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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 August 2003 (14.08.2003)

PCT

(10) International Publication Number
WO 03/067401 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/EP03/01120

(22) International Filing Date: 4 February 2003 (04.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/067,403 7 February 2002 (07.02.2002) US

(71) Applicant: ACTIVCARD IRELAND, LIMITED [IE/IE]; -, 30 Herbert Street, 2 DUBLIN (IE).

(72) Inventor: HAMID, Laurence; -, 561 Brookridge Crescent, OTTAWA, Ontario K4A 1Z3 (CA).

(74) Agent: CABINET JP COLAS; -, 37, avenue Franklin D. Roosevelt, F-75008 PARIS (FR).

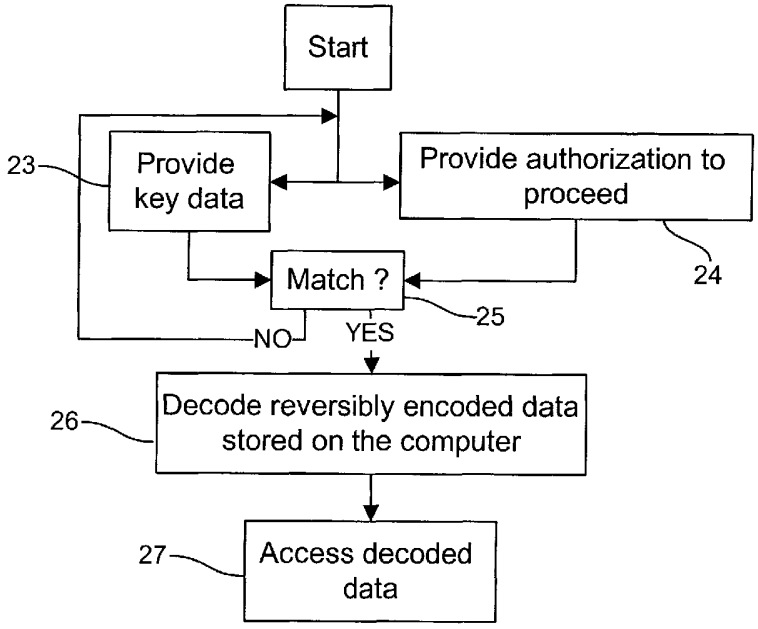
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT,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

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

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SUPPORT FOR MULTIPLE LOGIN METHODS.



(57) Abstract: A method of securing security data stored on a computer system is disclosed. The method comprises providing a data key to the computer system. The data key is used for transforming the security data in a reversible fashion to produce an encoded secure data such that the data key is required in order to perform a reverse transform and extract the security data from the encoded secure data. The encoded secure data are stored secure data in a fashion such that a user authorization process is used to retrieve the encoded secure data. Furthermore, the encoded secure data are stored such that the data key and the user authorization process in combination provide access to the security data and such that the stored data within the computer system is encoded.

WO 03/067401 A1

SUPPORT FOR MULTIPLE LOGIN METHODS

Field of the Invention

[001] The present invention relates to a method for allowing people to access data through a plurality of mechanisms and more precisely to a method for supporting multiple login.

Background of the Invention

[002] Computer security is fast becoming an important issue. With the proliferation of computers and computer networks into all aspects of business and daily life--financial, medical, education, government, and communications--the concern over secure file access and data communications is growing. One method of preventing unauthorized access to files is by using encryption and cipher techniques. These techniques convert data into other forms of data in a fashion that is reversible. Once encrypted, the data is unintelligible unless first decrypted. RSA, DES and CAST are known encryption techniques, which are currently believed to provide sufficient security for computer communications and files.

[003] Each of these encryption techniques uses a cipher key. Such a key is crucial to the encryption/decryption process. Anyone with a correct key can access information that has previously been encrypted using that key. The entry of the key from the keyboard is impractical since a user must remember such a key for entry and as such is liable to be discovered by an individual desiring access to existing encrypted files.

