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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 February 2011 (24.02.2011)

PCT

(10) International Publication Number
WO 2011/021113 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/IB2010/052783

(22) International Filing Date:
21 June 2010 (21.06.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/274,715 20 August 2009 (20.08.2009) US

(71) Applicant *(for all designated States except US)*: **NDS LIMITED** [GB/GB]; One London Road, Staines Middlesex TW18 4EX (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ZUCKER, Arnold** [IL/IL]; Rehov Hate'ena10, 73127 Hashmonaim (IL). **SMITH, Perry** [IL/IL]; 107 HaGilgal Street, 98412 Maale Adumim (IL). **TSURIA, Yossi** [IL/IL]; 14 Rabenu Polity Street, 93390 Jerusalem (IL). **CAIN, Harel** [IL/IL]; 2 Esther Hamalka Street, 93627 Jerusalem (IL). **SOLOW, Hillel** [IL/IL]; 67 Shimon Street, 99543 Beit Shemesh (IL). **EPSTEIN, Steve** [IL/IL]; 19 Hazayit Street P.O. Box 464, 73127 Hashmonaim (IL). **ATLOW, Shabtai** [IL/IL]; 36 Rimon Street, 90435 Efrat (IL).

(74) Agents: **ATLOW, Shabtai** et al.; NDS Technologies Israel Limited 5 Shlomo, Halevi Street, 97770 Jerusalem (IL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: ELECTRONIC BOOK SECURITY FEATURES

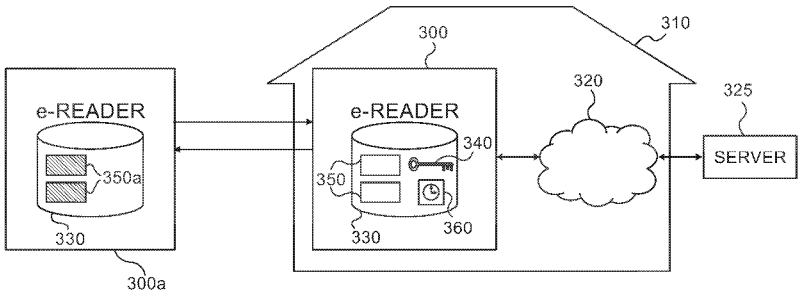

FIG. 3

(57) **Abstract**: A method and system for protecting content on a device are described, the method and system comprising providing a device, the device having at least one encrypted content item, the at least one encrypted content item being consumable only in at least one geographic zone, the device including a communication element and a storage module, the communication element being operative to communicate with a control center, the control center being operative to perform at least one of identifying the device, and tracking the device, establishing a communication session between the device and the control center, verifying that the device is within the one geographic zone, in response to a positive result of the verifying providing a decryption key to the device, thereby enabling decrypting the at least one encrypted content item, decrypting the at least one encrypted content item, thereby producing a decrypted content item, performing at least one of the following storing the decrypted content item in device memory, and outputting the decrypted content item to a device screen, and continuing, on an episodic basis, to verify that the device is within the one geographic zone, performing at least one of the following in response to a negative result of the verifying purging from the device memory the decrypted content item, preventing the device from continuing to operate, clearing the device display screen, and disabling the decryption key. Related hardware, methods and systems are also described.

WO 2011/021113 A1

ELECTRONIC BOOK SECURITY FEATURES

RELATED APPLICATION INFORMATION

The present application claims the benefit of priority from US provisional application number 61/274,715 of Arnold Zucker, et al., filed 20 August 2009, the disclosure of which is hereby incorporated herein by reference.

BACKGROUND OF THE INVENTION

The following references are believed to reflect the state of the art:

US 20050154891 of Skipper;

US 20050258234 of Silverbrook, et al.;

US 7,313,825 to Redlich, et al.;

US 6,094,483 to Fridrich, et al.;

US 5,982,897 to Clark;

US 6,370,629 to Hastings;

US 6,154,172 to Piccionelli;

US 5,887,269 to Brunts;

US 5,842,023 to Tsumura;

US 5,778,304 to Grube;

US 5,757,916 to MacDoran;

US 2009024661 of Kelliher;

JP 2004302913 of Kokuyo Co., Ltd.;

US 6008727 of Want, et al.;

WO 09150394 to De La Rue International, Ltd.;

US 7331725 of Troyansky et al.;

US 6204764 of Maloney;

US 2006197672 of Talamas Jr., et al.;

WO 99/045491 of Nuvomedia Inc.;

WO 98/08344 of The Virtual Press;

US 7,298,851 to Hendricks, et al.;

US 7,299,501 to Hendricks, et al.;

US 7,542,625 to Manber, et al.;

US 20020040472 of Hendricks, et al.;

US 20070201702 of Hendricks, et al;

US 20090171750 of Zhou, et al.; and

US 20090171751 of Zhou, et al.

JP 7036186 of Oriental Composition Industrial Incorporated Company;

US 6,009,116 to Bednarek, et al.;

US 6,724,920 to Berenz, et al.;

US 2008130904 of Whitelaw;

US 7,196.822 to Hu;

US 7,512,978 to Screen, et al.;

US 5,972,546 to Bjelkhagen;

US 2006284411 to Wu;

US 7,505,946 to Chellapilla, et al.;

US 6,195,698 to Lillibridge, et al.;

US 5,197,765 to Mowry, Jr. et al.;

US 5,018,767 to Wicker;

US 5,853,197 to Mowry, Jr. et al.;

US 6,209,922 to Klein;

US 20080019559 of Wang et al.; and

WO 2006/042460 of Liu.

SUMMARY OF THE INVENTION

There is thus provided in accordance with an embodiment of the present invention an e-Reader constructed and operative for protecting content and displaying protected content.

Accordingly, there is thus provided in accordance with an embodiment of the present invention a method for protecting content on a device, the method including providing a device, the device having at least one encrypted content item, the at least one encrypted content item being consumable only in at least one geographic zone, the device including a communication element and a storage module, the communication element being operative to communicate with a control center, the control center being operative to perform at least one of identifying the device, and tracking the device, establishing a communication session between the device and the control center, verifying that the device is within the one geographic zone, in response to a positive result of the verifying providing a decryption key to the device, thereby enabling decrypting the at least one encrypted content item, decrypting the at least one encrypted content item, thereby producing a decrypted content item, performing at least one of the following storing the decrypted content item in device memory, and outputting the decrypted content item to a device screen, and continuing, on an episodic basis, to verify that the device is within the one geographic zone, performing at least one of the following in response to a negative result of the verifying purging from the device memory the decrypted content item, preventing the device from continuing to operate, clearing the device display screen, and disabling the decryption key.

Further in accordance with an embodiment of the present invention the providing the decryption key includes repeatedly downloading the decryption key to the device from the control center, deleting the decryption key from the device immediately after the decryption key is used to decrypt the encrypted content, and requesting a new decryption key from the control center.

Still further in accordance with an embodiment of the present invention the new decryption key includes a different decryption key.

Additionally in accordance with an embodiment of the present invention the providing the decryption key includes flagging the decryption key as having expired immediately after the decryption key is used to decrypt the encrypted content, and receiving a message from the control center to the device, the message including a decryption key renewal message

Moreover in accordance with an embodiment of the present invention the decryption key includes a hash of the received message.

Further in accordance with an embodiment of the present invention the providing the decryption key includes transmitting authentication information from the device to the control center, receiving access to a one-time use decryption key in response to a positive result of an authentication performed at the control center, wherein the authentication information includes proof of freshness, and the decryption key is not stored on the device.

Still further in accordance with an embodiment of the present invention the providing the decryption key includes receiving a second decryption key, receiving an encrypted decryption key, the encrypted decryption key being encrypted according to the second decryption key, and decrypting the encrypted decryption key according to the second decryption key.

Additionally in accordance with an embodiment of the present invention and including receiving an updated version of the second decryption key, and the encrypted decryption key.

Moreover in accordance with an embodiment of the present invention the providing the decryption key includes receiving a content license, the content license being operative to enable decryption of the encrypted content, storing the content license in a device crypto-engine, and utilizing of the content license by a device processor in order to enable decryption of the encrypted content.

Further in accordance with an embodiment of the present invention and further including receiving a disabling message from the control center if the device is removed from the geographic zone, thereby disabling the processor from utilizing the content license.

Still further in accordance with an embodiment of the present invention and further including receiving a signal from the control center if the device is removed from the geographic zone, the signal requiring the device to delete all forms and copies of the decrypted content from the device memory.

Additionally in accordance with an embodiment of the present invention and further including receiving an enabling message from the control center if the device is brought into the geographic zone, thereby enabling the processor to utilize the content license.

Moreover in accordance with an embodiment of the present invention the device includes an e-Reader.

Further in accordance with an embodiment of the present invention the device includes a music player.

Still further in accordance with an embodiment of the present invention the device includes a video player.

Additionally in accordance with an embodiment of the present invention the device includes a memory device.

Moreover in accordance with an embodiment of the present invention the device includes a computer.

Further in accordance with an embodiment of the present invention the device includes a telephone.

Still further in accordance with an embodiment of the present invention the at least one geographic zone includes a single premises.

Additionally in accordance with an embodiment of the present invention the at least one geographic zone includes a region in a premises.

Moreover in accordance with an embodiment of the present invention the content item includes a time bound content item.

There is also provided in accordance with another embodiment of the present invention a system for protecting content on a device, the system including a device having at least one encrypted content item, the at least one encrypted content item being consumable only in at least one geographic zone, the device including a communication element and a storage module, the communication element being operative to communicate with a control center, the

control center being operative to perform at least one of identifying the device, and tracking the device, a communications module operative to establish a communication session between the device and the control center, a verification mechanism operative to verify that the device is within the one geographic zone, in response to a positive result of the verifying at least one of a decryption key is provided to the device, thereby enabling decrypting the at least one encrypted content item, a decryptor decrypts the at least one encrypted content item, thereby producing a decrypted content item, the device is enabled to perform at least one of the following device memory stores the decrypted content item, and the decrypted content item is output to a device screen for displaying, and the verification mechanism continues, on an episodic basis, to verify that the device is within the one geographic zone, in response to a negative result of the verifying performing at least one of the decrypted content item is purged from the device memory, the device is prevented from continuing to operate, the device display screen is cleared clearing, and the decryption key is disabled.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified illustration of a first embodiment of a system for protecting content for display on an electronic reader (e-Reader), constructed and operative in accordance with an embodiment of the present invention;

Fig. 2 is a simplified depiction of an e-Reader of the system of Fig. 1;

Fig. 3 is a simplified illustration of another embodiment of a system for protecting content for display on an e-Reader, constructed and operative in accordance with an embodiment of the present invention;

Fig. 4 is a simplified illustration of yet another embodiment of a system for protecting content for display on an e-Reader;

Fig. 5 is a simplified illustration of one implementation of the e--Reader depicted in Fig. 4;

Fig. 6 is a simplified illustration of still another embodiment of a system for protecting content for display on an e-Reader;

Fig. 7 is a simplified illustration of character elements being displayed on an e-Reader display, within the system of Fig. 6;

Fig. 7A is a simplified illustration of an alternative embodiment of the system depicted in Fig. 7;

Fig. 8 is a simplified illustration of a yet another embodiment of a system for protecting content for display on an e-Reader;

Fig. 9 is a simplified illustration of an alternative of the embodiment of the system of Fig. 8;

Fig. 10 is a simplified illustration of still another embodiment of a system for protecting content for display on an e-Reader; and

Figs. 11 - 15 are simplified flowcharts of preferred methods of operation of the various embodiments described herein.

DETAILED DESCRIPTION OF AN EMBODIMENT

Reference is now made to Fig. 1, which is a simplified illustration of a first embodiment of a system for protecting content for display on an electronic reader (e-Reader), constructed and operative in accordance with an embodiment of the present invention.

It is appreciated that although the specifications and claims refer to an e-Reader, the present invention may be embodied in any appropriate device, such as, but not limited to, music players; video players; memory devices (such embodiments of the present invention may not comprise rendering of content, however); and so forth.

The system of Fig. 1 comprises an e-Reader 100 and a "center" 110. The center 110 comprises some of a processor 120, an encryption key management system 125, a crypto-engine 130, an e-Reader registry 135, a communication interface, and other standard components well known in the art. It is appreciated that the center may be comprised in a plurality of different devices. Additionally, components comprised in the center may be comprised in hardware, software, or a combination of hardware and software, as is well known in the art.

The e-Reader 100 comprises a reading screen 150, manually actuated controls 155, and software and hardware, as is well known in the art. Those skilled in the art will appreciate that instead or in addition to the manually actuated controls 155 the e-Reader 100 reading screen 150 may comprise a touch screen which is operative to serve as a user interface for user command input, as is known in the art. The e-Reader 100 further comprises storage, an encryption key management system, and a crypto-engine.

The e-Reader 100 is in communication with the center 110. Any appropriate communication protocol may be utilized for the communication between the e-Reader 100 and the center 110. For example and without limiting the generality of the foregoing, communication between the e-Reader 100 and the center 110 may be via wireless TCP/IP communication, via wired TCP/IP communication, via a cellular telephone network, or via Bluetooth communication. Additionally, one way communication systems, such as satellite

broadcasting and terrestrial broadcasting systems may provide communication between a remote center 110 and the e-Reader 100.

The center 110 typically has access to a software process running on the e-Reader 100. The process has been granted at least read/write permission for files stored on the e-Reader 100 by an operating system which is resident on the e-Reader 100. By way of abstraction, the center itself may be referred to as having at least read/write permission. Alternatively, files comprised on the e-Reader 100 may be of two categories. Files of a first category comprise files which are controlled by the center 110. For such files, the software process to which the center 110 has access has read/write permission, and the e-Reader 100 has either read permission or no permission at all. Files of a second category comprise files which are controlled by the e-Reader 100 itself. For such files, the e-Reader 100 has read/write permission, and the software process to which the center 110 has access has read permission. A user of the e-Reader 100 has at least read permission for files stored on the e-Reader 100. In some implementations of the present invention the user of the e-Reader 100 also has write permission for files of the second category stored on the e-Reader 100. In some embodiments of the present invention the center 110 only has read permission for files stored on the e-Reader100. However, the center 110 will track and monitor the e-Reader 100, and take steps necessary to protect security breaches involving the e-Reader 100, as described herein.

Reference is now additionally made to Fig. 2, which is a simplified depiction of an e-Reader 100 of the system of Fig. 1. The e-Reader 100 comprises an RFID tag 205, a GPS system, or other marker which can identify and track an object (for ease of description, hereinafter referred to as the RFID tag 205). Typically, the e-Reader 100 is in the possession of a user for use in a place of work or other premises where security is a concern. In such premises, there is typically a human guard posted at each exit. For ease of description, it will be assumed that there is only one exit. At least one function of the human guard is to prevent the removal of items which may cause security risks or leaks, such as content stored on the e-Reader 100 which might comprise content which may cause security risks or leaks. Thus, one of the duties of the human guard is to

prevent the removal of the e-Reader 100 from the premises where security is a concern. Alternatively, a system may be in place whereby the content on the e-Reader 100 is either deleted or rendered not decryptable when an attempt is made to remove the e-Reader 100 from the premises or from a zone of the premises where reading secure content is allowed to a zone of the premises where reading secure content is not allowed (see below).

The e-Reader 100 typically comprises an e-Reader processor 210. The e-Reader processor 210 is operatively connected, as is known in the art, with an e-Reader storage 215, which stores files (such as, but not limited to, files for reading or viewing on the e-Reader 100, operating system files, program files, etc.). The e-Reader processor 210 outputs digital versions of text, video, and so forth, to a graphic digital to analog converter 220, which in turn, outputs analog images on the e-Reader 100 screen 150. The e-Reader processor 210 is further operative to receive and process input from a user interface 225, such as the manually actuated controls 155 (Fig. 1) or the reading screen 150 (Fig. 1), in cases where the reading screen 150 comprises a touch screen which is operative to serve as a user interface, as was noted above.

