted to be read. The security feature provided here is that there will be associated authentication of the unique tag id and the seed hash value, and the content will not play on players without the hash value, as the content will have to be decrypted. Furthermore, by having the RFID tag store information for decrypting the data, the data storage apparatus is self contained and includes the information necessary to decrypt and read its data.

[0056] At step 905, decryption information, such as the seed hash value from entry 210 in FIG. 2a, is read from the RFID tag. At step 910, frames of data are read from the data storage apparatus. For example, the frames may include audio and/or video data on a CD or DVD. Referring also to FIG. 11, a frame 1100 can include an encrypted header portion or other meta data 1102 and an unencrypted payload portion 1104. The frames may also be considered to be data blocks. The header portions typically include information, e.g., meta data, needed for decoding the payload portions, which may include audio and video samples, for instance. For example, with the MPEG Audio Layer 3 (MP3) audio coding format, header information includes frame synchronization bits, MPEG audio version identifier, MPEG layer identifier, a protection bit indicating whether a checksum follows the
header, a bit rate index identifying a lookup table used to specify the bit rate for the MPEG version and layer, and an identification of the sampling rate frequency as determined by a lookup table. Meta data can also be provided as side information. For instance, with the MP3 audio coding format, side information can include information concerning which Huffman table to use during the Huffman decoding process.

[0057] At step 915, the frames are buffered, e.g., in the volatile memory 149 of FIG. 1. Thus, a number of frames may be stored in the buffer at a given time. At step 920, for each frame, meta data such as the header portion is decrypted using the decryption information to obtain decrypted meta data. At step 925, the frames with the decrypted headers and unencrypted payloads are provided to the conventional decoder 150 (FIG. 1) to be decoded to provide an output signal at step 930. Thus, the encrypted part of the content is decrypted, and the resulting data stream is pipelined to the decoder 150 from the control 142.

[0058] FIG. 10 depicts an alternative process for reading data from a data storage apparatus. Data such as computer software, including multimedia applications and databases, can be stored in a data CD such as a CD-ROM, for instance, using a data format which includes sectors, frames and bytes of data. For instance, a frame may have 33 bytes, while a sector contains 98 frames, and holds 98×24 = 2352 bytes. Further, a standard 74 min CD includes 333,000 sectors. For software stored on a data CD, it is only necessary to protect a small number of bytes through encryption, e.g., one or more bytes, to control access to the software. This is true because the software can be rendered useless, or its integrity otherwise compromised, if only a small number of bytes are not properly read from the data CD. In such cases, encrypted data location information can be stored by the control 142, such as in the non-volatile memory 148, and used to identify the locations on the data storage apparatus. For example, the encrypted data location information can identify the location of encrypted bytes of data based on sector, frame and/or byte locations. Thus, the encrypted data location information, which can be provided in the form of a table, for instance, can identify, e.g., a sector, between 1 and 333,000, a frame between 1 and 98, and a byte position between 1 and 24. Further, data regarding the number of data blocks encrypted, e.g., sectors, frames or bytes, can be added as a CRC checksum for reliability.
[0059] FIG. 12 depicts bytes of data in sectors and frames of a data storage apparatus. A number of example sectors include sector n-1 (1200), sector n (1210), and sector n+1 (1250). Example sector n (1210) includes a number of frames including frame j-1 (1220), frame j (1230) and frame j+1 (1240). Example frame j (1230) includes example byte position i-1 (1232), byte position i (1234) and byte position i+1 (1236). Bytes positions 1232 and 1236 are unencrypted, while byte position 1234 is encrypted, in one possible example. It is also possible to have multiple encrypted bytes together, such as by encrypting a frame. Thus, the location information for byte position i is (sector n, frame j, byte position i). If frame j is encrypted, the location information is (sector n, frame j). The location information can therefore include a sector location and a frame and/or byte location.

[0060] At step 1000, reading of the data storage apparatus begins. At step 1005, the decryption information, such as the seed hash value, is read from the RFID tag. At step 1010, The control reads the encrypted data location information from the non-volatile memory 148. The encrypted data location information identifies locations on the data storage apparatus in which the encrypted data is found, such as by using a table. The locations of the data which are encrypted can be predetermined, e.g., at the time of manufacture, and randomly dispersed on the data storage apparatus among other locations in which unencrypted portions of the data are stored, so that only the control 142 knows where the encrypted data is located. In another approach, all of the data is encrypted and there is no need for the location information. In yet another approach, the location information can be provided on the RFID tag.