[004] Further, there is great concern over communication of keys within commercial and governmental offices. It is common for users to inform others of their keys or to transfer their keys to others for use during holidays, sick days, or even as a reminder of the key should the user forget. Also, keys are often written down at the workstation in case a user should forget. Such written passwords undermine the security of many systems.

[005] In DES encryption, the key is a numerical value, for example 56 bits in length. Such a key can be used to encrypt and subsequently to decrypt data. The security of the data once encrypted is sufficient that the key is required to access the data in an intelligible form. Thus the security of the data is related to the security of the key.

[006] Some encryption systems use keys stored on the same device as the encrypted files. This is akin to storing a lock and its key in the same location. A knowledgeable user gaining access to the device could locate the key and access the data. Other encryption systems use keys stored on portable cards. Such a key is accessed via a password entered at the keyboard. Other users can take such a portable card and such a password can be discovered. The portable card is equally subject to transfer between employees and improper storage--at a user's desk.

[007] A security access system that provides substantially secure access and does not require a password or access code is a biometric identification system. A biometric identification system accepts unique biometric information from a user and identifies the user by matching the information against information belonging to registered users of the system.

[008] Unfortunately, a device specifically designed to gain access to a system secured through biometric information is plausible. Such a device connects to a personal computer in a same fashion as a contact-imaging device but does not require provision of biometric information. Some forms of infiltrating biometric systems include a record-play back attack wherein biometric information is intercepted, recorded, and then played back at a later time; repeat pattern sending, wherein patterns are sent to the biometric identification system until an authorization occurs; etc. It would be advantageous to restrict the use of third party contact imaging systems with a security identification system in order to improve security.

[009] Typically, data or information is secured on a hard drive by using an encryption key to encrypt data and decryption key to restore the data. Thus, providing a password to the system activates the encryption/decryption key that allows

encryption or decryption of the data. A major concern exists when considering a security system based upon such system; the key and the encrypted data are stored on the same hard drive. As such, knowing a user's password give access to the encrypted data.

Object of the Invention

[0010] It is an object of this invention to provide a key data to a system, the key data being encoded using a data value in the form of a password.

[0011] It is another object of this invention to transform the key data using a reversible hash process.

[0012] It is a further object of this invention to allow an individual to access encrypted data through a plurality of mechanisms.

[0013] It is another further object of this invention to provide a method for supporting multiple login.

Summary of the Invention

[0014] In accordance with a preferred embodiment of the present invention, there is provided a method of securing security data stored on a computer system comprising the steps of: providing a data key to the computer system; transforming the security data with the data key in a reversible fashion to produce encoded secure data such that the data key is required in order to perform a reverse transform and extract the security data from the encoded secure data; and, storing the encoded secure data in a fashion such that a user authorization process is used to retrieve the encoded secure data such that the data key and the user authorization process in combination, provide access to the security data and such that the stored data within the computer system is encoded.

[0015] In accordance with another preferred embodiment of the present invention, there is provided a method of securing security data stored on a computer system

comprising the steps of: providing a biometric information source and comparing the biometric information source against stored templates associated with the biometric information source; and for, in dependence upon a comparison result pairing biometric information source with a first individual identity; providing a data key associated with a second individual identity; the data key being other than stored on the computer system; retrieving encoded security data associated with the biometric information, and using the key data for decoding the encoded security data

[0016] In accordance with another preferred embodiment of the present invention, there is provided a method of securing data stored on a computer system comprising the steps of: providing a first information sample to a computer system; hashing the first information sample to produce a first hash value; encoding key data in dependence upon the first hash value to produce first security data, the key data for use in decoding stored encoded data; providing at least one biometric information sample; securing the first security data in dependence upon at least one of the at least one biometric information sample.

Brief Description of the Drawings

[0017] Exemplary embodiments of the invention will now be described in conjunction with the following drawings, in which:

[0018] Fig. 1 is a flow diagram of a prior art method of associating a password to a fingerprint upon a match of a fingerprint with an associated template;

[0019] Fig. 2a is a flow diagram of a method of securing security data stored on a computer system;

[0020] Fig. 2b shows a method of accessing the secured data stored on a computer system according to a preferred embodiment of the present invention;

[0021] Fig. 3 is a flow diagram of a method of getting an authorization to proceed according to the invention.