The e-Reader 100 further comprises an encryption key management system 230 and a crypto-engine 235, corresponding to the encryption key management system 125, and crypto-engine 130 of the center 110. The e-Reader encryption key management system 230 and a crypto-engine 235 are in communication with each other and the e-Reader processor 210. Those skilled in the art will appreciate that the crypto-engine 235 may be comprised within the e-Reader processor 210. The e-Reader processor 210 typically outputs communications to the center via a communication module 240, which is operatively connected to an antenna 245. Depending on protocol and other concerns, such as deciding with which type of marker system (e.g. GPS, RFID, etc.) to communicate, the communication module 240 may intermediate communications signals between the RFID tag 205, the GPS system, or other marker which can identify and track an object and the e-Reader processor 210. The communication module 240 and the RFID tag 205 are typically associated with at least one antenna 245. Those skilled in the art will appreciate that decisions

concerning with which type of marker system to communicate, may involve load balancing, as some communication channels may be busier than others.

Additionally, the e-Reader 100 typically comprises a battery 250, which is at least partially controlled and/or monitored by the e-Reader processor 210, in order to apply, where needed, power saving and power-monitoring applications.

Returning now to the explanation of Fig. 1, it is appreciated that in some embodiments of the present invention, an element of the e-Reader 100 must remain active in the e-Reader 100 and report back to the center 110 at short periodic intervals. For example and without limiting the generality of the foregoing, the RFID tag 205 may be required to report back to the center 110 every 5, 10, or more seconds. It is appreciated that the frequency of reporting back may be a function of the proximity of the e-Reader 100 to the exit of the premises. Typically, the closer the e-Reader 100 is to the exit, the more frequently the e-Reader 100 is required to report back. It is appreciated that it may not be practical to ensure that the element of the e-Reader 100 must remain active in the e-Reader 100 under all circumstances. Thus, the element of the e-Reader 100 must remain active in the e-Reader 100 under normal operating parameters (for example and without limiting the generality of the foregoing, the battery is not removed).

In some embodiments of the present invention, if the RFID tag 205 fails to report back to the center 110, and is turned off or removed, the e-Reader 100 may no longer operate without a partial or full software reload. Alternatively, the crypt-engine 130 may not decrypt encrypted content if the RFID tag 205 fails to report back to the center 110, and is turned off or removed.

The center 110 broadcasts a signal to any e-Reader 100 in the vicinity of the exit (S160). The signal comprises an instruction to the e-Reader 100 to turn on if it is in standby, and to identify itself. In response to receipt of the signal (S160), the e-Reader 100 powers up (if it was in standby mode) and returns a handshake (S165), thereby establishing communications with the center 110. In some embodiments of the present invention, the communications between the e-Reader 100 and the center 110 comprises a non-secure communications session. Alternatively, the communications between the e-Reader 100 and the center 110

comprises a secure communications session. Accordingly, the handshake returned in step S165 ensures the center 110 that the e-Reader 100 is indeed powered up, and provides a secure session key which can be used as an encryption key for the duration of the communication session. The encryption of the communication session ensures that the communication between the e-Reader 100 and the center 110 is genuine and that no eavesdroppers can view the contents of the session.

Once communications with the center 110 are established (S165), the e-Reader 100 sends the center 110 a unique device ID (S170). The e-Reader 100 then further sends the center 110 a cryptographic digest of each file in the storage comprised in the e-Reader 100 (S175). The cryptographic digest may be generated in real time by the e-Reader 100, or alternatively, in order to save time, the cryptographic digest could be stored in the e-Reader 100 storage with the file itself.

It is appreciated that, in order for step S160 to operate properly, the e-Reader 100 does not enter a state of being truly powered off. Rather, attempts to power off the e-Reader 100 result in the e-Reader 100 being put into standby mode. Alternatively, the e-Reader 100 may power-off but have some dedicated component which is left on (for example and without limiting the generality of the foregoing, as is well known, in some personal computers, even when the power is off, the LAN card is still functional at a low level of functionality). Further alternatively, the e-Reader 100 may automatically turn on every few seconds or minutes to check that it is in communication with the center 110.

It is appreciated that in step S175 the cryptographic digest need not comprise all of the classic properties of a cryptographic hash, such as collision resistance, first-preimage-resistance, and second-preimage-resistance. The digest's function is to identify the file in a brief manner.

The center 110 comprises an e-Reader registry 135 which comprises a database which lists all known unique device IDs and, for each unique device ID has a collection of cryptographic digests for files which were legally (i.e. with the knowledge and consent of the center 110) copied to each e-Reader 100 device. It is appreciated that certain files, for example and without limiting the generality of the foregoing, operating system files may be marked as unclassified, and need

not be checked. Alternatively, such operating system files might be checked and approved by the center 110 for removal from the premises.

Upon receipt of the cryptographic digest of each file in the storage, the center 110 compares the received hash with the database of unique device IDs and determines if the user is attempting to remove any files which are not permitted to be removed from the center (S180). It is appreciated that the user may be removing the file in an entirely innocent fashion, for instance, if the user has forgotten that the file was not deleted from the e-Reader 100 before the user attempted to leave. Alternatively, the user could be deliberately attempting to remove information from the premises which should not be removed. Additionally, should the center 110 receive a cryptographic digest of a file which is does not match any of the hashes stored in the database, the center 110 might take action as if the file should not be removed from the premises, as described below.

Should the center 110 determine that the user is attempting to remove an e-Reader 100 comprising a file which should not be removed from the premises, the center will alert the human guard (S185). Additionally and alternatively, the center 110 may also direct the e-Reader 100 to securely delete the file which is not to be removed from the premises, or to block access to the file which is not to be removed from the premises in any appropriate fashion (move the file to a directory which the user may not access; encrypt the file to a key not available to the user; and so forth).

It is appreciated that should the user of the e-Reader 100 be allowed to write files to the e-Reader 100, those files will also require registration of a cryptographic hash of the user file with the center 110. It is appreciated that in the case of registering a file written by the user on the e-Reader 100 a cryptographic hash is required instead of a weaker cryptographic digest, as in such a case, it is necessary to avoid a second-preimage-attack, whereby an innocuous file would be registered with the center 110, and a secret file would be stored instead of the innocuous file.

It is appreciated that the user might attempt to tamper with the e-Reader 100 hardware. In such an event, a plurality of methods might be used, individually or together, to detect the attempt to tamper:

An indelible, permanent ink can be put inside the cover of the e-Reader 100 such that tampering with the e-Reader causes the hands of the tamperer to be squirted with the ink;

A label can be placed over two opposing sides of the e-Reader 100 such that tampering with the e-Reader 100 causes the label to tear. The user of the e-Reader 100 might be required to display the two opposing sides of the e-Reader 100 to the human guard at intervals.

A second RFID tag can be embedded in a hidden location in the e-Reader 100 such that, if a first RFID tag is removed, the control center is aware that only one of two RFID tags report.

Operating system files can be stored in ROM in the processor (such as a CPU) comprised in the e-Reader 100, thereby making the operating systems harder to tamper with.

The e-Reader 100 cover is itself a part of an electrical circuit comprised in the e-Reader 100. If the cover is opened in an unauthorized fashion, the circuit comprising the cover would be broken, rendering the e-Reader 100 inoperable.

Reference is now made to Fig. 3, which is a simplified illustration of another embodiment of a system for protecting content for display on an e-Reader, constructed and operative in accordance with an embodiment of the present invention.

Fig. 3 depicts an e-Reader 300 while inside the premises 310 referred to above, with reference to Fig. 1. The premises 310 are depicted as comprising a communications network 320. As described above, the communications network 320 may be a wireless TCP/IP network, a Bluetooth communication network, or any other appropriate communication network over which the e-Reader 300 is in communication with a server 325. Although depicted in Fig. 3 as being outside the premises 310, it is appreciated that the server 325 need not actually be physically outside the premises.

The e-Reader 300 of Fig. 3 comprises a storage 330, corresponding to the e-Reader storage 215 of Fig. 2. The storage 330 is depicted comprising a decryption key 340, various decrypted content items 350, and a time bound content item 360.

The decryption key 340 is only active while the e-Reader 300 is located in communication with the communication network 320. The decryption key 340 is repeatedly downloaded or renewed from the server 325 through the communication network 320 after each access of the content 350. Alternatively, the decryption key 340 is never stored in the e-Reader 300. Rather a one-time use decryption key 340 may be accessed from the server 325 after an appropriate authentication of the e-Reader 300 which includes proof of freshness (in order to avoid replay attacks).

Alternatively, instead of requiring that the e-Reader is in communication with the communication network 320, the RFID tag 205 may be used to determine that the e-Reader 300 is within the premises 310.

Still another option is for the decryption key 340 to be stored in an encrypted form, encrypted according to a second key. The decryption key could periodically be encrypted to a different version of the second key.

Alternatively, the crypto-engine 235 (Fig. 2) is operative to receive and process a content license. The content license may not be processed by the crypto-engine 235 (Fig. 2) if the secure processor 210 (Fig. 2) has been disabled. An explicit command disabling the secure processor 210 (Fig. 2) may be broadcast by the center 110 (Fig. 1) to the e-Reader 300 when the e-Reader 300 is taken out of an exit from the premises 310. Correspondingly, an explicit command enabling the secure processor may be broadcast by the center 110 (Fig. 1) to the e-Reader 300 when the e-Reader 300 is brought in to an entrance to the premises 310. Similarly and optionally, a signal may be broadcast to the e-Reader 300 upon departure from the premises 310 requiring the e-Reader 300 to delete all forms and copies of each file which is presently stored in the e-Reader 300 memory in a decrypted form.

Once the e-Reader 300a is no longer in the premises 310, content 350 which was previously decrypted by the decryption key 340 is now no longer

decrypted 350a, and thus, unreadable by the e-Reader 300a. Once a file which comprises content 350 which was decrypted is closed, the memory which stored the decrypted content is purged of the decrypted content, using appropriate techniques well known in the art. It is appreciated that periodic polling of the e-Reader 300 occur in order to determine if the content 350 which was previously decrypted by the decryption key 340 should be deleted. It is appreciated that the period of the polling of the e-Reader 300 depends on external factors, such as the range of the communications network and so forth.

Those skilled in the art will appreciate that the server 325 may be located in the premises 310. As an additional security feature, the server 325 may be located in a locked room or otherwise secured area, as is well known in the art. Alternatively, as depicted in Fig. 3, the server may be located off-site, and in secure communication with the e-Reader 300 via the communication network 320.

Alternatively, documents may not be locally stored at all on the e-Reader 300, but rather remotely stored on the server 325. Thus, when the e-Reader 300a is no longer in communications with the communication network 320, and thus, no longer able to communicate with the server 325, such a document is no longer available.

It is also appreciated that within a single building there might be several zones corresponding to the premises described above. For example and without limiting the generality of the foregoing, in one area of the premises 310, a first group of e-Readers, associated with a first project, may be able to view encrypted content associated with the first project and a second group of e-Readers, associated with a second project, may not be able to view encrypted content associated with a first project. However, in a second area of the building, the second group of e-Readers may be able to view encrypted content associated with the second project and the first group of e-Readers may not be able to view encrypted content associated with the second project. For instance, and without limiting the generality of the foregoing, area specific wireless networking equipment can be utilized in each zone such that in each zone, a zone specific key or key stream was broadcast. The aforementioned zone specific key or key stream can also be enforced using GPS hardware in the e-Readers.

Some content may comprise a time bound content item 360. For example and without limiting the generality of the foregoing, some content may only be accessible during certain times. If the content is accessed at other times, the content may not be viewable, or if the content is viewable, only meaningless content may be displayed. Alternatively, the time bound content item 360 may be accessible only during limited fixed times, for example and without limiting the generality of the foregoing, between 10:00 AM to 5:00 PM, Monday - Friday

In some embodiments of the present invention, the server 325 may comprise a secure clock. In such embodiments, if the e-Reader 300 loses communication with the server 325 (for example and without limiting the generality of the foregoing, the e-Reader 300 is taken outside of the communication network 320; or alternatively, the e-Reader 300 enters stand-by mode), without receiving a time packet from the secure clock, the e-Reader 300 might not be able to process any content restricted to a time frame which, for the e-Reader 300, still lies in the future. It is appreciated that in order to ensure that a received time packet is fresh a challenge-response based time protocol, as is known in the art, would be implemented.

In some embodiments of the present invention, the user may be required to insert a smart card into a smart card reader associated with one or both of the e-Reader 300, or the server 325 on an episodic basis. For example and without limiting the generality of the foregoing, the user may required to insert the smart card into the smart card reader at certain intervals of time, or alternatively, after displaying a certain amount of text on the e-Reader 300. It is appreciated that a contactless smart card may be used, so that, rather than insert the smart card, it may only be necessary to bring the smart card into proximity of e-Reader 300 or the server 325. Alternatively, instead of the smart card, a secure chip, a secure ID, or biometric identification may be required (for example and without limiting the generality of the foregoing, a fingerprint, a handprint, or a retinal scan). The secure chip or secure ID interface may be via USB, SD (secure device), or other appropriate interface.

Reference is now made to Fig. 4, which is a simplified illustration of a yet another embodiment of a system for protecting content for display on an e-

Reader. In some implementations of the present invention, the e-Reader 100, the e-Reader 100 comprises, a lens 410, an optical system 420, such as, and without limiting the generality of the foregoing, a CCD (charge-coupled device) camera, and face recognition software. When operative, the face recognition software is invoked in a face recognition processor 430 as a face recognition program 440.

Reference is now additionally made to Fig. 5, which is a simplified illustration of one implementation of the e-Reader depicted in Fig. 4.The e-Reader 100, through the lens 410 and optical system 420 episodically detects the presence of a user 510. The episodic detection of the user comprises capturing an image of whatever is directly in the line of focus of the lens, thereby producing an image. The image is processed, and further action is taken, as described below.

The face recognition program 440 may not be equipped to detect a particular face, 510 as is well known in the art. Rather, the face recognition program 440 is equipped to detect the presence of the face 510 opposite the e-reader 100, regardless of whose face the face 410 is. Alternatively, the e-Reader 100 may rely on either a retinal scan indicating the presence of the reader's eye, rather than the face recognition software or other facial recognition techniques, such as those which rely on facial geometry.

In example A, depicted in Fig. 5, the user of the e-Reader 500 is positioned so that the e-Reader 500 is opposite the face 510 of the user. A check mark indicates that in example A, the e-Reader 500 functions normally, and the user may continue to read normally.

In example B, depicted in Fig. 5, the user of the e-Reader 500 is positioned so that the e-Reader 500 is not opposite the face 510 of the user. For example, if the user attempts to scan or photocopy text which appears on the e-Reader 500, the face recognition processor 430 prevents the e-Reader 100 from functioning normally. Thus, the text no longer appears on the e-Reader 500, and thus, the text may not be scanned or photocopied. An X is depicted next to example B, in order to indicate that the e-Reader 500 does not function normally.

In example C, depicted in Fig. 5, a camera 520 or cell phone comprising a camera 520 is positioned between the e-Reader 500 and the face of the user of the e-Reader 500, so that the e-Reader 500 is not directly opposite the

face 510 of the user. Thus, if the user attempts to photograph text which appears on the e-Reader 400, the face recognition processor 430 prevents the e-Reader 100 from functioning normally. Thus, the text may not be photographed. An X is depicted next to example C, in order to indicate that the e-Reader 500 does not function normally. Additionally, the e-Reader 500 software may detect the presence of the camera 520 or other imaging devices, and deny access to the content, as discussed above.

It is appreciated that in order to avoid attempts to circumvent the face recognition system described above by placing a photograph opposite the e-Reader 400, the face recognition processor 430 analyzes the image for depth of image, which would be lacking in a two dimensional image, as opposed to a face. The face recognition processor 430 is also operative, in some embodiments, to determine the presence of ocular motion on the part of the face.

Alternatively, the e-reader 500 is equipped with a gaze tracking system which uses the optical system 420 to track and monitor where the user of the e-reader 500 is looking. The e-Reader 500 then uses the gaze tracking system to determine where on the e-Reader 500 screen 150 (Fig. 1) the user of the e-Reader 500 is reading. The e-Reader 500 then distorts other portions of the e-Reader 500 screen 150 (Fig. 1). Typically, the distortion of the portions of the e-Reader 500 screen 150 (Fig. 1) is performed by pixelization, the pixelization comprising any of blurring and displaying of the portions of the e-Reader 500 screen 150 (Fig. 1) at a resolution at which reading is difficult.