[0061] At step 1015, the encrypted and unencrypted bytes of data are read from the data storage apparatus, and buffered, at step 1020. At step 1025, the encrypted bytes, frames or other data storage units, are located using the location information. At step 1030, the encrypted bytes are decrypted using the decryption information read from the RFID tag to obtain decrypted bytes. At step 1035, the decrypted and unencrypted bytes are provided to the conventional decoder 150 to be decoded to provide an output signal at step 1040.
FIG. 13 depicts the encoding of purchase validity data on a data storage apparatus at a point of sale. A goal of this approach is to provide purchase validity data on the RFID tag at a point of sale of the data processing apparatus, and to require the user to subsequently enter the purchase validity data into the reading apparatus in order to access the data storage apparatus. In this manner, only authorized users who have possession of the purchase validity data can gain access. Unauthorized users, such as those who have stolen the data storage apparatus or received unauthorized copies, will not be able to gain access. Moreover, the purchase validity data may be used by itself, without the biometric authentication data discussed previously, or it may be used in conjunction with the biometric authentication data as an additional layer of security.

A user may purchase a data storage apparatus at a point of sale location which can include, among many possibilities, a retail store, a self-service machine such as a kiosk, or an e-commerce location, such as a facility of a web-based e-commerce site which receives an order for the data storage apparatus from the user via the user's web browser. In each case, a data storage apparatus is delivered to the user, whether the delivery occurs immediately, such as when a transaction is conducted in a retail store or using a self-service machine, or at a later date, such as when the data storage apparatus is delivered by mail or other delivery service.

A transaction processor 1300 can be a checkout station at a retail store, a processor in a server that processes web-based orders, or a processor in a self-service machine, for instance. One or more transaction processors may be used. For example, in a retail store, the user can select a data storage apparatus from a store display and proceed to a checkout station. Once payment is tendered by the user, the transaction processor 1300 instructs an RFID tag writer 1310 to write purchase validity data to an RFID tag 1322 on the data storage apparatus 1320. RFID tag readers/writers are expected to be common place at point-of-sale locations in the near future due to the adoption of RFID technology by the retail sector. The purchase validity data can be any type of data. For example, the purchase validity data can be a purchase validity hash which is based on the store number or any token specified by the store, and/or a date-time stamp of purchase. The purchase validity hash can be calculated from a purchase validity code. This hash is written to, and locked
on, the RFID tag during purchase by the store personnel using an apparatus which has an embedded RFID reader/writer, for instance.

[0065] The purchase validity data is provided to the user 1350, such as by hardcopy 1340 (e.g., receipt) via a printer 1330, or by e-mail via an e-mail/web server 1360, which communicates with a user computer 1370, for instance. The purchase validity data could be provided via other communication techniques as well, such as text messaging by cell phone, automated telephone response system, and so forth. The first time the user attempts to access the data storage apparatus using the reading apparatus 1370, the user is prompted to enter the purchase validity data. The user can then manually enter the purchase validity data into the reading apparatus 1380 via a user interface such as a touch screen keypad. In another option, the reading apparatus 1380 is in a network with the user computer 1370, and receives the purchase validity data automatically, without manual entry by the user, using any available communication technique.

[0066] Once the user successfully enters the purchase validity data, the reading apparatus 1380 can immediately grant access to the data storage apparatus. Or, it can proceed to request a biometric input, as an additional layer of security. The user may be given a few chances to correctly enter the purchase validity data, such as three attempts. If the purchase validity data is not successfully entered, the data storage apparatus 1320 can be rendered unplayable by adding a “void” token to the RFID tag and locking it. The void token can be added to the purchase validity data segment 212 of the RFID tag data structure (FIG. 2a), for instance.