Detailed Description of the Invention

[0025] In password based security systems, secure data such as encryption keys are stored encoded based on the password to access same. In effect, a password must be provided in order to access the encryption keys stored within the system. Since the password is not stored anywhere within the data store, it is very difficult to decode the encryption keys without having actual knowledge of the password.

[0026] The security systems wherein biometric information is used for identifying and authorizing access to an individual mostly rely on a prior art method as shown in Fig.1. After biometric information sample, in a form of a fingertip for example, has been provided to a system at step 10, the fingertip is imaged and the fingerprint is characterized at step 11. During the process of identification, the fingerprint is compared to stored templates associated with fingerprints of the person – for a one-to-one identification system - or of any person susceptible to access the system – in a one-to-many identification system at step 12. Upon a positive result of the comparison, when there is a match between the provided fingerprint and a stored template associated with a fingerprint at step 13, the system provides a password associated with the stored template at step 14 and the user is identified and authorized at step 15. According to such a method, passwords are stored with the templates giving rise to security concerns. Moreover, when the system uses encryption to secure the passwords, the decryption key is stored within the system and as such a skilled person may find the decryption key given sufficient time by simply mining the data stored.

[0027] The use of a biometric imaging device with a personal computer is considered inevitable. Unfortunately, a sample of biometric information is unchanging. Once a person has left their fingerprint on a table, or a glass, or a window, it is available to everyone. Once someone is in possession of a fingerprint, that fingerprint is known and cannot easily be modified. Therefore, data cannot simply be encoded using fingerprint data.

[0028] A major problem with a security system as described is that the password for accessing to the data is stored on the hard drive secured by the biometric information. Furthermore, the password when provided gives access to an encryption/decryption key on the same system or another system. When the key is decoded, the data are retrievable in an intelligible human language. As is apparent to a person with skill in the art, the key and the encrypted data are stored in a same system. As such, as soon as a user's password is found by an unauthorized person – for example through a process of data mining, the encryption/decryption key and the encrypted data stored on the same hard drive are accessible, and the system security is breached.

[0029] To overcome such a major inconvenience, Fig. 2a illustrates in flow diagram a method of securing security data stored on a computer system. Typically, for securing data on a computer system, key data in the form of a password for example is provided to the computer system or is generated therein at step 20. The key data is typically associated with a single user or group. For example, the key data is in the form of a 128-bit encryption key. According to the invention, the key data is encoded using a data value in the form of a password provided by a user at step 21. The transformation of the key data, according to the present invention, comprises a reversible hash process.

[0030] Preferably, the password is also hashed in an irreversible fashion and stored on the system to allow for password validation at step 22. An example of such a hash process is described below. Assuming a user's password is a series of symbols related to the user, as for example the user's name, the password is hashed to provide a series of symbols representing a transformation of the password into numerals and a conversion using a hexadecimal based numeric system. A result of the hashing procedure is 41 4E 4E 45. After the encoding step, the series of symbols is irreversibly encoded to provide a set of values. The set of values obtained is stored within the system to allow for comparison of provided passwords to ensure that they are correct.

[0031] As is evident to those of skill in the art, the password is not stored within the system. The key data is encoded with the password and can be decoded therewith. A password provided to the system is verifiable by hashing it and comparing the result to the stored hash result. That said, the stored hash result is not useful for uniquely determining the password.

[0032] Advantageously, what has been typed in by a user to encode any convenient data key, in the case of a password for example, is unknown because it is not stored on the hard drive. As such, someone trying to break into the system using data mining software for example will fail to find the password because none is stored in the system. What can eventually be found is an encoded key, or PIN, or access code that is useless to the hacker absent the password, and a hashed password.