In an alternative embodiment of the present invention, the e-Reader 500 may periodically photograph the face 510 of the user 510 of the e-Reader 500 and send a perceptual hash of the face 510 of user 510 to a security server (such as the server 225 of Fig. 3) in order to compare the hash of the photograph with a database of hashes of photographed faces of authorized users. Alternatively, other facial recognition techniques, such as, but not limited to, retinal matching, facial geometry matching, and so forth, may be utilized to verify that the user 510 of the e-Reader 500 is one of the authorized users.

If the hash of the photograph of the face 510 does not match a hash of a photograph of a face stored in the database of hashes of photographed faces of

authorized users, security server (such as the server 225 of Fig. 3) sends a message to the e-Reader 500 instructing the e-Reader 500 to perform at least one of the following: cease displaying text; and enter standby mode. Additionally, the security server (such as the server 225 of Fig. 3) may also notify the center 110 (Fig. 1) of a potential security violation. Alternatively, the e-Reader 500 may cause files containing the displayed text to be locked either logically (with a bit so indicating) or by changing the encryption method or encryption key by which the file is encrypted, or by changing the file itself so that the file appears to be an illegal file (for instance, by changing the signature or contents of the file).

Alternatively, the photograph of the face 510 and/or the hash of the photograph may be stored on the e-Reader 500 itself or a secure ID or chip associated with the e-Reader 500. The e-Reader 500 may then securely compare the photograph of the face 510 with the stored photograph or hash. Alternatively, if the photograph of the face 510 and/or the hash of the photograph are stored on a secure ID or chip associated with the e-Reader 500, the secure ID or chip may be inserted into the e-Reader 500 or an appropriate interface proximate to the e-Reader 500 and compared with the real time image.

Those skilled in the art will appreciate that perceptual hashes are, in the present embodiment, preferred to cryptographic hashes, due to the nature of photographs of human faces. A perceptual hash is a fingerprint of a multimedia file, such as a photograph of a human face, derived from various features from the content of the multimedia file. Unlike cryptographic hash functions which rely on an avalanche effect of small changes in input leading to drastic changes in the output, perceptual hashes are "close" to one another if the features are similar. Furthermore, different photographs of the same person will yield, with high probability, the same perceptual hash values, whereas photographs of different people will yield, with high probability, different perceptual hash values. Thus, minor changes in a face on a day-to-day basis, are less likely to negatively impact the operation of the system of Fig. 5. Alternatively, any secure pattern matching software system may be used to compare the stored perceptual hash with the perceptual hash of the photograph of the face 510.

In still another alternative embodiment of the present invention, the e-Reader 500 may comprise a screen of polarized glass over a viewing screen, thereby preventing circumventing the embodiment discussed in Fig. 5 example C by taking a picture of the text displayed in the viewing screen from an angle, such that the camera 520 is not interposed between the e-Reader 500 and the face 510 of the user.

In yet another alternative embodiment of the present invention, the e-Reader 500 is only functional in the presence of one or more other e-Readers. For example and without limiting the generality of the foregoing, a student's e-Reader may only be functional in proximity to a teacher's e-Reader.

Reference is now made to Fig. 6, which is a simplified illustration of still another embodiment of a system for protecting content for display on an e-Reader 600. A typical e-reader comprises hardware and software, as is known in the art, which is operative to display text based content on the screen 150 (Fig. 1). It is appreciated that the screen may comprise any appropriate screen including, but not limited to, LCD and eInk.

Typically, the content is rendered for display utilizing at least one font. Content which is designated as secure content is rendered using a font which comprises elements which are resistant to optical character recognition. In particular, the font utilized to render the text based content comprises modifications which render the text such that a human can still comfortably read the text, but a machine attempting OCR will introduce errors. For example and without limiting the generality of the foregoing, subtle techniques are utilized during the rendering process that will successfully introduce enough letter recognition errors, and layout errors, so as to render the OCR version of the text significantly less valuable than the original.

Those skilled in the art will appreciate that OCR resistance can be increased using a combination of varying character sizes in the same font (such as the large "p" 630 in the word "adipisicing" and the small "b" 640 in the word "flabore"), using anti-aliased characters, ensuring that the characters are displayed using abutted spacing (such as the "am" 650 in the word "amet") or extreme kerning (such as the "re" 680 in the word "dolore"), and typographical ligatures

between two or more letters (such as rendering lower case “f” and lower case “l” as “fl”), ensuring that similar letters (such as upper case “I” 660 and lower case “l” 670) appear similar in appearance after rendering, and so forth. Likewise, adding additional typographical elements (such as the line 690 connecting between the “c” and the “i” in the word “incididunt”) increases resistance of the font to optical character resistance.

In Fig. 6, the e-Reader 600 is depicted with text 610 on the viewing screen 620. The text 610 is displayed using a font which is resistant to optical character recognition. Thus, attempts to scan the text 610 and then perform optical character recognition on the scanned image, as is well known in the art, is thereby frustrated.

Reference is now additionally made to Fig. 7, which is a simplified illustration of character elements being displayed on an e-Reader display, within the system of Fig. 6. Figure 7 shows a letter E 700. The letter E can be broken down into a plurality of character elements:

A first character element, similar to the Greek letter Gama Γ 710;

A second character element, corresponding to the middle bar of the letter E, − 720; and

A third character element, corresponding to the lower bar of the letter E, _ 730.

The combination of the plurality of character elements Γ 710; − 720; and _ 730 would comprise the letter E 700. It is appreciated that the choice of the three elements selected, and not three other elements which would also combine to the letter E (for example and without limiting the generality of the foregoing, ├; _; and ¯) or the choice of using three character elements and not two character elements or four character elements is purely by way of example, and is not intended to be limiting.

For e-Reader display screens which operate at a slow enough refresh rate, displaying only some of, but not all of, the character elements on the device display screen for at least one screen refresh period would result in the character being displayed too slowly for many camera shutter speeds or scanners to capture

the entire character. On the other hand, the character would appear to the human eye as being displayed in toto.

In Fig. 7, each box depicted above the time line is one displaying of one of the three character elements 710, 720, and 730 for a single screen refresh period.

If a camera has a shutter speed greater than the amount of time it would take all of the character elements to display (i.e. three consecutive boxes above the time line of Fig. 7), then the camera would not capture the entire character image. Thus, the image in the photograph would not easily lend itself to optical character recognition. For example, if the shutter speed of a camera is 1/125 second and the refresh rate of the display screen is 1/30 second, a three character element character would take 3 X 1/30 second to display, i.e. 1/10 second. The camera would, therefore, only be able to capture one of the character elements. In order to capture all of the three character element characters in this example the camera would have to have a shutter speed of less than 1/10 second.

Similarly, if a digital scanner is able to scan 15 pages per minute (ppm), it would therefore require 4 seconds to scan a single page. A typical A4 page is 8.27 inches in length. Thus, an A4 page would be scanned in:

8.27 inches / 4 seconds = 2.0675 inches / second

Assuming a font size of 12 point on average for the font displayed on the e-Reader (this varies depending on a variety of factors, including the resolution of the display screen, the material used to manufacture the display screen, and so forth), a theoretical 12 point font character which occupies the full 12 points is 0.16667 inches high.

Thus, a character of 0.16667 inches would be scanned in:

(0.16667 inches) / (2.0675 inches / second) = 0.0806 seconds

A display refresh rate should be chosen such that the character elements all appear as a single letter to the human eye. Additionally, the refresh rate should be chosen so that the refresh rate is faster than the 0.0806 seconds needed to scan a character. Accordingly, a refresh rate of at least 15 Hz (0.067 seconds) should be chosen to satisfy both of these requirements. If the character is segmented into three elements, as in the present example, 3 x 0.067 seconds = 0.20

seconds would be needed to display the entire character. Thus, scanning the entire character in 0.0806 seconds occurs too quickly in order to capture all of the character elements comprising the character, since only a single element of the character is displayed during a single screen refresh period.

The above example relates to a case where the camera or scanner is too fast to capture the entire letter E 700.

In an alternative embodiment, a blocking character, such as the number 8, could be displayed very briefly thereby preventing a slow scanner or camera from recording a character correctly. Reference is now made to Fig. 7A, which is a simplified illustration of an alternative embodiment of the system depicted in Fig. 7. For example if character elements 710, 720 and 730 are each displayed for 1/15 second and blocking character element 740 is displayed for 1/60 second, which is generally faster than the human eye can register, the character E 700 would appear to the human eye as being displayed in toto correctly, while a scanner or camera would see only the character 8 715.

It is appreciated that in some embodiments, if the screen refresh rate of the viewing screen 620 is sufficiently fast, then a scanner or a camera might be too slow to capture the text displayed, if for instance the camera ISO setting is too low.

Reference is now made to Fig. 8, which is a simplified illustration of yet another embodiment of a system for protecting content for display on an e-Reader 800. In Fig. 8, the e-Reader 800 is depicted with text 810 on the viewing screen 820. By way of example, the embodiment of the present invention depicted in Fig. 8 is described with reference to a single letter "r" 830 which is part of the text appearing in the viewing screen 820.

An encrypted document which is produced for distribution for reading on an e-Reader 500 may be subjected to at least one of two types of attempts to pirate the document:

1. The document decryption key may be intercepted used to decrypt the document. The decrypted document is then saved and may be redistributed. In this case, the plain text version of the decrypted document is, in principle, identical to the plain text version of the encrypted document.

2. The document may be subjected to one of photographing, scanning, and optical character recognition, in order to produce an unprotected version of the document for redistribution. A document produced in this manner is not in principle, identical to the plain text version of the encrypted document.

It is appreciated that using attack number 1, described above produces a file which, when subjected to a binary comparison with the source file will produce a nearly perfect match. On the other hand, a file produced using attack number 2 will still preserve the layout and contents of the source file, but will not produce a match when subjected to a binary comparison with the source file.

It is appreciated that once the document is saved in its plain text form, as discussed above, a photographed, scanned, or otherwise subjected to optical character recognition version of the document may then be prepared.

Aside from the methods discussed above which describe techniques for resisting optical character recognition, it is advantageous to be able to identify the source of a pirated document, once such a document is obtained.

Various watermarking and fingerprinting techniques may be applied to the production of such a document, as described below.

Typical characters, when displayed on a displaying device, such as a viewing screen are comprised of pixels. In a typical character, such as the letter "r" 830 of Fig. 8, the letter appears as a solid area, typically of a single color, often black.

However, in the embodiment of the present invention depicted in Fig. 8, the letter "r" 830 is depicted as having a small zone which is not solid, unlike the remainder of the letter "r" 830. Rather, the letter "r" comprises a small zone 840 which is not solid, but is not apparent to an eye of a viewer possessing typical visual acuity. Nonetheless, the letter "r" 830 comprises an embedded watermark 840. The embedded watermark 840 is depicted in Fig. 8 as comprising a string of zeros and ones 850, that is to say, a string of bits. A watermark comprised of a string of bits may comprise information relating to any or all of: a device ID of the e-Reader 800; a user ID of the user of the e-Reader 800; a document ID, if, for instance, the displayed text is one of a series of numbered

copies of the document being read; and any other information which might be useful in identifying a potential source of a leak of the document.

For example and without limiting the generality of the foregoing, if a copy of the document is found to be illegally distributed, the embedded watermark 540 and the bits 550 comprised therein can be used to identify a potential source of a leak of the document, such as the actual e-Reader 500 device from which the document was leaked, or the user to whom the e-Reader 500 device from which the document was leaked is assigned.

In yet another alternative embodiment of the present invention, the embedded watermark 540 may comprise a microscopic or near-microscopic version of a logo or other uniquely identifying graphic element.

Returning to the discussion of the case where the document decryption key may be intercepted used to decrypt the document. As was noted above, the decrypted document is then saved and may be redistributed. In this case, the plain text version of the decrypted document is, in principle, identical to the plain text version of the encrypted document.

It is appreciated that although the discussion herein centers on text based documents, any appropriate content item, including, but not limited to text, graphics, video, and audio content may be subject to the methods described herein.

On a conceptual level, a content item may be viewed as comprising a set of elements making up the content item. This set of elements may comprise a set of:

characters for a text based content item;

pixels comprising the characters displayed in a text based content item;

pixels comprising a portion of a graphical or video based content item;

and so forth.

The set of content item elements may be denoted E, such that $E = \{E_1, E_2, \ldots E_i, \ldots E_m\}$.

Each user of the e-Reader is typically associated with some unique user information. The unique user information may comprise the user's name, or

the user's user identification number, or some other information associated with the user. The unique user information is converted into a string of bits, using techniques well known in the art.

The string of bits, hereinafter denoted S_0, is parsed by a parser into a plurality of subsequences of strings of bits, hereinafter denoted $S_1, \ldots, S_n$, the parsing being performed such that S_0 equals a function of $S_1, \ldots, S_n$. Examples of the parsing would be to break up a 32 bit string into 16 two bit strings. In such a case, the function may be concatenation. Alternatively, S_1, may be equal to the first and last bits of S_0; S_2, may be equal to the second and penultimate bits of S_0, and so forth.

Those skilled in the art will appreciate that the parser is typically disposed in a computer, frequently in a processor or other appropriate hardware. Alternatively, the parser is a software based parser, in which case the parser software is typically invoked by a processor.

A matrix of content replacement items is developed, the matrix denoted R, the matrix comprising at least n rows, each row of matrix R corresponding to at least one of n members of set E. There are at least n rows of R corresponding to at least one of n members of set E in order that each possible combination of subsequences of bits which may occur in $S_1, \ldots, S_n$, may be matched with a corresponding element from row R_n of matrix R. (It is appreciated that in certain cases, matrix R may comprise only one row).

One element of R, R_{ij} corresponding to E_i and S_j is replaced in the content item. The replacement of E_i with R_{ij} for the corresponding S_j is recorded in a record stored by the computer processor performing the steps mentioned herein. The process of replacing content item elements in set E with members of matrix R is performed repeatedly, typically until at least one content item element in the content item has been replaced for each one of the subsequences of $S_1, \ldots, S_n$.

Matrix R is populated by matrix elements having a similarity criterion to the content item element to be replaced by said matrix element. The basis of the similarity criterion is that a typical user of the content item will either not notice the replacement, or if the replacement is noticeable to the typical user, the replacement will not result in a reduction of the quality of the consumption or use of the content item.

By way of example, consider a user having a unique user identification number, expressed in binary, of:

$$S_0 = 11010010000100101101011011$$

If each subsequence of $S_1, \ldots, S_n$ is to be two bits, then:

$$S_1 = 11$$

$$S_2 = 01$$

$$S_3 = 00$$

$$S_4 = 10$$

$$S_5 = 01$$

$$S_6 = 00$$

$$S_7 = 10$$

$$S_8 = 11$$

$$S_9 = 01$$

$$S_{10} = 01$$

$$S_{11} = 10$$

$$S_{12} = 11$$

Examples are now provided first for video and graphic content items.

For video and graphic content items, the set E comprises a plurality of pixels, in at least one embodiment. Each pixel in a video frame or in a graphic element has a coordinate, and is typically associated with one of a color value (for color pictures) or a grey scale value (for black and white pictures). It is appreciated

that various color systems are in use, including, but not limited to RGB (red-green-blue), CYMK (cyan, magenta, yellow), CIE, chrominance-luma (YUV), and so forth. For the purpose of this example, the RGB color system is used, but any color system may be used.

In the present example, where S_0 is divided into twelve subsequences of bits, at least twelve pixels in the content item are selected.

As was noted above, each pixel within a video frame or a graphic element has a coordinate, indicating the pixel's location. The pixel has a color value or grey scale. Additionally, each pixel in a video is located in a single frame in the video. Thus, for over all of the pixels in E, we can create the following matrix: $E_{x,y,f,R,G,B}$, where x and y indicate the coordinates at which the pixel is located in the frame/graphic. In the case of video, the frame in which the pixel is located is denoted by f. The color of the pixel is indicated by the subscripts R, G, and B.

In the present example, for ease of the present description, assume that either a single video frame or a picture is being discussed. In the case of video, a frame number would be added as well.