[0067] FIG. 14 depicts a process for providing purchase validity data on a data storage apparatus at a point of sale. At step 1400, purchase validity data such as a purchase validity code is generated at the point of sale. For example, the purchase validity code may be a string of numbers, similar to a password. At step 1410, a hash of the code can be calculated at the point of sale as another form of purchase validity data. The code can be processed by a hash algorithm such as a one way function to obtain the purchase validity hash. At step 1420, the purchase validity hash is written to the RFID tag of the data storage apparatus at the point of sale. At step 1430, the purchase validity code is provided to the user.
FIG. 15 depicts a process for verifying purchase validity data on a data storage apparatus at a reading apparatus. At step 1500, at the time of first use, as determined by first use flag 215, for instance, the user inputs the purchase validity code to the reading apparatus via a user interface. At step 1510, the reading apparatus calculates a hash from the code using the same hashing algorithm that was used at the transaction processor 1300. At step 1520, the reading apparatus reads the purchase validity hash which was previously stored in the RFID tag. At step 1530, the reading apparatus compares the calculated and stored purchase validity hashes to determine if they match. In another approach, the code can be stored in the RFID tag and compared to the input code. If there is a match, a setup procedure can continue, at step 1550, as discussed previously, or reading of the data storage apparatus can be immediately authorized. If there is not a match, after providing a suitable number of retries in which the user can re-enter the code, the reading apparatus writes a void token to the RFID tag and locks it into place, rendering the data storage apparatus unusable, at step 1540. To avoid having an authorized user lose access permanently to the locked data storage apparatus, the user may be allowed to exchange the data storage apparatus at the point of sale for a new one, upon providing an acceptable proof of purchase.

The foregoing detailed description of the technology herein has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the technology to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. The described embodiments were chosen in order to best explain the principles of the technology and its practical application to thereby enable others skilled in the art to best utilize the technology in various embodiments and with various modifications as are suited to the particular use contemplated. It is intended that the scope of the technology be defined by the claims appended hereto.
 We claim:

1. A data storage apparatus, comprising:
   a data storage media encoded with digital data, at least a portion of the digital data being encrypted;
   at least one RFID tag carried by the data storage media, the at least one RFID tag storing information for decrypting the at least a portion of the digital data which is encrypted, and storing biometric authentication data of a user.

2. The data storage apparatus of claim 1, wherein:
   the biometric authentication data is obtained from a biometric input of the user.

3. The data storage apparatus of claim 1, wherein:
   the biometric authentication data comprises a message digest which is obtained from a digital representation of a biometric input of the user.

4. The data storage apparatus of claim 1, wherein:
   the biometric authentication data comprises a digital representation of a biometric input of the user.

5. The data storage apparatus of claim 1, wherein:
   the information for decrypting comprises a seed hash value which is based on at least one of a unique RFID tag identifier of the at least one RFID tag, a secret key, and descriptive text associated with the digital data.

6. The data storage apparatus of claim 1, wherein:
   the digital data comprises encrypted meta data and associated unencrypted payload data, where the encrypted meta data carries information needed for decoding the associated unencrypted payload data.
7. The data storage apparatus of claim 6, wherein:
the digital data comprises frames of data in which the encrypted meta data is
provided in a header portion of the frames, and the associated unencrypted payload data is
provided in a payload portion of the frames.

8. The data storage apparatus of claim 1, wherein:
the at least one RFID tag stores a password which is set by the user.

9. The data storage apparatus of claim 1, wherein:
the at least one RFID tag stores information which authorizes limited reading of the
digital data without requiring authentication of the user using the biometric authentication
data.

10. The data storage apparatus of claim 1, wherein:
the data storage media comprises a flash memory.

11. The data storage apparatus of claim 1, wherein:
the data storage media comprises a hard disk.

12. The data storage apparatus of claim 1, wherein:
the data storage media comprises an optical disc.

13. The data storage apparatus of claim 1, wherein:
the at least a portion of the digital data which is encrypted is stored in predetermined
locations identified by a sector location and at least one of a frame location and a byte
location.

14. The data storage apparatus of claim 13, wherein:
the predetermined locations are randomly dispersed among other locations in which
unencrypted portions of the digital data are stored.
15. The data storage apparatus of claim 1, wherein:
the at least one RFID tag stores information indicating whether the data storage
apparatus is being read for the first time.

16. An apparatus for controlling access to digital data, comprising:
a biometric device for receiving a biometric input from a user;
at least one control, responsive to the biometric device, for generating biometric
authentication data based on the biometric input; and
an RFID tag writer, responsive to the at least one control, for writing the biometric
authentication data to at least one RFID tag which is carried by a data storage apparatus.

17. The apparatus for controlling access to digital data of claim 16, further
comprising:
an RFID tag reader for reading the at least one RFID tag;
wherein the at least one control authenticates the user, when the user provides a
subsequent biometric input to the biometric input device, by instructing the RFID tag reader
to read the biometric authentication data which was written to the at least one RFID tag, and
comparing the read biometric authentication data to biometric authentication data which is
generated based on the subsequent biometric input.