[0033] The key data, which is an encoded key, is used for encoding accessible data. Encoding data transform them from an accessible data onto an inaccessible data. For example, if the accessible data are in a form of an intelligent human readable text, the key data transforms the readable text into a series of unintelligible symbols. Advantageously, the data are reversibly encoded by the data key so that a user can retrieve them upon the provision of the data key for decoding the encoded data. Otherwise, without providing the key data, only the encoded data, as for the example the series of unintelligible symbols are retrieved from the computer system. Further advantageously, the key data is provided to the system for reversibly transforming the data in one way or the other, but it is not stored in the computer system in unencoded form along with the encrypted data.

[0034] Of course, instead of providing a password to the computer system for initiating the encoding/decoding of key data for a security purpose, another value is usable. Such other value originates from a smart card belonging to a user that contains information, which triggers the encoding/decoding for example. Of course, other possessions such as digital keys, PCMCIA cards, chips and so forth are useful for providing longer more complex access codes.

[0035] In a subsequent step, the encoded key data is stored secured by biometric information of the user. For example, a fingerprint template is stored in association with the encoded data for retrieving the encoded data. Thus, both biometric information and a password or electronic code are necessary to access the key data. That said, data mining may provide access to encoded key data absent a step of biometric authentication.

[0036] Referring now to Fig. 2b, a method of accessing the secured data stored on a computer system is shown. In order to retrieve secured data stored within the computer system, the key data must be retrieved in decoded form. Retrieval of the encoded key data necessitates provision and registration of biometric information of the user in order to provide an authorization to proceed. As shown in Fig. 3, the authorization to proceed comprises identifying a user based on biometric information provided therefrom. This provides an indication that the correct person was actually present when the key data was retrieved. Typically, the user provides biometric information at step 30 from a biometric source at step 31. The biometric information is characterized at step 32, processed and compared against templates stored in the system at step 33. Upon a match of the features extracted from the templates and the characterized biometric information corresponding to the biometric source provided by the user, an authorization to proceed is either provided at step 34 or denied at step 35. Advantageously, the system discriminates between various types of biometric sources provided to the system. The biometric source is for example in the form of a fingertip, which is imaged on a contact imager. Furthermore, the biometric source reader is in the form of any imager as for example, but not limited to, a palm print imager, a retinal imager, toe print imager, or a hand writing recognition system. Alternatively, a voice sensor or a keystroke-timing sensor is used.

[0037] Referring back to Fig. 2b, the password data is needed at step 23 for decoding the key data, and an authorization to proceed is also required at step 24 for causing the decoding process to be performed at step 25 for accessing the encoded data at step 26. Thus, even once the user is authorized and authenticated by the biometric identification process, the key data is unavailable in decoded form until the

password is provided. This allows for a more secure use of biometric authentication since the key data is other than stored in decoded form.

[0038] When a system supports a plurality of different login data formats, it is difficult to support the above method. For example, if a password or a smart card are usable to access a system, the key data cannot be decoded with the password or the smart card. Therefore, the key data are stored multiple times; each time encoded using a different one of the possible password data. This provides flexibility in identification and enhanced security over prior art methods. For example, when a system supports multiple methods of logging in such as (fingerprint and password), (fingerprint and smart card), (retina and smart card), (voice and password and digital key), and (password and smart card and typing interval data), the biometric data is substantially unchanging and its use in encoding of the key data is typically ineffective. Thus, the key data is encoded in each possible fashion to support each identification method. Here, as can be seen, encoding of the key data with the smart card code and separately with the password supports all access methods – the digital key being used with the password in one of the methods. Thus, each method remains supported and the key data is not stored in unencoded form.

[0039] Advantageously, as the system expands and access methods increase in numbers, such a method is sufficiently flexible to support changes and variations in system access requirements that arise over time.

[0040] Numerous other embodiments might be envisioned without departing from the scope and the spirit of the present invention.

Claims

What is claimed is:

1. A method of securing security data stored on a computer system comprising the steps of:

providing a data key to the computer system (20);

transforming the security data with the data key in a reversible fashion to produce encoded secure data such that the data key is required in order to perform a reverse transform and extract the security data from the encoded secure data (21); and,

storing the encoded secure data (22) in a fashion such that a user authorization process is used to retrieve the encoded secure data such that the data key and the user authorization process in combination (23; 24), provide access to the security data and such that the stored data within the computer system is encoded.