Thus, the following pixels might be selected for replacement:

PIXEL and COLOR
(x = 127; y = 12; R= 62; G = 240; B = 197)
(x = 17; y = 112; R= 68; G = 240; B = 193)
(x = 227; y = 184; R= 97; G = 119; B = 17)
(x = 18; y = 96; R= 211; G = 111; B = 97)
(x = 107; y = 120; R= 129; G = 24; B = 19)
(x = 63; y = 80; R= 162; G = 20; B = 7)
(x = 182; y = 85; R= 112; G = 200; B = 251)
(x = 208; y = 1912; R= 93; G = 164; B = 227)
(x = 6233; y = 963; R= 18; G = 226; B = 69)
(x = 7351; y = 858; R= 243; G = 24; B = 227)
(x = 1327; y = 1020; R= 62; G = 245; B = 73)
(x = 6207; y = 412; R= 105; G = 20; B = 39)

The following replacement table might be developed. A rule might be applied to determine how a change is performed (for example and without limiting the generality of the foregoing, if the subsequence S_i is 00, increase the red value by 3; if the subsequence S_i is 01, decrease the blue value by 1; if the subsequence S_i is 10, increase the green value by 3; and if the subsequence S_i is 11, increase the green value by 1). Alternatively, the change could be performed in a pseudo-random fashion. Small changes of this fashion in individual pixels typically result in video and graphic files which should be nearly or totally indistinguishable to a viewer of the file. In video files where the twelve replaced/changed pixels may be spread out over thousands of frames, the change should be even less noticeable. The tradeoff is that the replaced pixels result in the unique user information being embedded in the file. If the file is subsequently decrypted and the plaintext then made publically available, the owner or controller of the content will be able to determine the source of the file.

PIXEL and COLOR	SUBSEQUENCE of $S_1, \ldots, S_n$
(x = 127; y = 12; R= 62; G = 241; B = 197)	$S_1 = 11$
(x = 17; y = 112; R= 68; G = 240; B = 192)	$S_2 = 01$
(x = 227; y = 184; R= 100; G = 119; B = 17)	$S_3 = 00$
(x = 18; y = 96; R= 211; G = 114; B = 97)	$S_4 = 10$
(x = 107; y = 120; R= 129; G = 24; B = 18)	$S_5 = 01$
(x = 63; y = 80; R= 165; G = 20; B = 7)	$S_6 = 00$
(x = 182; y = 85; R= 112; G = 203; B = 251)	$S_7 = 10$
(x = 208; y = 1912; R= 93; G = 165; B = 227)	$S_8 = 11$
(x = 6233; y = 963; R= 18; G = 226; B = 68)	$S_9 = 01$
(x = 7351; y = 858; R= 243; G = 24; B = 226)	$S_{10} = 01$

(x = 1327; y = 1020; R= 62; G = 243; B = 73)	$S_{11} = 10$
(x = 6207; y = 412; R= 105; G = 21; B = 39)	$S_{12} = 11$

As was noted above, if a video or graphic is black and white, then the gray scale can be altered in developing the replacement table. It is also the case that, for a text document, characters in the document can be related to as graphic elements as well.

Reference is now made to Fig. 9, which is a simplified illustration of an alternative of the embodiment of the system of Fig. 8. In Fig. 9, the character "r" 830 is depicted as appearing, almost, entirely, in one color (typically black). Two of the pixels comprising the character "r" 830, pixel 910 and pixel 920, are depicted as having a different gray scale than the body of character "r" 830. Thus, pixel 910 might have a gray scale of 93%, corresponding to and pixel $S_8 = 11$; pixel 920, corresponding to $S_6 = 00$ might have a gray scale of 97%. Such variations in single pixels will typically be either indistinguishable to a reader of the text 810 or will not interfere with the reading of the text 810 displayed on the e-Reader 800.

It is appreciated that although the two pixels pixel 910 and pixel 920 are depicted as appearing in a single character "r" 830, this depiction is merely presented this way as a matter of convenience.

In another example of a possible replacement matrix R, characters could be used. Consider the following three characters:

A

A

A

The first of the three characters appearing above is the character "A", designated in the Unicode standard as Latin capital letter A, having the Unicode value 0041. The second of the three characters appearing above is the character "A", designated in the Unicode standard as Greek capital letter Alpha, having the

Unicode value 0391. The third of the three characters appearing above is the character “A”, designated in the Unicode standard as Cyrillic capital letter A, having the Unicode value 0410. Similar tables could be produced comprising:

B	Latin capital letter B	Unicode 0042
B	Greek capital letter Beta	Unicode 0392
B	Cyrillic capital letter VE	Unicode 0412

and

a	Latin small letter a	Unicode 0061
α	Greek small letter alpha	Unicode 03B1
a	Cyrillic small letter a	Unicode 0430

It is appreciated that aside from the Greek small letter alpha, the characters grouped together are indistinguishable to the typical reader. Furthermore, the typical reader would have no trouble reading the phrase “typicαl reader” correctly.

The concept behind the replacement tables presented above can be extended to other similar but not identical Unicode characters. Consider the following characters:

A	Unicode 0041
À	Unicode 00C0
Ä	Unicode 00C4
Å	Unicode 00C5
Ă	Unicode 0102
Ą	Unicode 0104

Characters presented in the above table may be substituted, using the system presented above, for the character A. A typical reader would have little or no trouble reading a word with such a substitution correctly.

Reference is now made to Fig. 10, which is a simplified illustration of a sixth embodiment of a system for protecting content for display on an e-Reader 1040, 1045,. Fig. 10 depicts a system whereby different versions of a document to be displayed on an e-Reader 1040, 1045 are authored so as to produce slightly different versions of the document 1050a, 1050b. By storing a record of which e-Reader 1040, 1045 receives which version of the document 1050a, 1050b, it is possible, at a later time, to determine which e-Reader 1040, 1045 is the source of a leak, should one of the versions of the document 1050a, 1050b be discovered to be leaked. One implementation of such a system is now described.

When authoring the document, the author of the document may suggest synonyms for several words comprised in the document. Alternatively and additionally, alternative spellings of words (for example and without limiting the generality of the foregoing, color/colour; center/centre; program/programme, etc) could be used for several words comprised in the document. Further alternatively and additionally, subtle misspellings may be suggested for some words comprised in the document for example and without limiting the generality of the foregoing, informal/imformal; truly/truely; rescusitate/resuscitate, etc.). Alternatively, grammatical variations may be used, for example and without limiting the generality of the foregoing, commas, semicolons, and colons may be placed or omitted in various places throughout the document. An electronic version of the document 1010, which includes all of the different synonyms, alternative spelling, and misspellings which were proposed by the author of the document, is uploaded to an electronic document authoring system 1020. Each e-Reader 1040, 1045 to which a version of the document is loaded, receives a slightly different version of the document 1050a, 1050b from an electronic document authoring system 1020 management unit 1030.

Each different version of the document 1050a, 1050b, or a cryptographic hash thereof, which is issued to a different e-Reader is stored in a database along with a device ID 1070, 1080.

In such a case, should a suspicious copy of the document be obtained, and it is determined that the copy of the obtained document has been illegally distributed, by comparing the obtained copy of the document (or the cryptographic hash thereof) to the database 1060 of versions of the document 1050a, 1050b, it is possible to determine which e-Reader 1040, 1045 is the source of the illegally distributed version of the document.

In an alternative embodiment of the present invention described in many of the various embodiments of the present invention described herein, different portions of the source document 1010 may be tagged as being available to different levels of security clearances (for example and without limiting the generality of the foregoing, secret, top secret, eyes-only, etc.). If the e-Reader 1040, 1045 to which the an electronic document authoring system 1020 management unit 1030 is to issue the document 1050a, 1050b is not cleared for a certain security level, then only those portions of the document 1050a, 1050b tagged with allowed security levels may be distributed to the e-Reader 1040, 1045.

It is appreciated that the various embodiments of the present invention described herein may be implemented individually in an e-Reader device or in combination with each other. For example and without limiting the generality of the foregoing, the embedded watermark 840 of Fig. 8, or the embedded watermarks 910 and 920 of Fig. 9 may be embedded in a character in the optical character recognition resistant font of Fig. 6 or 7. Similarly, the selectively authored document of Figs. 8 or 9 may be displayed in the optical character recognition resistant font of Figs. 6 or 7, where some letters comprise the embedded watermark 840 of Fig. 8, or the embedded watermarks 910 and 920 of Fig. 9, on an e-Reader device which is operative to detect that the face of the user is directly in line with the display screen, as described above with reference to Fig. 5, and so forth, with implementations of all of the various embodiments of the present invention described herein.

Reference is now made to Figs. 11 - 15, which simplified flowcharts of preferred methods of operation of the various embodiments described herein. Figs. 11 - 15 are believed to be self-explanatory in light of the above discussion.

It is appreciated that software components of the present invention may, if desired, be implemented in ROM (read only memory) form. The software components may, generally, be implemented in hardware, if desired, using conventional techniques. It is further appreciated that the software components may be instantiated, for example: as a computer program product; on a tangible medium; or as a signal interpretable by an appropriate computer.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the invention is defined by the appended claims and equivalents thereof:

What is claimed is:

CLAIMS

1. A method for protecting content on a device, the method comprising:

providing a device, the device having at least one encrypted content item, the at least one encrypted content item being consumable only in at least one geographic zone, the device comprising a communication element and a storage module, the communication element being operative to communicate with a control center, the control center being operative to perform at least one of:

identifying the device; and

tracking the device;

establishing a communication session between the device and the control center;

verifying that the device is within the one geographic zone;

in response to a positive result of the verifying:

providing a decryption key to the device, thereby enabling decrypting the at least one encrypted content item;

decrypting the at least one encrypted content item, thereby producing a decrypted content item;

performing at least one of the following:

storing the decrypted content item in device memory; and

outputting the decrypted content item to a device screen; and

continuing, on an episodic basis, to verify that the device is within the one geographic zone;

performing at least one of the following in response to a negative result of the verifying:

purging from the device memory the decrypted content item;

preventing the device from continuing to operate;

clearing the device display screen; and

disabling the decryption key.

2. The method according to claim 1 and wherein the providing the decryption key comprises:

repeatedly downloading the decryption key to the device from the control center;

deleting the decryption key from the device immediately after the decryption key is used to decrypt the encrypted content; and

requesting a new decryption key from the control center.

3. The method according to claim 2 and wherein the new decryption key comprises a different decryption key.

4. The method according to claim 1 and wherein the providing the decryption key comprises:

flagging the decryption key as having expired immediately after the decryption key is used to decrypt the encrypted content; and

receiving a message from the control center to the device, the message comprising a decryption key renewal message

5. The method according to claim 4 and wherein the decryption key comprises a hash of the received message.

6. The method according to claim 1 and wherein the providing the decryption key comprises:

transmitting authentication information from the device to the control center;

receiving access to a one-time use decryption key in response to a positive result of an authentication performed at the control center,

wherein the authentication information comprises proof of freshness, and the decryption key is not stored on the device.

7. The method according to claim 1 and wherein the providing the decryption key comprises:

receiving a second decryption key;

receiving an encrypted decryption key, the encrypted decryption key being encrypted according to the second decryption key; and

decrypting the encrypted decryption key according to the second decryption key.

8. The method according to claim 7 and also comprising receiving an updated version of:

the second decryption key; and

the encrypted decryption key.

9. The method according to claim 1 and wherein the providing the decryption key comprises:

receiving a content license, the content license being operative to enable decryption of the encrypted content;

storing the content license in a device crypto-engine; and

utilizing of the content license by a device processor in order to enable decryption of the encrypted content.

10. The method according to claim 9 and further comprising receiving a disabling message from the control center if the device is removed from the geographic zone, thereby disabling the processor from utilizing the content license.

11. The method according to either claim 9 or claim 10 and further comprising receiving a signal from the control center if the device is removed from the geographic zone, the signal requiring the device to delete all forms and copies of the decrypted content from the device memory.

12. The method according to any of claims 9 - 11 and further comprising receiving an enabling message from the control center if the device is

brought into the geographic zone, thereby enabling the processor to utilize the content license.

13. The method according to any of claims 1 - 12 and wherein the device comprises an e-Reader.

14. The method according to any of claims 1 - 12 and wherein the device comprises a music player.

15. The method according to any of claims 1 - 12 and wherein the device comprises a video player.

16. The method according to any of claims 1 - 12 and wherein the device comprises a memory device.

17. The method according to any of claims 1 - 12 and wherein the device comprises a computer.

18. The method according to any of claims 1 - 12 and wherein the device comprises a telephone.

19. The method according to any of claims 1 - 18 and wherein the at least one geographic zone comprises a single premises.

20. The method according to any of claims 1 - 18 and wherein the at least one geographic zone comprises a region in a premises.

21. The method according to any of claims 1 - 20 and wherein the content item comprises a time bound content item.

22. A system for protecting content on a device, the system comprising:

a device having at least one encrypted content item, the at least one encrypted content item being consumable only in at least one geographic zone, the device comprising a communication element and a storage module, the communication element being operative to communicate with a control center, the control center being operative to perform at least one of:

identifying the device; and

tracking the device;

a communications module operative to establish a communication session between the device and the control center;

a verification mechanism operative to verify that the device is within the one geographic zone;

in response to a positive result of the verifying at least one of:

a decryption key is provided to the device, thereby enabling decrypting the at least one encrypted content item;

a decryptor decrypts the at least one encrypted content item, thereby producing a decrypted content item;

the device is enabled to perform at least one of the following:

device memory stores the decrypted content item; and

the decrypted content item is output to a device screen for displaying; and

the verification mechanism continues, on an episodic basis, to verify that the device is within the one geographic zone;

in response to a negative result of the verifying performing at least one of:

the decrypted content item is purged from the device memory;

the device is prevented from continuing to operate;

the device display screen is cleared clearing; and

the decryption key is disabled.

Respectfully submitted,

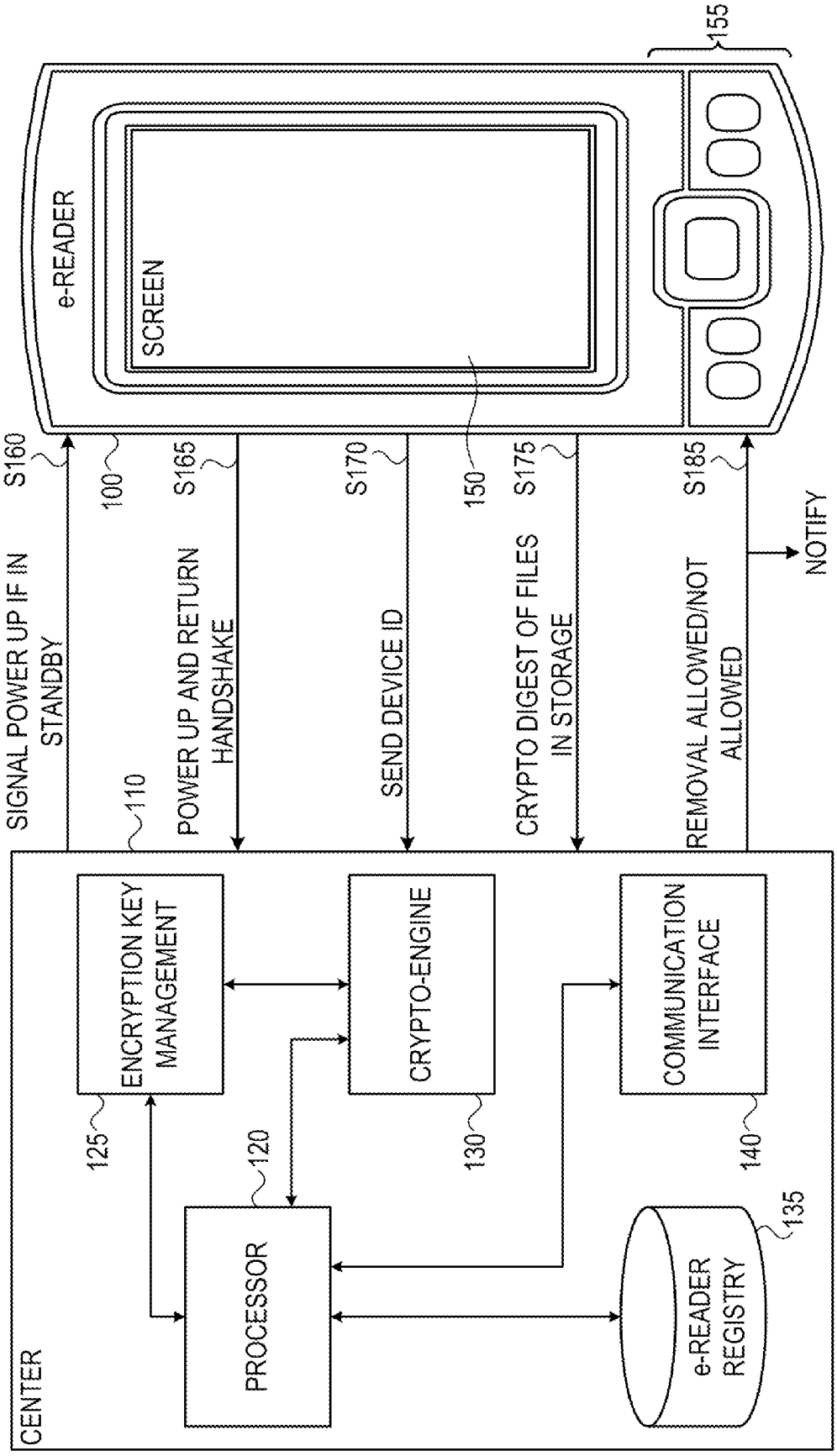
155
e-READER
SCREEN
100
150
S160
S165
S170
S175
S185
SIGNAL POWER UP IF IN STANDBY
110
POWER UP AND RETURN HANDSHAKE
SEND DEVICE ID
CRYPTO DIGEST OF FILES IN STORAGE
REMOVAL ALLOWED/NOT ALLOWED
NOTIFY GUARD
CENTER
ENCRYPTION KEY MANAGEMENT
CRYPTO-ENGINE
COMMUNICATION INTERFACE
125
130
140
120
PROCESSOR
e-READER REGISTRY
135