18. The apparatus for controlling access to digital data of claim 17, wherein:
the at least one control authorizes reading of digital data encoded on the data storage
apparatus when the compared biometric authentication data match.

19. The apparatus for controlling access to digital data of claim 16, wherein:
the RFID tag writer performs the writing of the biometric authentication data to the
at least one RFID tag when information read from the at least one RFID tag indicates that
the data storage apparatus is being read for the first time.

20. The apparatus for controlling access to digital data of claim 16, further
comprising:
an interface for receiving a password from the user, wherein the RFID tag writer writes the password to the at least one RFID tag.

21. The apparatus for controlling access to digital data of claim 16, wherein:
the at least one control generates the biometric authentication data as a message digest which is obtained from a digital representation of the biometric input.

22. An apparatus for controlling access to digital data, comprising:
a biometric device for receiving a biometric input from a user;
at least one control, responsive to the biometric device, for generating biometric authentication data based on the biometric input; and
an RFID tag reader, responsive to the at least one control, for reading biometric authentication data stored in at least one RFID tag which is carried by a data storage apparatus, the at least one control comparing the generated biometric authentication data to the read biometric authentication data to determine if there is a match.

23. The apparatus for controlling access to digital data of claim 22, wherein:
the at least one control generates the biometric authentication data which is based on the biometric input as a message digest which is obtained from a digital representation of the biometric input.

24. The apparatus for controlling access to digital data of claim 22, wherein:
the at least one control, upon determining that there is a match between the compared biometric authentication data, instructs the RFID tag reader to read information from the at least one RFID tag for decrypting encrypted digital data encoded on the data storage apparatus.

25. The apparatus for controlling access to digital data of claim 24, wherein:
the information for decrypting comprises a seed hash value which is based on at least one of a unique RFID tag identifier of the at least one RFID tag, a secret key, and descriptive text associated with the digital data.
26. The apparatus for controlling access to digital data of claim 24, wherein:
the encrypted digital data comprises encrypted meta data which carries information
needed for decoding associated unencrypted payload data which is encoded on the data
storage apparatus.

27. The apparatus for controlling access to digital data of claim 26, wherein:
the encrypted meta data is provided in a header portion of frames of data, and the
associated unencrypted payload data is provided in a payload portion of the frames.

28. The apparatus for controlling access to digital data of claim 24, wherein:
the at least one control accesses the encrypted digital data from predetermined
locations of the data storage apparatus which are identified by a sector location and at least
one of a frame location and a byte location.

29. The apparatus for controlling access to digital data of claim 28, wherein:
the predetermined locations are randomly dispersed among other locations in which
unencrypted digital data is stored.

30. The apparatus for controlling access to digital data of claim 28, further
comprising:
a non-volatile memory associated with the at least one control for storing
information identifying the predetermined locations.

31. The apparatus for controlling access to digital data of claim 22, further
comprising:
an interface for receiving a password from the user;
wherein the RFID tag reader reads a password stored in the at least one RFID tag,
the at least one control comparing the received password to the read password to determine
if there is a match.
32. The apparatus for controlling access to digital data of claim 31, wherein: the at least one control, upon determining that there is a match between the compared passwords, instructs the RFID tag reader to read information from the at least one RFID tag for decrypting encrypted digital data encoded on the data storage apparatus.

33. An apparatus for controlling access to digital data, comprising: a user interface for receiving purchase validity data which is input by a user; an RFID tag reader for reading purchase validity data stored in at least one RFID tag which is carried by a data storage apparatus; and at least one control, responsive to the user interface and the RFID tag reader, for determining whether the user has made a valid purchase of the data storage apparatus based on the input purchase validity data and the stored purchase validity data.

34. The apparatus for controlling access to digital data of claim 33, wherein: the at least one control allows the user to begin a setup procedure in which the user provides a biometric input if it is determined that the user has made a valid purchase of the data storage apparatus.

35. The apparatus for controlling access to digital data of claim 33, wherein: the at least one control authorizes the user to access the data storage apparatus if it is determined that the user had made a valid purchase of the data storage apparatus.

36. The apparatus for controlling access to digital data of claim 33, wherein: the stored purchase validity data was written to the at least one RFID tag at a point of sale of the data storage apparatus.