FIG. 1

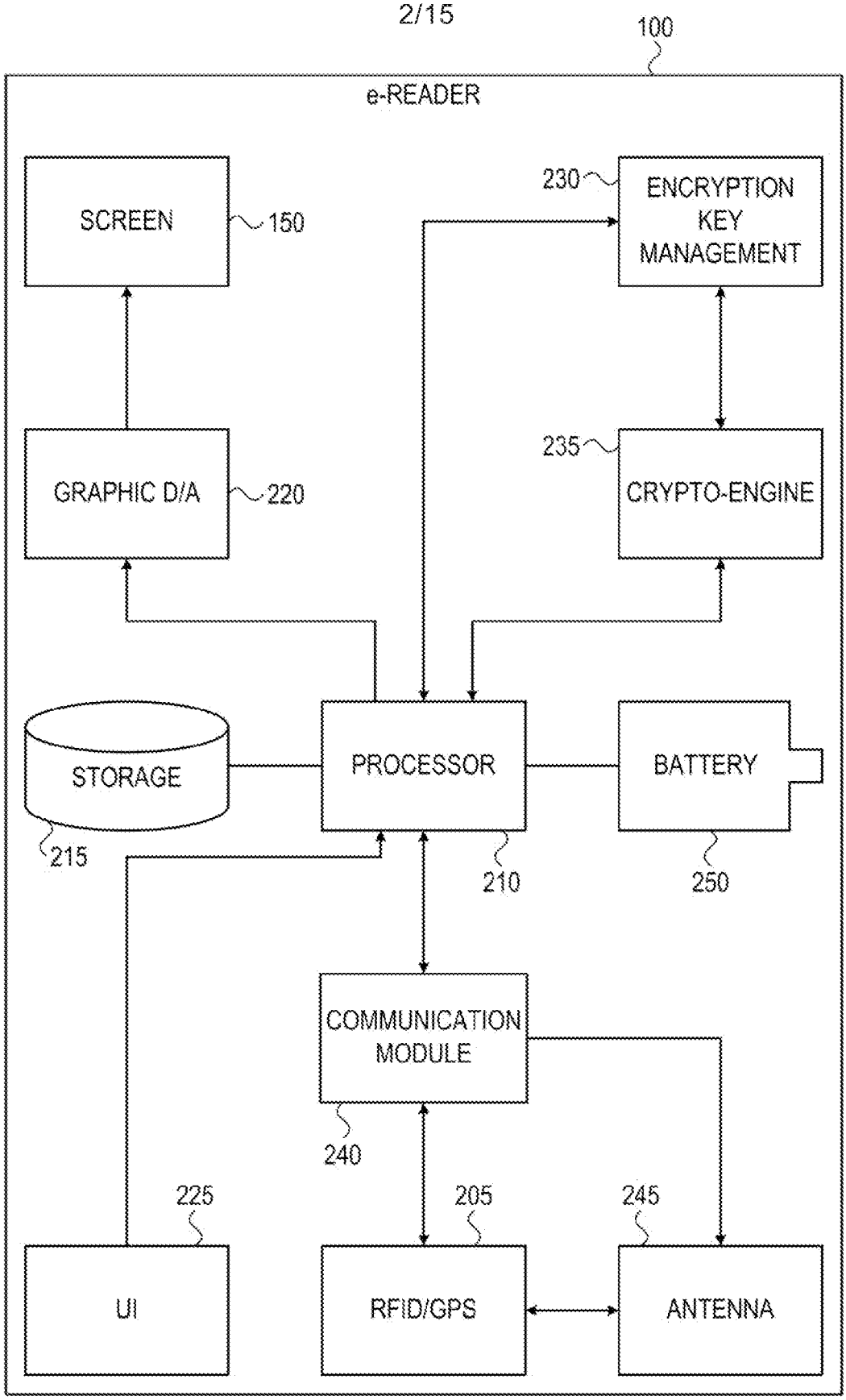
100
e-READER
SCREEN
150
230
ENCRYPTION KEY MANAGEMENT
GRAPHIC D/A
220
235
CRYPTO-ENGINE
STORAGE
215
PROCESSOR
210
BATTERY
250
COMMUNICATION MODULE
240
225
205
245
UI
RFID/GPS
ANTENNA

FIG. 2

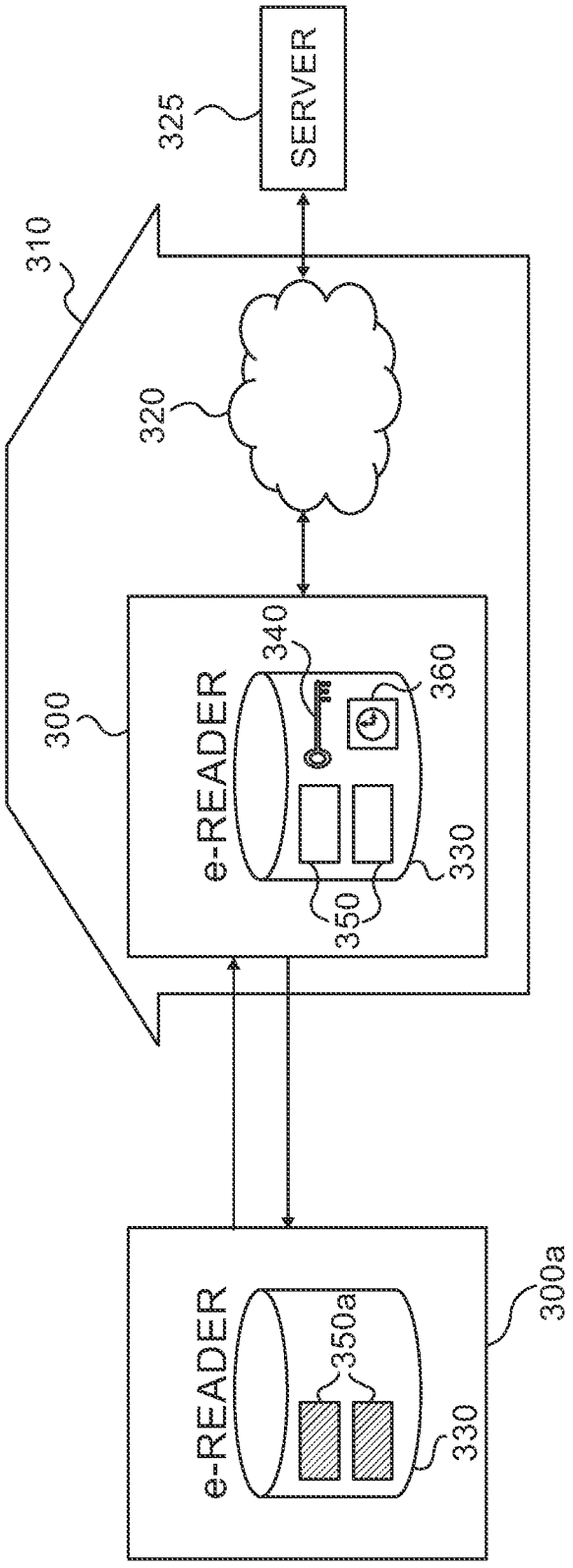

FIG. 3

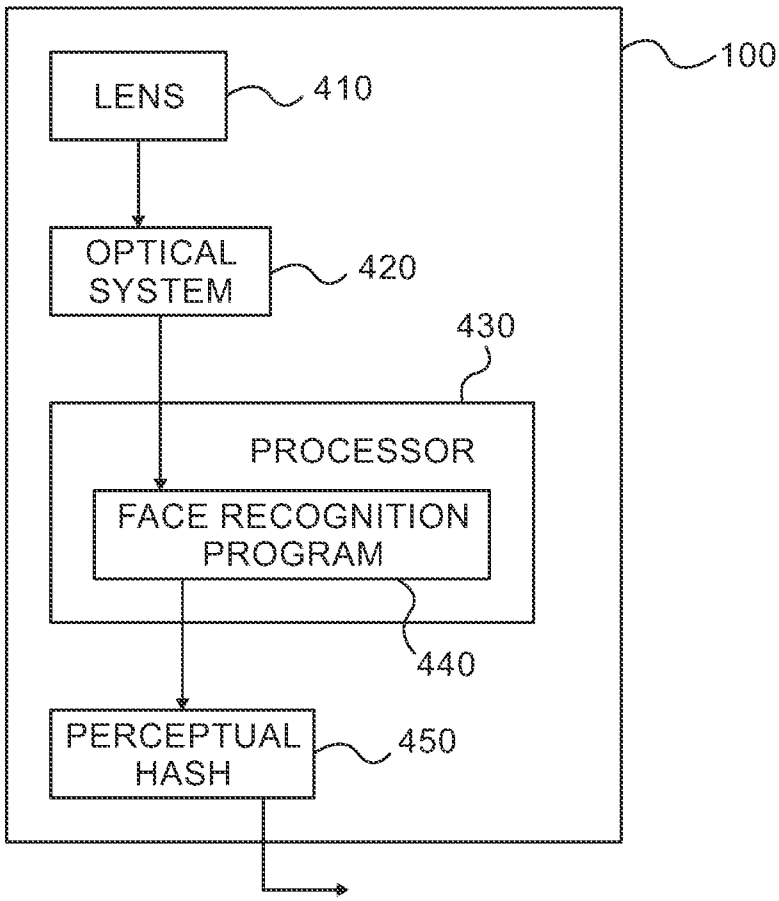
100
LENS
410
OPTICAL SYSTEM
420
430
PROCESSOR
FACE RECOGNITION PROGRAM
440
PERCEPTUAL HASH
450

FIG. 4

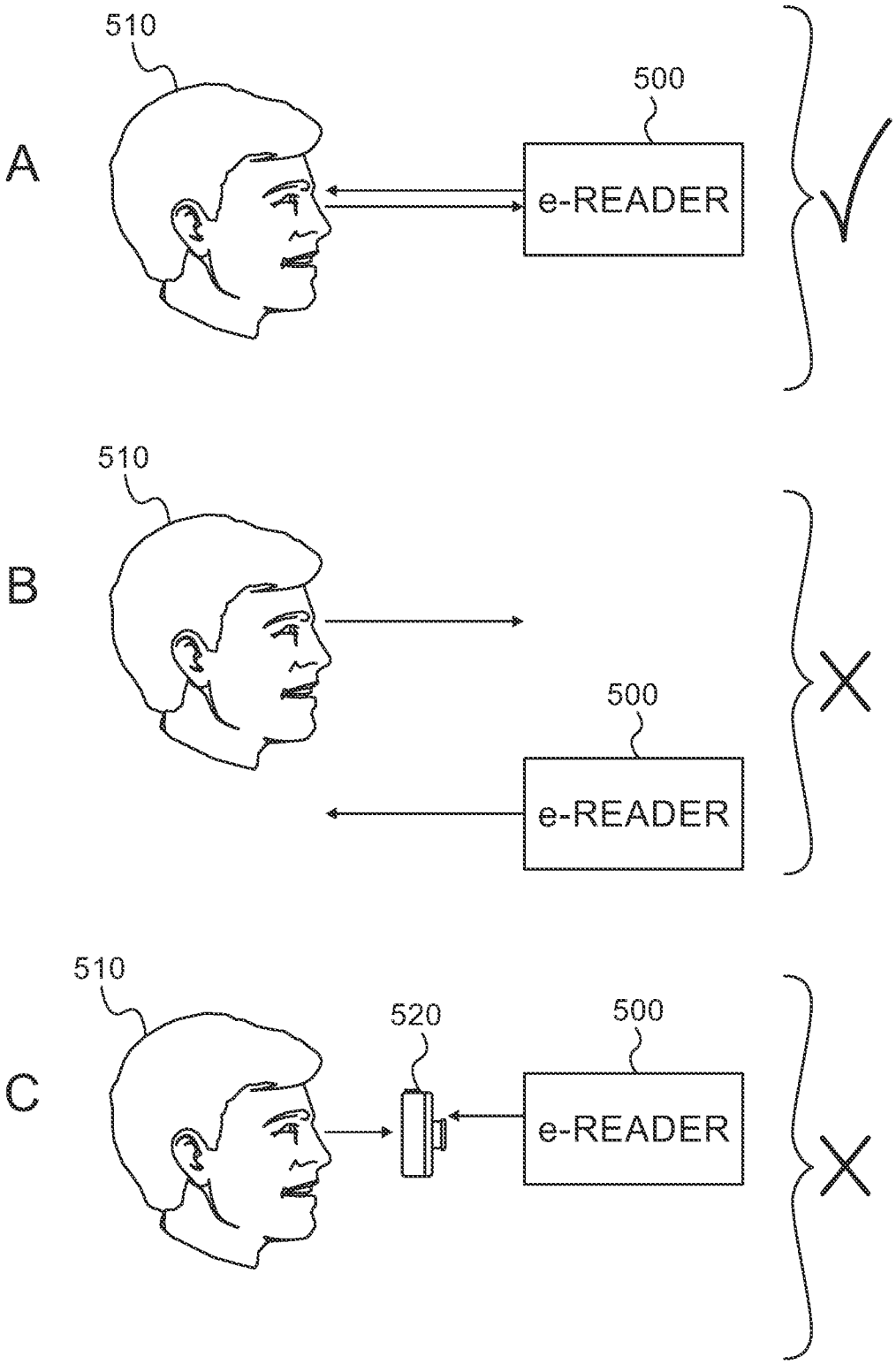

FIG. 5

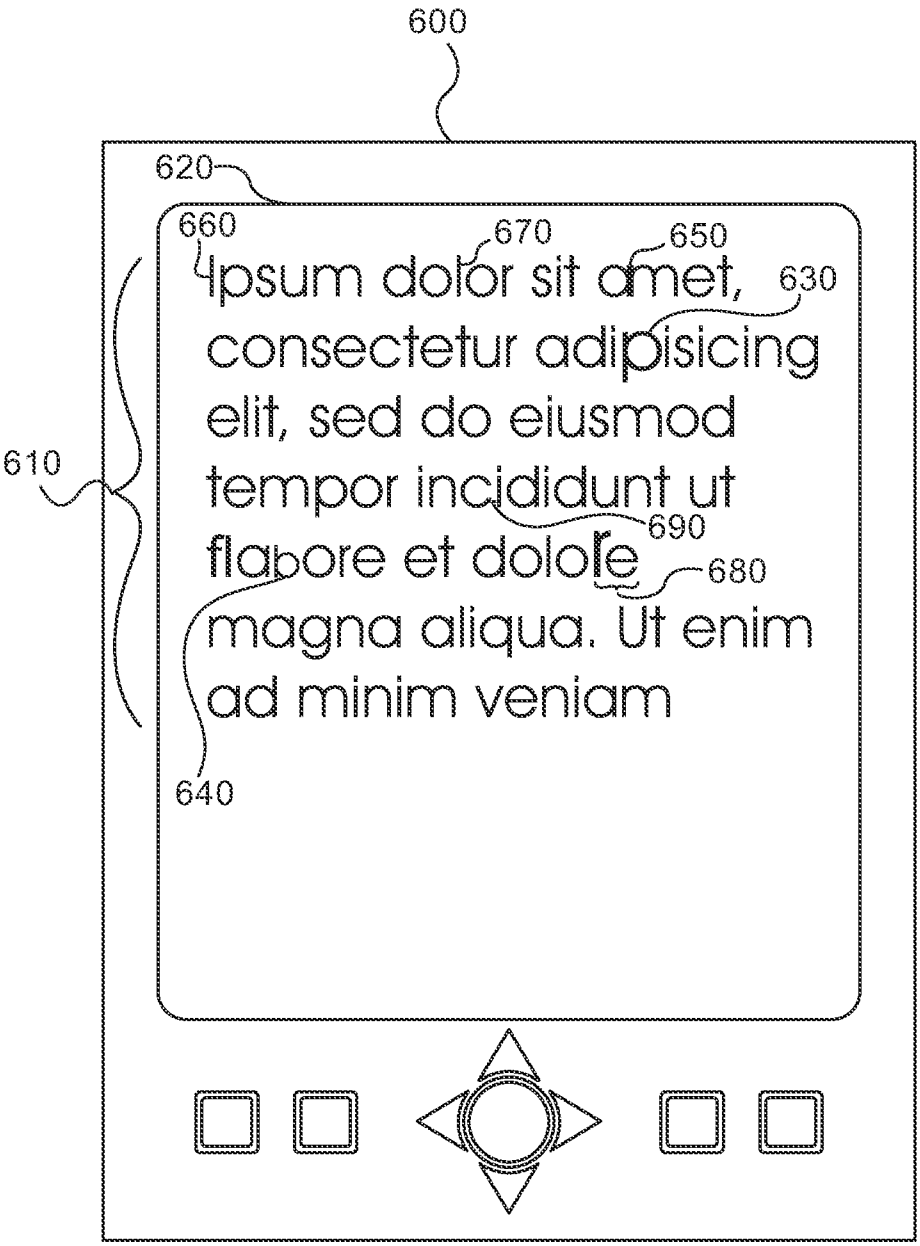
600
620
660
670
650
630
610
690
680
640
Ipsum dolor sit amet,
consectetur adipisicing
elit, sed do eiusmod
tempor incididunt ut
flabore et dolore
magna aliqua. Ut enim
ad minim veniam

FIG. 6

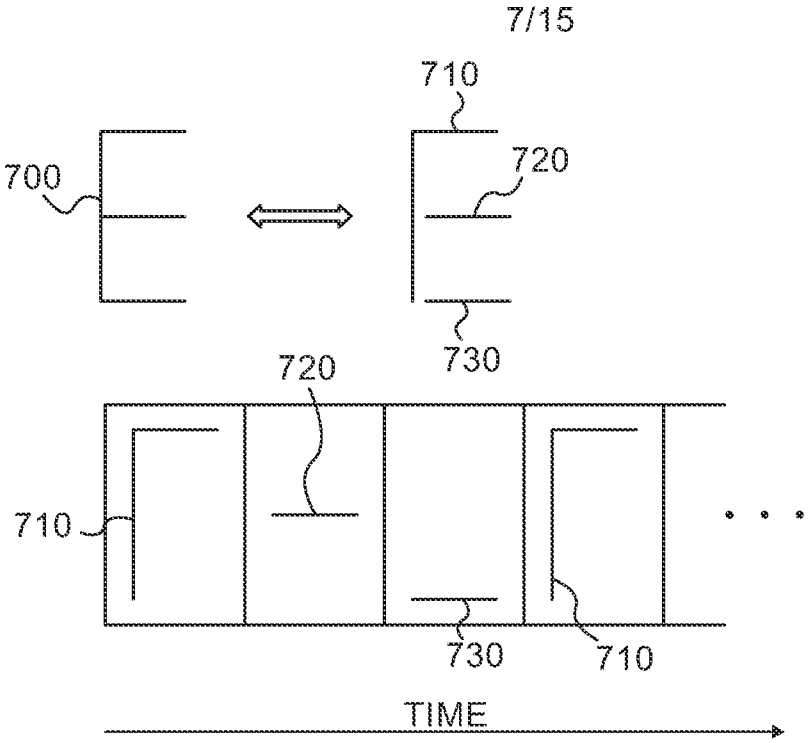
710
700
720
730
720
710
730
710
TIME

FIG. 7

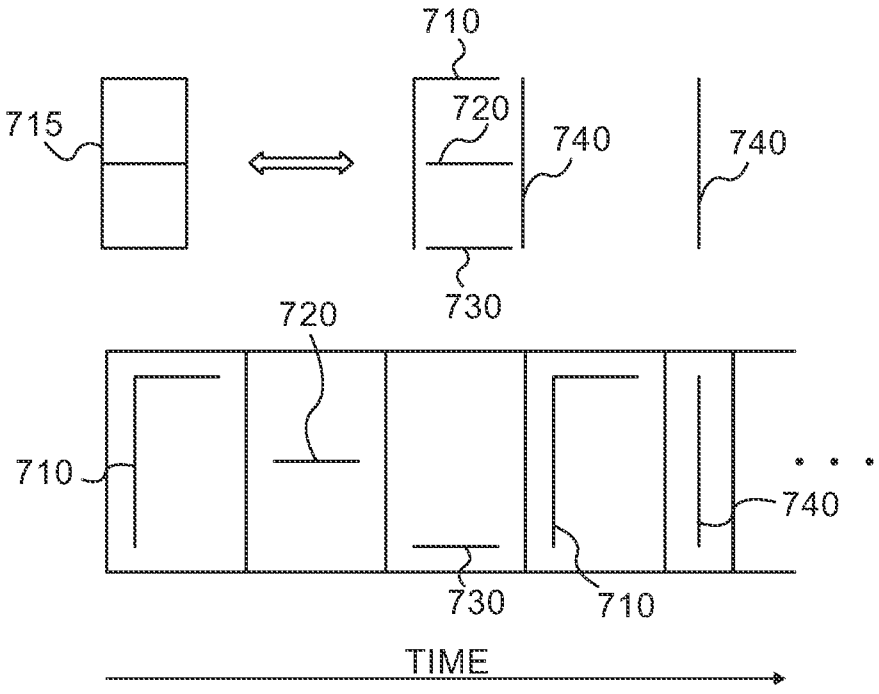
710
715
720
740
740
730
720
710
740
730
710
TIME

FIG. 7A

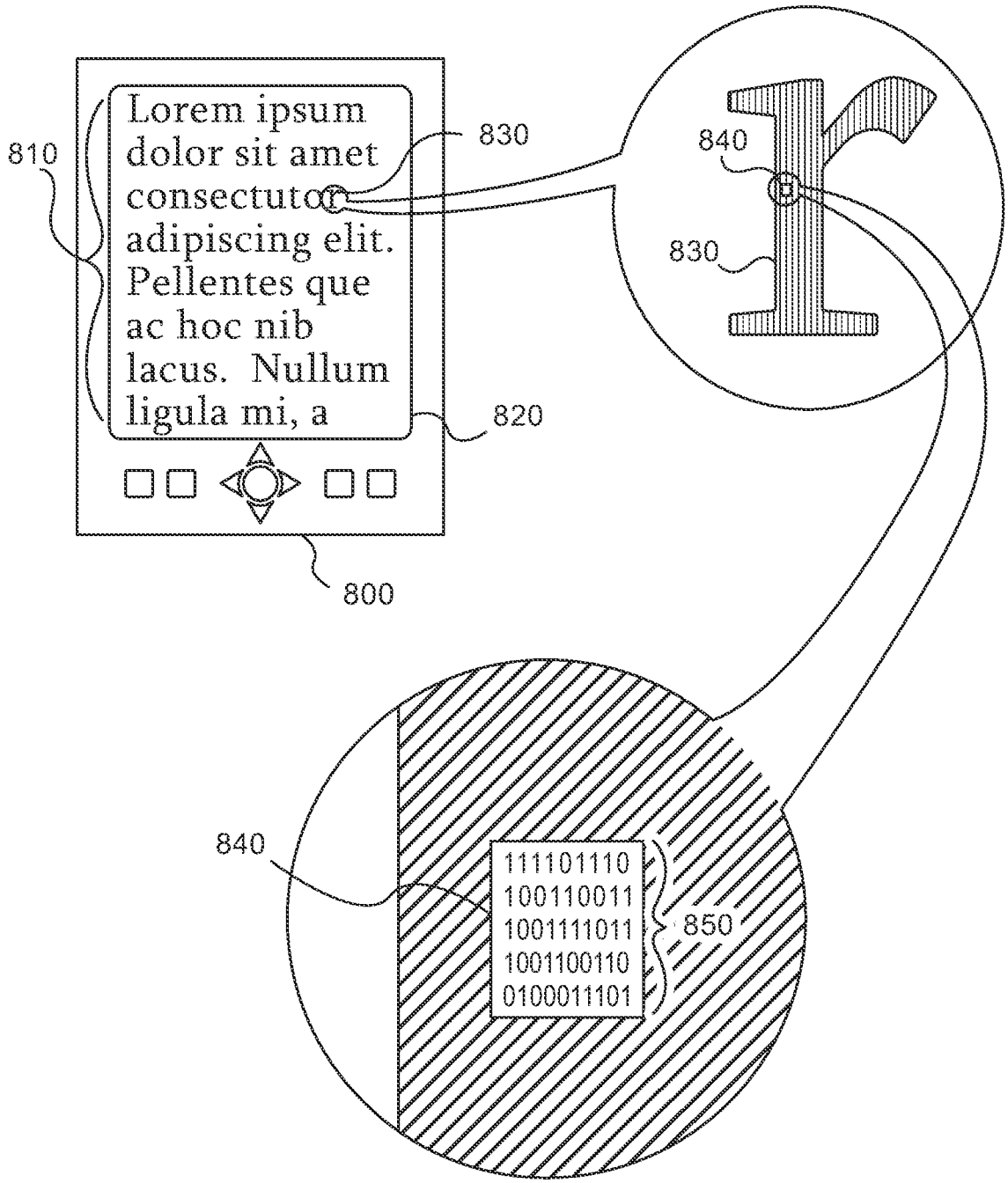
Lorem ipsum dolor sit amet consectutor adipiscing elit. Pellentes que ac hoc nib lacus. Nullum ligula mi, a
810
820
830
840
800
830
840
111101110
100110011
1001111011
1001100110
0100011101
850

FIG. 8

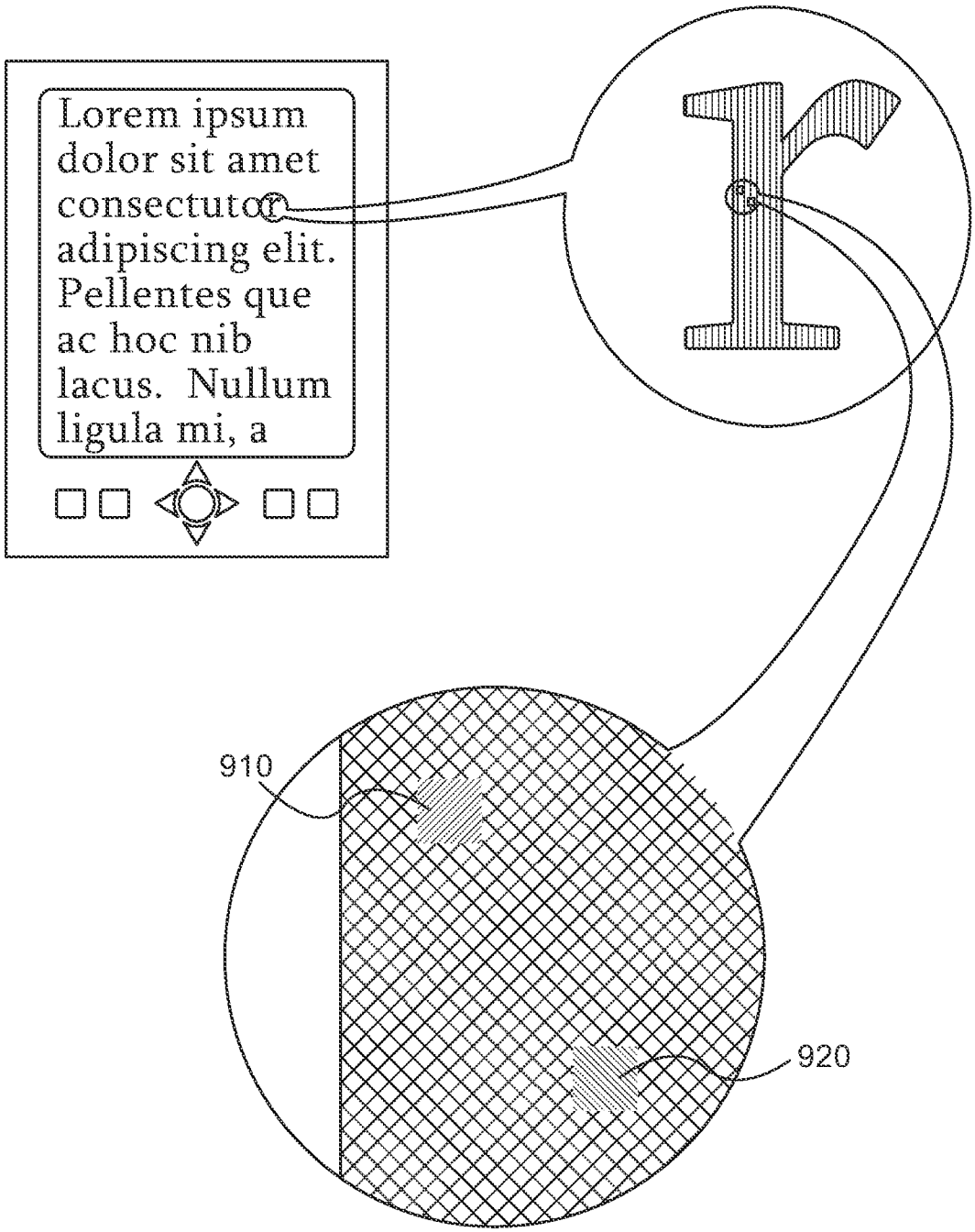
Lorem ipsum dolor sit amet consectutor adipiscing elit. Pellentes que ac hoc nib lacus. Nullum ligula mi, a
910
920