37. The apparatus for controlling access to digital data of claim 33, wherein: the input purchase validity data comprises a purchase validity code; the stored purchase validity data comprises a hash of the purchase validity code; and
the at least one control calculates a hash from the input purchase validity data for comparison with the stored hash to determine if the user has made a valid purchase of the data storage apparatus.

38. The apparatus for controlling access to digital data of claim 33, wherein:
the input purchase validity data comprises a purchase validity code;
the stored purchase validity data comprises a purchase validity code; and
the at least one control compares the input and stored purchase validity codes to determine if the user has made a valid purchase of the data storage apparatus.

39. The apparatus for controlling access to digital data of claim 33, further comprising:
an RFID tag writer, responsive to the at least one control, for writing data to the at least one RFID tag which prevents reading of the data storage apparatus, if it is determined that the user has not made a valid purchase of the data storage apparatus.

40. An apparatus for controlling access to digital data, comprising:
at least one transaction processor at a point of sale location for processing a transaction for delivering a data storage apparatus to a user, and for initiating delivery of purchase validity data to the user; and
an RFID writer at the point of sale location, responsive to the at least one transaction processor, for writing purchase validity data to at least one RFID tag which is carried by the data storage apparatus, for use in determining whether the user has made a valid purchase of the data storage apparatus.

41. The apparatus for controlling access to digital data of claim 40, wherein:
the point of sale location comprises at least one of a retail store, a self-service machine, and an e-commerce location.

42. The apparatus for controlling access to digital data of claim 40, wherein:
the purchase validity data delivered to the user comprises a purchase validity code;

and

the purchase validity data written to the at least one RFID tag comprises a hash
which is calculated from the purchase validity code.

43. A data storage apparatus, comprising:
a data storage media encoded with digital data; and
at least one RFID tag carried by the data storage media, the at least one RFID tag
storing purchase validity data which is written at a point of sale of the data storage
apparatus, for use in determining whether a user has made a valid purchase of the data
storage apparatus.

44. The data storage apparatus of claim 43, wherein:
the point of sale location comprises at least one of a retail store, a self-service
machine, and an e-commerce location.

45. A method for controlling access to digital data, comprising:
receiving a biometric input from a user;
generating biometric authentication data based on the biometric input; and
writing the biometric authentication data to at least one RFID tag which is carried by
a data storage apparatus.

46. The method for controlling access to digital data of claim 45, further
comprising:
authenticating the user, when the user provides a subsequent biometric input, by
reading the biometric authentication data which was written to the at least one RFID tag,
and comparing the read biometric authentication data to biometric authentication data which
is generated based on the subsequent biometric input.

47. The method for controlling access to digital data of claim 46, further
comprising:
authorizing reading of digital data encoded on the data storage apparatus when the compared biometric authentication data match.

48. The method for controlling access to digital data of claim 46, wherein:
the biometric authentication data written to the at least one RFID tag is written when information read from the at least one RFID tag indicates that the data storage apparatus is being read for the first time.

49. The method for controlling access to digital data of claim 45, further comprising:
receiving a password from the user; and
writing the password to the at least one RFID tag.

50. The method for controlling access to digital data of claim 45, wherein:
the biometric authentication data is generated as a message digest which is obtained from a digital representation of the biometric input.

51. A method for controlling access to digital data, comprising:
receiving a biometric input from a user;
generating biometric authentication data based on the biometric input;
reading biometric authentication data stored in at least one RFID tag which is carried by a data storage apparatus; and
comparing the generated biometric authentication data to the read biometric authentication data to determine if there is a match.

52. The method for controlling access to digital data of claim 51, wherein:
the biometric authentication data which is based on the biometric input is generated as a message digest which is obtained from a digital representation of the biometric input.

53. The method for controlling access to digital data of claim 51, further comprising:
reading information from the at least one RFID tag for decrypting encrypted digital data encoded on the data storage apparatus, upon determining that there is a match between the compared biometric authentication data.

54. The method for controlling access to digital data of claim 53, wherein:
the information for decrypting comprises a seed hash value which is based on at least one of a unique RFID tag identifier of the at least one RFID tag, a secret key, and descriptive text associated with the digital data.

55. The method for controlling access to digital data of claim 53, wherein:
the encrypted digital data comprises encrypted meta data which carries information needed for decoding associated unencrypted payload data which is encoded on the data storage apparatus.

56. The method for controlling access to digital data of claim 55, wherein:
the encrypted meta data is provided in a header portion of frames of data, and the associated unencrypted payload data is provided in a payload portion of the frames.