FIG. 9

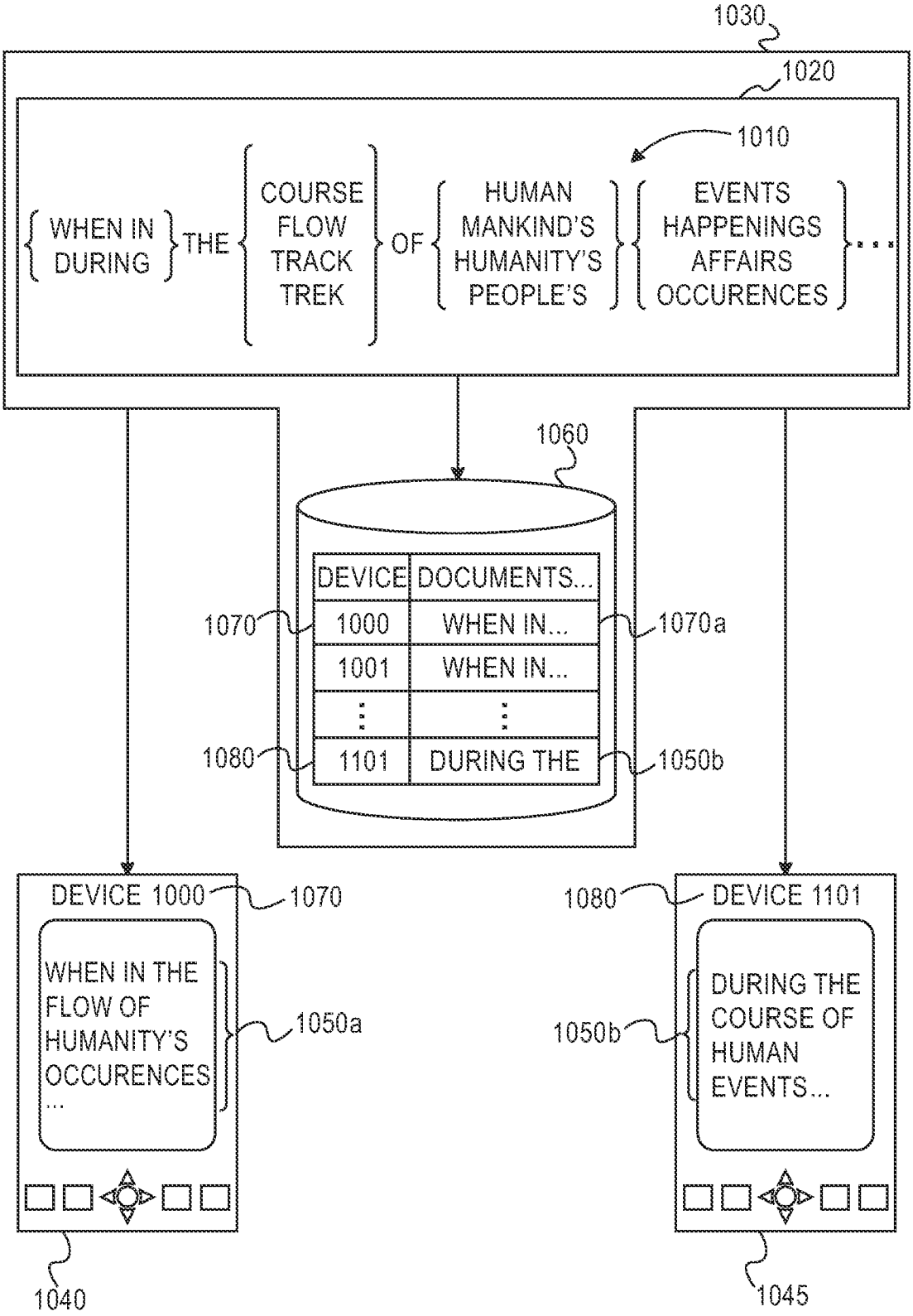
1030
1020
1010
WHEN IN
DURING
THE
COURSE
FLOW
TRACK
TREK
OF
HUMAN
MANKIND'S
HUMANITY'S
PEOPLE'S
EVENTS
HAPPENINGS
AFFAIRS
OCCURENCES
1060
DEVICE
DOCUMENTS...
1070
1000
WHEN IN...
1070a
1001
WHEN IN...
1080
1101
DURING THE
1050b
DEVICE 1000
1070
WHEN IN THE FLOW OF HUMANITY'S OCCURENCES ...
1050a
1040
1080
DEVICE 1101
DURING THE COURSE OF HUMAN EVENTS...
1050b
1045

FIG . 10

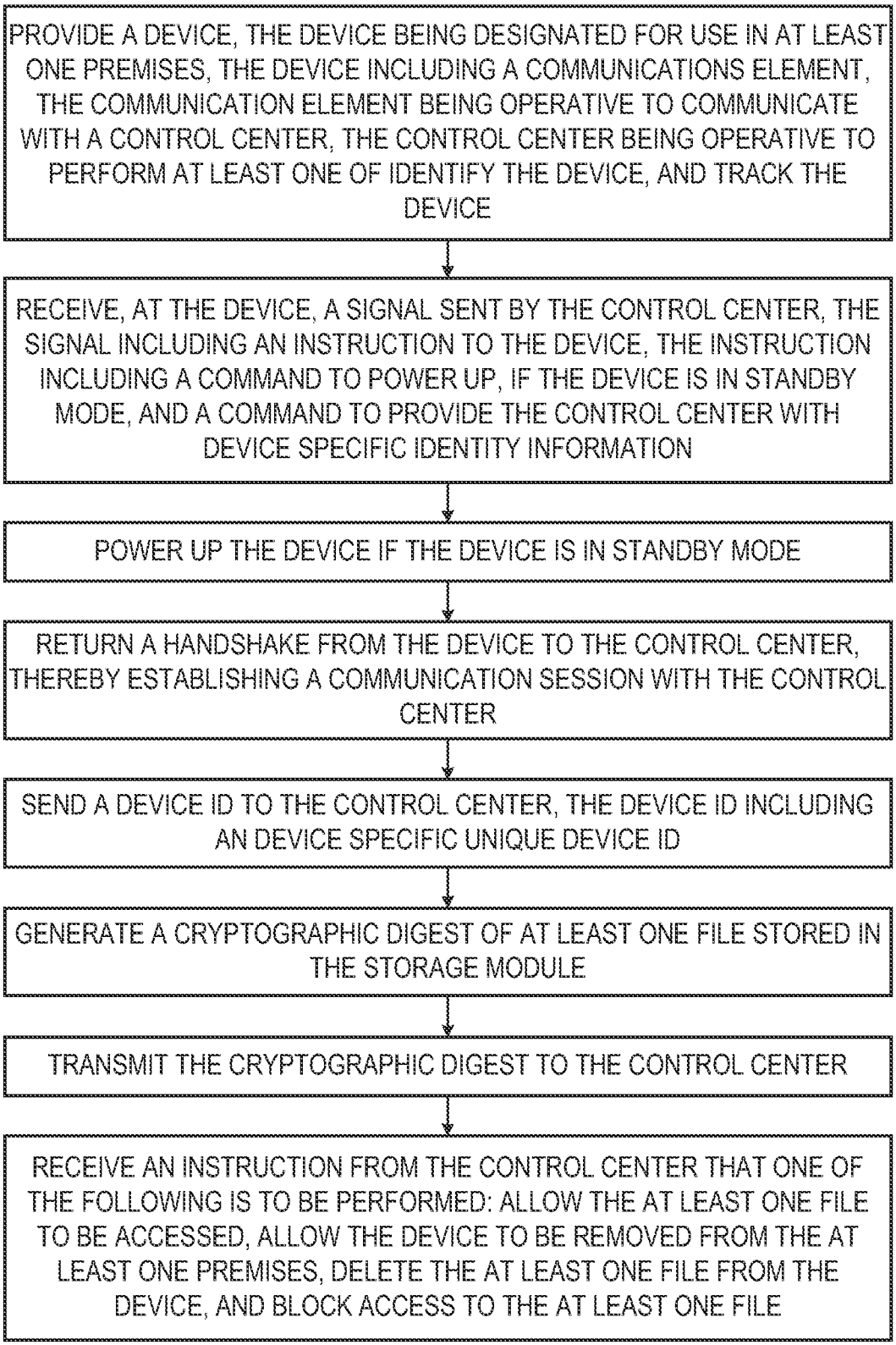
PROVIDE A DEVICE, THE DEVICE BEING DESIGNATED FOR USE IN AT LEAST ONE PREMISES, THE DEVICE INCLUDING A COMMUNICATIONS ELEMENT, THE COMMUNICATION ELEMENT BEING OPERATIVE TO COMMUNICATE WITH A CONTROL CENTER, THE CONTROL CENTER BEING OPERATIVE TO PERFORM AT LEAST ONE OF IDENTIFY THE DEVICE, AND TRACK THE DEVICE
RECEIVE, AT THE DEVICE, A SIGNAL SENT BY THE CONTROL CENTER, THE SIGNAL INCLUDING AN INSTRUCTION TO THE DEVICE, THE INSTRUCTION INCLUDING A COMMAND TO POWER UP, IF THE DEVICE IS IN STANDBY MODE, AND A COMMAND TO PROVIDE THE CONTROL CENTER WITH DEVICE SPECIFIC IDENTITY INFORMATION
POWER UP THE DEVICE IF THE DEVICE IS IN STANDBY MODE
RETURN A HANDSHAKE FROM THE DEVICE TO THE CONTROL CENTER, THEREBY ESTABLISHING A COMMUNICATION SESSION WITH THE CONTROL CENTER
SEND A DEVICE ID TO THE CONTROL CENTER, THE DEVICE ID INCLUDING AN DEVICE SPECIFIC UNIQUE DEVICE ID
GENERATE A CRYPTOGRAPHIC DIGEST OF AT LEAST ONE FILE STORED IN THE STORAGE MODULE
TRANSMIT THE CRYPTOGRAPHIC DIGEST TO THE CONTROL CENTER
RECEIVE AN INSTRUCTION FROM THE CONTROL CENTER THAT ONE OF THE FOLLOWING IS TO BE PERFORMED: ALLOW THE AT LEAST ONE FILE TO BE ACCESSED, ALLOW THE DEVICE TO BE REMOVED FROM THE AT LEAST ONE PREMISES, DELETE THE AT LEAST ONE FILE FROM THE DEVICE, AND BLOCK ACCESS TO THE AT LEAST ONE FILE

FIG. 11

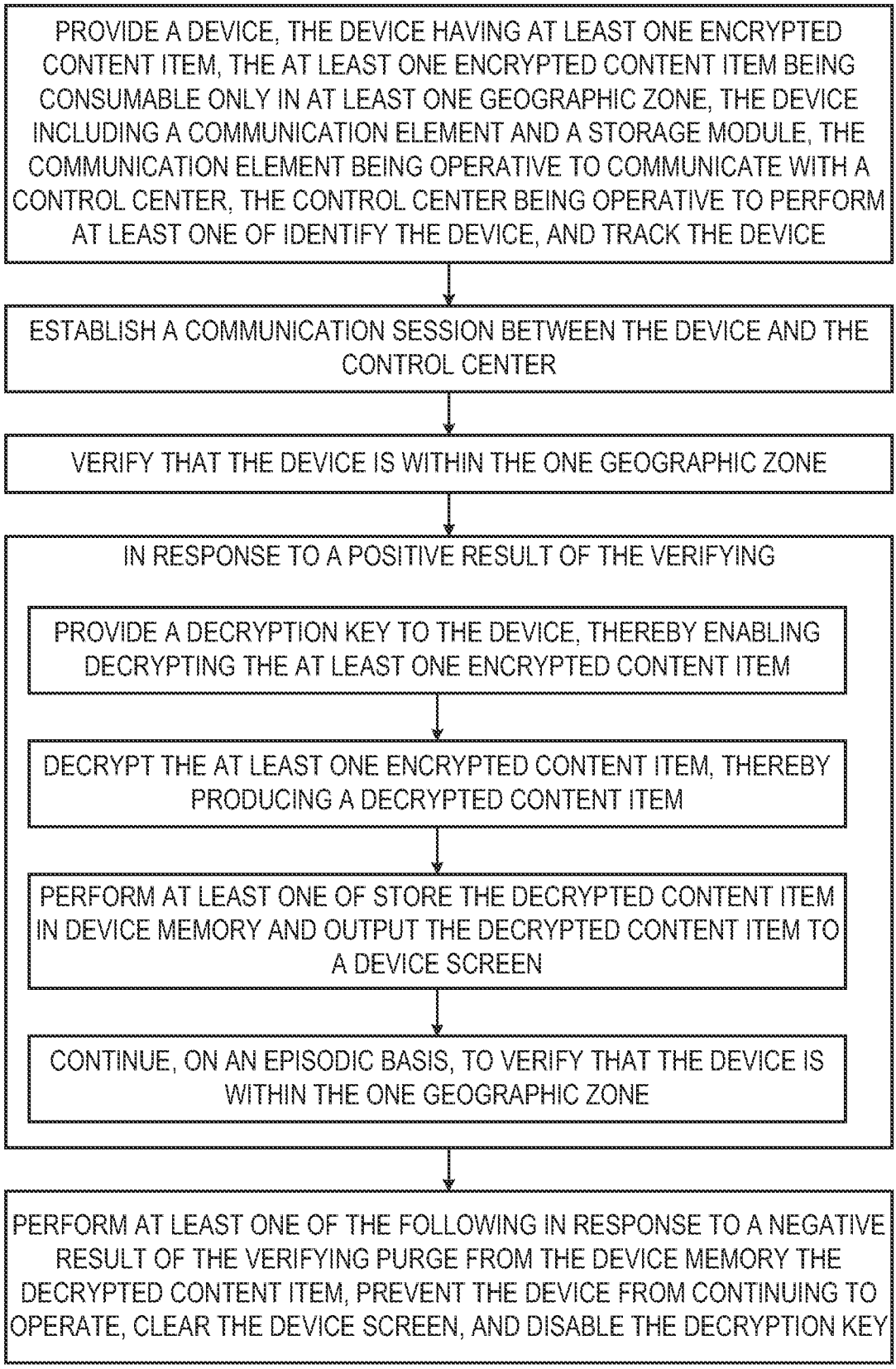
PROVIDE A DEVICE, THE DEVICE HAVING AT LEAST ONE ENCRYPTED CONTENT ITEM, THE AT LEAST ONE ENCRYPTED CONTENT ITEM BEING CONSUMABLE ONLY IN AT LEAST ONE GEOGRAPHIC ZONE, THE DEVICE INCLUDING A COMMUNICATION ELEMENT AND A STORAGE MODULE, THE COMMUNICATION ELEMENT BEING OPERATIVE TO COMMUNICATE WITH A CONTROL CENTER, THE CONTROL CENTER BEING OPERATIVE TO PERFORM AT LEAST ONE OF IDENTIFY THE DEVICE, AND TRACK THE DEVICE
ESTABLISH A COMMUNICATION SESSION BETWEEN THE DEVICE AND THE CONTROL CENTER
VERIFY THAT THE DEVICE IS WITHIN THE ONE GEOGRAPHIC ZONE
IN RESPONSE TO A POSITIVE RESULT OF THE VERIFYING
PROVIDE A DECRYPTION KEY TO THE DEVICE, THEREBY ENABLING DECRYPTING THE AT LEAST ONE ENCRYPTED CONTENT ITEM
DECRYPT THE AT LEAST ONE ENCRYPTED CONTENT ITEM, THEREBY PRODUCING A DECRYPTED CONTENT ITEM
PERFORM AT LEAST ONE OF STORE THE DECRYPTED CONTENT ITEM IN DEVICE MEMORY AND OUTPUT THE DECRYPTED CONTENT ITEM TO A DEVICE SCREEN
CONTINUE, ON AN EPISODIC BASIS, TO VERIFY THAT THE DEVICE IS WITHIN THE ONE GEOGRAPHIC ZONE
PERFORM AT LEAST ONE OF THE FOLLOWING IN RESPONSE TO A NEGATIVE RESULT OF THE VERIFYING PURGE FROM THE DEVICE MEMORY THE DECRYPTED CONTENT ITEM, PREVENT THE DEVICE FROM CONTINUING TO OPERATE, CLEAR THE DEVICE SCREEN, AND DISABLE THE DECRYPTION KEY

FIG. 12

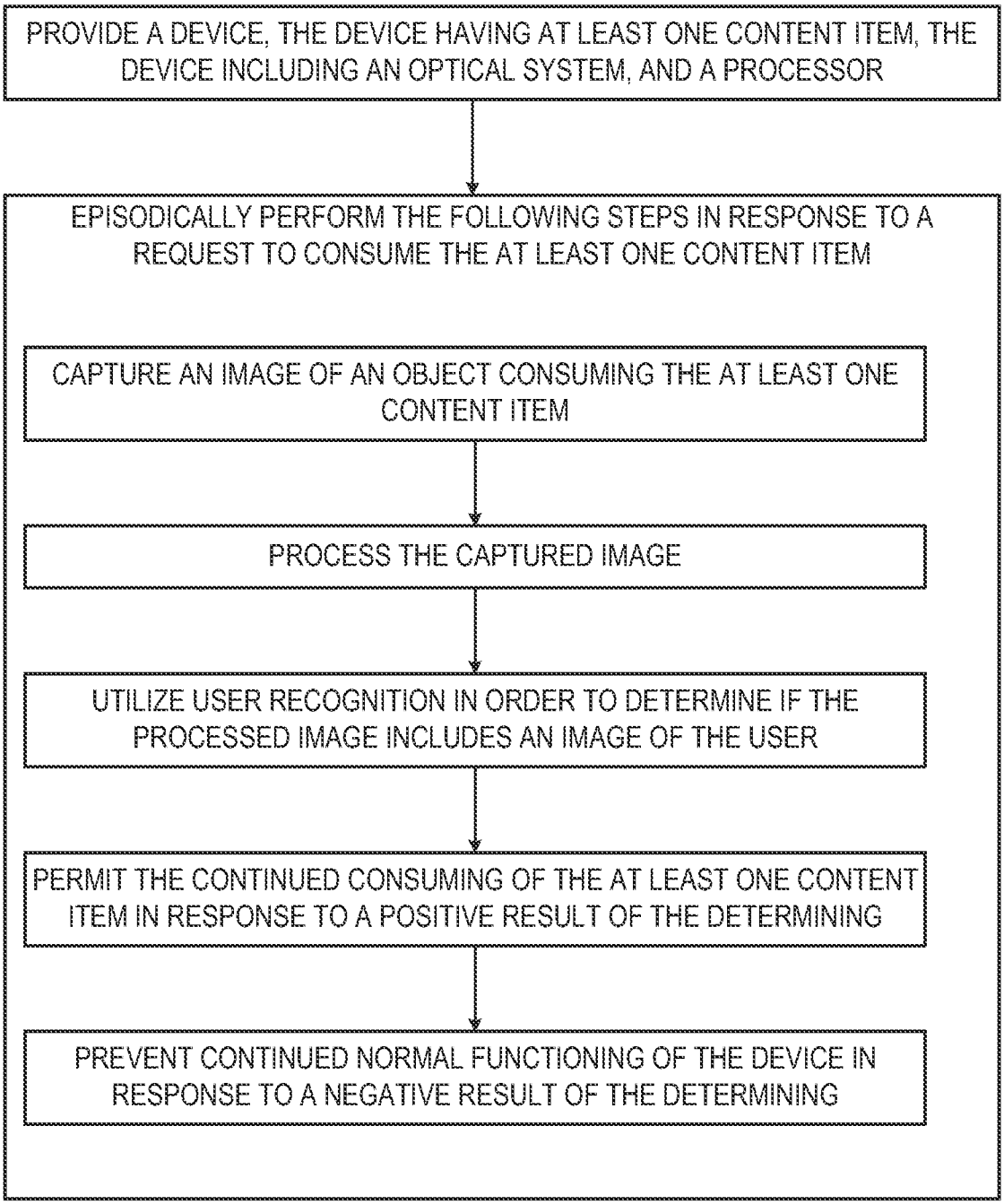
PROVIDE A DEVICE, THE DEVICE HAVING AT LEAST ONE CONTENT ITEM, THE DEVICE INCLUDING AN OPTICAL SYSTEM, AND A PROCESSOR
EPISODICALLY PERFORM THE FOLLOWING STEPS IN RESPONSE TO A REQUEST TO CONSUME THE AT LEAST ONE CONTENT ITEM
CAPTURE AN IMAGE OF AN OBJECT CONSUMING THE AT LEAST ONE CONTENT ITEM
PROCESS THE CAPTURED IMAGE
UTILIZE USER RECOGNITION IN ORDER TO DETERMINE IF THE PROCESSED IMAGE INCLUDES AN IMAGE OF THE USER
PERMIT THE CONTINUED CONSUMING OF THE AT LEAST ONE CONTENT ITEM IN RESPONSE TO A POSITIVE RESULT OF THE DETERMINING
PREVENT CONTINUED NORMAL FUNCTIONING OF THE DEVICE IN RESPONSE TO A NEGATIVE RESULT OF THE DETERMINING

FIG. 13

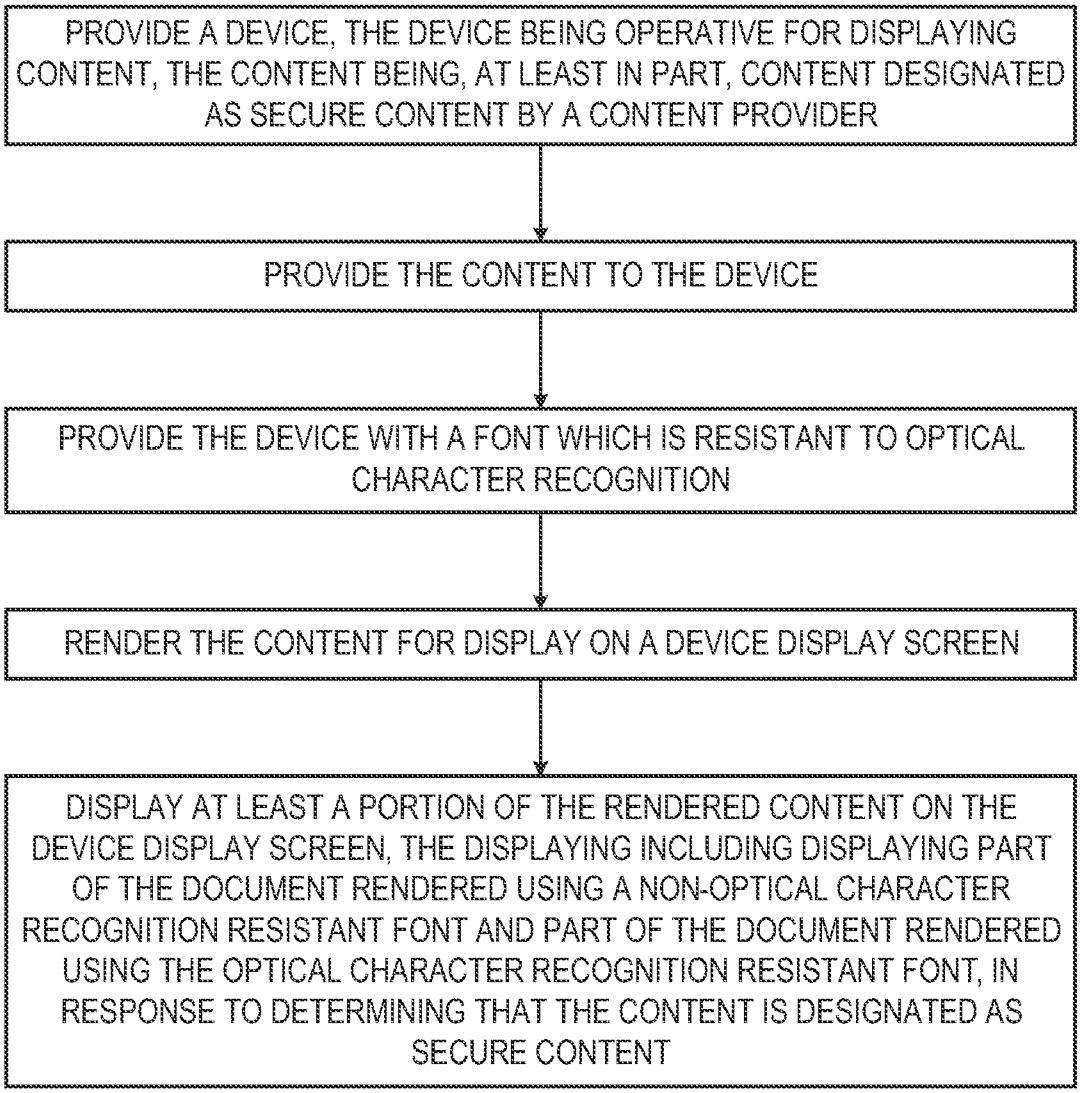
PROVIDE A DEVICE, THE DEVICE BEING OPERATIVE FOR DISPLAYING CONTENT, THE CONTENT BEING, AT LEAST IN PART, CONTENT DESIGNATED AS SECURE CONTENT BY A CONTENT PROVIDER
PROVIDE THE CONTENT TO THE DEVICE
PROVIDE THE DEVICE WITH A FONT WHICH IS RESISTANT TO OPTICAL CHARACTER RECOGNITION
RENDER THE CONTENT FOR DISPLAY ON A DEVICE DISPLAY SCREEN
DISPLAY AT LEAST A PORTION OF THE RENDERED CONTENT ON THE DEVICE DISPLAY SCREEN, THE DISPLAYING INCLUDING DISPLAYING PART OF THE DOCUMENT RENDERED USING A NON-OPTICAL CHARACTER RECOGNITION RESISTANT FONT AND PART OF THE DOCUMENT RENDERED USING THE OPTICAL CHARACTER RECOGNITION RESISTANT FONT, IN RESPONSE TO DETERMINING THAT THE CONTENT IS DESIGNATED AS SECURE CONTENT

FIG. 14

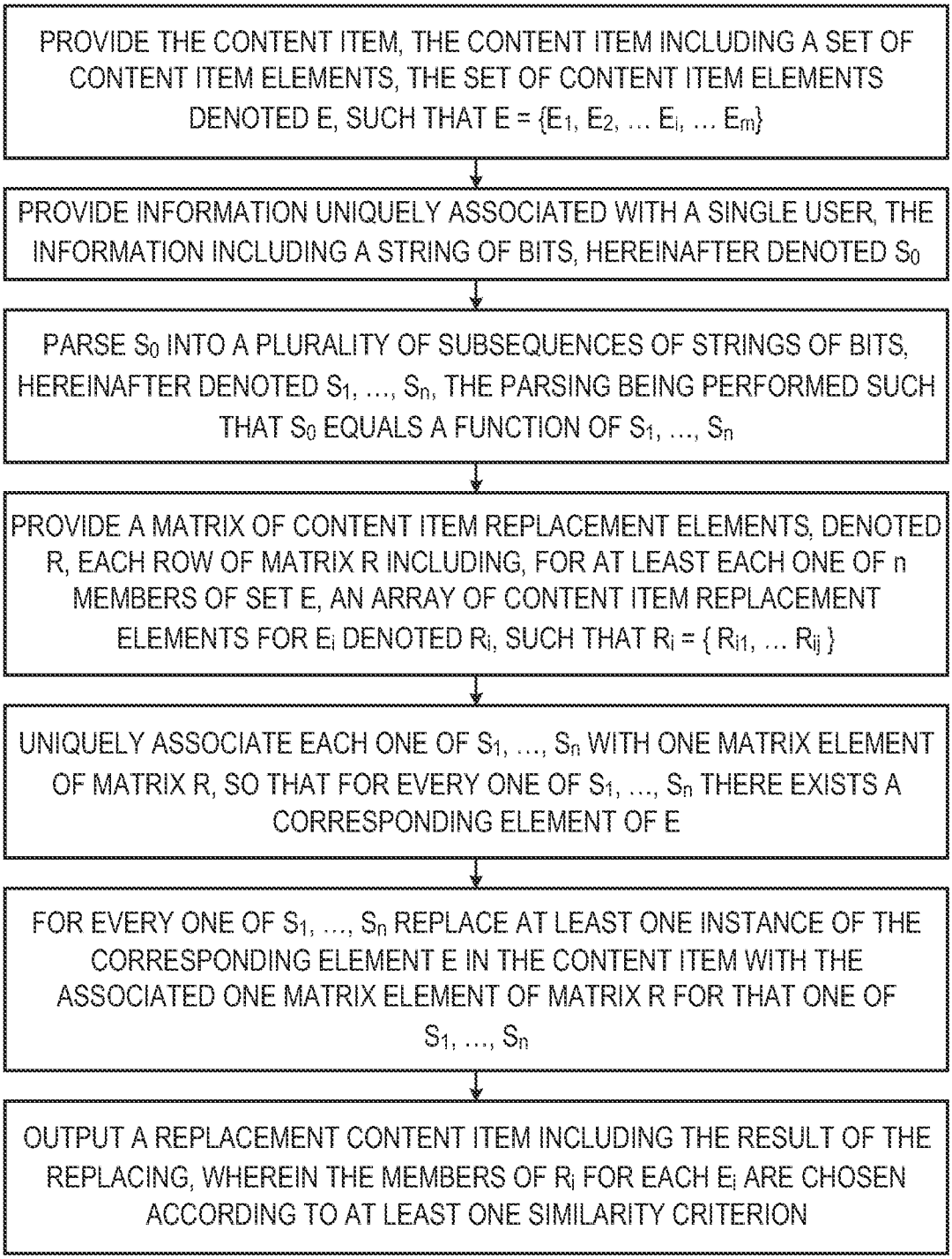
PROVIDE THE CONTENT ITEM, THE CONTENT ITEM INCLUDING A SET OF CONTENT ITEM ELEMENTS, THE SET OF CONTENT ITEM ELEMENTS DENOTED E, SUCH THAT E = {E1, E2, … Ei, … Em}
PROVIDE INFORMATION UNIQUELY ASSOCIATED WITH A SINGLE USER, THE INFORMATION INCLUDING A STRING OF BITS, HEREINAFTER DENOTED S0
PARSE S0 INTO A PLURALITY OF SUBSEQUENCES OF STRINGS OF BITS, HEREINAFTER DENOTED S1, …, Sn, THE PARSING BEING PERFORMED SUCH THAT S0 EQUALS A FUNCTION OF S1, …, Sn
PROVIDE A MATRIX OF CONTENT ITEM REPLACEMENT ELEMENTS, DENOTED R, EACH ROW OF MATRIX R INCLUDING, FOR AT LEAST EACH ONE OF n MEMBERS OF SET E, AN ARRAY OF CONTENT ITEM REPLACEMENT ELEMENTS FOR Ei DENOTED Ri, SUCH THAT Ri = { Ri1, … Rij }
UNIQUELY ASSOCIATE EACH ONE OF S1, …, Sn WITH ONE MATRIX ELEMENT OF MATRIX R, SO THAT FOR EVERY ONE OF S1, …, Sn THERE EXISTS A CORRESPONDING ELEMENT OF E
FOR EVERY ONE OF S1, …, Sn REPLACE AT LEAST ONE INSTANCE OF THE CORRESPONDING ELEMENT E IN THE CONTENT ITEM WITH THE ASSOCIATED ONE MATRIX ELEMENT OF MATRIX R FOR THAT ONE OF S1, …, Sn
OUTPUT A REPLACEMENT CONTENT ITEM INCLUDING THE RESULT OF THE REPLACING, WHEREIN THE MEMBERS OF Ri FOR EACH Ei ARE CHOSEN ACCORDING TO AT LEAST ONE SIMILARITY CRITERION

FIG. 15

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2010/052783

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 243 652 A (TEARE MELVIN J [US] ET AL) 7 September 1993 (1993-09-07) column 2 - column 4	1-22
X	WO 02/089442 A1 (NOKIA CORP [FI]) 7 November 2002 (2002-11-07) page 6, last paragraph - page 11, last paragraph	1-22
X	US 2008/147434 A1 (DURAND JULIAN [US] ET AL) 19 June 2008 (2008-06-19) paragraph [0022] - paragraph [0046]	1-22

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 September 2010	01/10/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Alecu, Mihail

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2010/052783

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 166 688 A (CROMER DARYL CARVIS [US] ET AL) 26 December 2000 (2000-12-26) * abstract column 2; figure 3 column 3, line 22 - column 4, line 42 column 6, line 7 - line 27	1-22
A	WO 03/034192 A1 (ENUVIS INC [US]) 24 April 2003 (2003-04-24) page 17 - page 18	1-10
A	WO 2005/057846 A1 (NOKIA CORP [FI]; RANTALAHTI ANTTI [FI]) 23 June 2005 (2005-06-23) page 6 page 10 page 12, last paragraph - page 13, paragraph 1	1-22

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2010/052783

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5243652 A	07-09-1993	WO 9408408 A1	14-04-1994
WO 02089442 A1	07-11-2002	EP 1384363 A1	28-01-2004
		JP 2004530210 T	30-09-2004
		JP 2007188534 A	26-07-2007
		US 2003023578 A1	30-01-2003
US 2008147434 A1	19-06-2008	NONE	
US 6166688 A	26-12-2000	NONE	
WO 03034192 A1	24-04-2003	NONE	
WO 2005057846 A1	23-06-2005	AU 2003304608 A1	29-06-2005
		CN 1879345 A	13-12-2006
		EP 1692812 A1	23-08-2006
		US 2007283420 A1	06-12-2007