57. The method for controlling access to digital data of claim 53, further comprising:
accessing the encrypted digital data from predetermined locations of the data storage apparatus which are identified by a sector location and at least one of a frame location and a byte location.

58. The method for controlling access to digital data of claim 57, wherein:
the predetermined locations are randomly dispersed among other locations in which unencrypted digital data is stored.

59. The method for controlling access to digital data of claim 57, further comprising:
storing information identifying the predetermined locations.
60. The method for controlling access to digital data of claim 51, further comprising:
   receiving a password from the user;
   reading a password stored in the at least one RFID tag; and
   comparing the received password to the read password to determine if there is a
   match.

61. The method for controlling access to digital data of claim 60, further comprising:
   reading information from the at least one RFID tag for decrypting encrypted digital
   data encoded on the data storage apparatus, upon determining that there is a match between
   the compared passwords.

62. A method for controlling access to digital data, comprising:
   receiving purchase validity data which is input by a user;
   reading purchase validity data stored in at least one RFID tag which is carried by a
   data storage apparatus; and
   determining whether the user has made a valid purchase of the data storage
   apparatus based on the input purchase validity data and the stored purchase validity data.

63. The method for controlling access to digital data of claim 62, further comprising:
   allowing the user to begin a setup procedure in which the user provides a biometric
   input if it is determined that the user has made a valid purchase of the data storage
   apparatus.

64. The method for controlling access to digital data of claim 62, further comprising:
   authorizing the user to access the data storage apparatus if it is determined that the
   user had made a valid purchase of the data storage apparatus.
65. The method for controlling access to digital data of claim 62, wherein:
the stored purchase validity data was written to the at least one RFID tag at a point
of sale of the data storage apparatus.

66. The method for controlling access to digital data of claim 62, wherein:
the input purchase validity data comprises a purchase validity code;
the stored purchase validity data comprises a hash of the purchase validity code; and
a hash is calculated from the input purchase validity data for comparison with the
stored hash to determine if the user has made a valid purchase of the data storage apparatus.

67. The method for controlling access to digital data of claim 62, wherein:
the input purchase validity data comprises a purchase validity code;
the stored purchase validity data comprises a purchase validity code; and
the input and stored purchase validity codes are compared to determine if the user
has made a valid purchase of the data storage apparatus.

68. The method for controlling access to digital data of claim 62, further
comprising:
writing data to the at least one RFID tag which prevents reading of the data storage
apparatus, if it is determined that the user has not made a valid purchase of the data storage
apparatus.

69. A method for controlling access to digital data, comprising:
processing, at a point of sale location, a transaction for delivering a data storage
apparatus to a user, and for initiating delivery of purchase validity data to the user; and
responsive to the processing, writing purchase validity data to at least one RFID tag
which is carried by the data storage apparatus, for use in determining whether the user has
made a valid purchase of the data storage apparatus.

70. The method for controlling access to digital data of claim 69, wherein:
the point of sale location comprises at least one of a retail store, a self-service machine, and an e-commerce location.

71. The method for controlling access to digital data of claim 69, wherein:
the purchase validity data delivered to the user comprises a purchase validity code;
and
the purchase validity data written to the at least one RFID tag comprises a hash which is calculated from the purchase validity code.
Fig. 1

Reading apparatus, 100

Biometric reader, 105
Non-volatile memory, 106

User Interface, 110
Switches/keypad, 112
Display/touchscreen, 114

Control, 142
Client software, 144
Non-volatile memory, 148
Volatile memory, 149

Data storage media reader, 120

Data storage media, 132
RFID tag, 136

RFID tag reader/writer, 146

Decoder, 150
Output ports, 160
**Fig. 2a**

- Tag id
- Seed hash value
- Purchase validity hash
- First use flag
- Loan flag
- Password flag/Password
- Biometric authentication data 1
- Biometric authentication data 2
- Biometric authentication data 3
- Biometric authentication data 4

**Fig. 2b**

1. Read RFID tag identifier and descriptive text of the media content
2. Apply one-way hash function to [RFID tag identifier, descriptive text of the media content, secret key] to obtain seed hash value
3. Write seed hash value to RFID tag and lock
4. Encrypt portion of content using seed hash value
5. Write encrypted and unencrypted content to data storage media

**Fig. 3**

- Fingerprint Image 1
- Fingerprint Image 2
- Fingerprint Image 3
- Fingerprint Image 4
User attempts to access data storage apparatus

Read RFID tag

First use? yes

Purchase validity procedure (FIG. 15) fail

Begin setup procedure

Prompt user for biometric input

Generate and store digital representation of biometric input

Calculate message digest from digital representation

Use message digest as biometric authentication data

Write biometric authentication data to RFID tag

Set first use flag

Authorize reading of data storage apparatus

Display authorization message on user interface

Password setup procedure (FIG. 8)

Loan flag set? no

Authorize limited reading of data storage apparatus

Password flag set? yes

Prompt user to enter password

Read password stored in RFID tag

Compare passwords

match

no match

Do not authorize reading of data storage apparatus

Display non-authorization message on user interface

Begin biometric authentication process (FIG. 5 or 6)
Fig. 5

1. Begin biometric authentication process
2. Prompt user for biometric input
3. Generate digital representation of biometric input
4. Calculate message digest from digital representation
5. Use message digest as biometric authentication data
6. Read biometric authentication data stored in RFID tag
   - If match: Compare biometric authentication data
     - If match: Authorize reading of data storage apparatus
       - Display authorization message on user interface
     - If no match: Do not authorize reading of data storage apparatus
       - Display non-authorization message on user interface
   - If no match: Do not authorize reading of data storage apparatus
     - Display non-authorization message on user interface

Password setup procedure (FIG. 8)

Fig. 6

1. Begin alternative biometric authentication process
2. Prompt user for biometric input
3. Generate digital representation of biometric input
4. Read digital representation stored in RFID tag
5. Compare digital representations
   - If match: Display non-authorization message on user interface
   - If no match: Do not authorize reading of data storage apparatus
     - Display non-authorization message on user interface
**Fig. 7**

1. **Begin alternative setup procedure**
2. **Prompt user for biometric input**
3. **Generate digital representation of biometric input**
4. **Write digital representation to RFID tag**
5. **Set first use flag**
6. **Authorize reading of data storage apparatus**
7. **Display authorization message on user interface**

**Password setup procedure (FIG. 8)**

**Fig. 8**

1. **Receive user command via user interface to enter password setup procedure**
2. **Begin password setup procedure**
3. **Prompt user for password via user interface**
4. **Write password flag and password to RFID tag**
Fig. 9

900: Begin reading of data storage apparatus

905: Read decryption information (seed hash value) from RFID tag

910: Read frames of data from data storage apparatus

915: Buffer frames

920: For each frame, decrypt meta data using decryption information to obtain decrypted meta data

925: Provide frames with decrypted headers and unencrypted payloads to decoder

930: Decoder decodes frames and provides output signal

Fig. 10

1000: Begin reading of data storage apparatus

1005: Control reads decryption information (seed hash value) from RFID tag

1010: Control reads encrypted data location information from non-volatile memory

1015: Read encrypted and unencrypted bytes of data from data storage apparatus

1020: Buffer bytes

1025: Locate encrypted bytes using location information

1030: Decrypt the encrypted bytes using decryption information to obtain decrypted bytes

1035: Provide decrypted and unencrypted bytes to decoder

1040: Decoder decodes bytes and provides output signal
Fig. 11

Frame, 1100

Encrypted header or other meta data, 1102

Unencrypted payload, 1104

Fig. 12

Sector n-1, 1200

Frame j-1, 1220

Frame j, 1230

Byte position i-1, Byte position i, Byte position i+1

Unencrypted data, 1232

Encrypted data, 1234

Unencrypted data, 1236

Sector n, 1210

Frame j+1, 1240

Sector n+1, 1250

...
Fig. 13

Transaction processor

RFID tag writer

Purchase validity data receipt

E-mail/web server

User computer

Reading apparatus

Fig. 14

Generate purchase validity code at point of sale

Generate purchase validity hash at point of sale from code

Write purchase validity hash to RFID tag of data storage apparatus at point of sale

Provide purchase validity code to user

Fig. 15

At time of first use, user inputs purchase validity code to reading apparatus via user interface

Reading apparatus generates purchase validity hash from code

Reading apparatus reads purchase validity hash stored on RFID tag

Reading apparatus compares calculated and stored purchase validity hashes

If match, continue setup procedure or authorize reading of data storage apparatus

If no match:

Reading apparatus writes void token to RFID tag. Locks void token.

Continue setup procedure or authorize reading of data storage apparatus