2. A method of securing security data stored on a computer system according to claim 1, wherein a same security data is encoded with several different data keys to provide several different encoded secure data such that a combination of user authorization and any of a plurality of data keys allows for retrieval and decoding.

3. A method of securing security data stored on a computer system according to claim 1, wherein a same security data is encoded with several different data keys to provide several different encoded secure data and wherein each encoded secure data is associated with one or more user authorization processes such that a combination of one or more user authorization processes and any of a plurality of data keys allows for retrieval and decoding.

4. A method of securing security data stored on a computer system according to claim 1, wherein the user authorization process is a biometric information verification process.

5. A method of securing security data stored on a computer system according to claim 1, wherein the data keys include a password.

6. A method of securing security data stored on a computer system comprising the steps of:

providing (30) a biometric information source and comparing (33) the biometric information source against stored templates associated with the biometric information source; and for, in dependence upon a comparison result pairing biometric information source with a first individual identity;

providing (23) a data key associated with a second individual identity; the data key being other than stored on the computer system;

retrieving encoded security data associated with the biometric information, and using the key data for decoding the encoded security data (26).

7. A method of securing security data stored on a computer system according to claim 6, wherein the decoded security data is for performing at least one of encrypting and decrypting data on the computer system.

8. A method of securing security data stored on a computer system according to claim 6, wherein the decoded security data is for allowing access of the data to the identified individual.

9. A method of securing security data stored on a computer system according to claim 6, wherein the step of accepting biometric information source comprises imaging the biometric information source using a contact imager.

10. A method of securing security data stored on a computer system according to claim 9, wherein the contact imager is a fingerprint imager.

11. A method of securing security data stored on a computer system according to claim 6, wherein the step of providing the data key comprises the step of providing a password.

12. A method of securing security data stored on a computer system according to claim 6, wherein the step of providing the data key comprises the step of providing

information stored on a smart card.

13. A method of securing data comprising the steps of:

providing a first information sample to a computer system;

encoding key data in dependence upon the first information sample to produce first security data, the key data for use in decoding stored encoded data;

providing at least one biometric information sample; and

securing the first security data in dependence upon at least one of the at least one biometric information sample.

14. A method of securing data as defined in claim 13, wherein the step of providing a first information sample to a computer system comprises the step of:

hashing the first information sample to produce a first hash value.

15. A method of securing data as defined in claim 13, comprising the steps of:

providing a second other information sample to the computer system;

hashing the second information sample to produce a second hash value;

encoding the key data in dependence upon the second hash value to produce second security data; and

securing the second security data in dependence upon at least one of the at least one biometric information sample.

16. A method of securing data according to claim 13, wherein the step of providing information to a computer system comprises the step of providing a password.

17. A method of securing data according to claim 13, wherein the step of providing information to a computer system comprises the step of providing information stored on a smart card.

18. A method of securing data according to claim 13, wherein the key data is used for encrypting data.

19. A method of securing data comprising the steps of:

providing a first information sample to a computer system;

providing at least one biometric information sample;

encoding the at least one biometric information sample using the first information sample;

encoding key data in dependence upon encoded biometric sample to produce first security data, the key data for use in decoding stored encoded data; and

securing the first security data in dependence upon at least one of the at least one biometric information sample.

20. A method of securing data according to claim 19, comprises the steps of:

providing a first information sample to a computer system for decoding the encoded biometric sample; and

comparing the decoded biometric sample against stored templates associated with the biometric information source.

21. A method of securing data as defined in claim 19 wherein the step of providing a first information sample to a computer system comprises the step of:

hashing the first information sample to produce a first hash value.

22. A method of securing security data stored on a computer system comprising the steps of:

providing a first information sample that is other than stored on said computer system (20),

providing at least one first biometric sample,

using said first information sample to produce encoded security data (21),

using said al least one biometric data to securely store (22) said encoded security data.

23. A method according to claim 22 further comprising the steps of:

providing key data to said computer system ,

providing a first data value that is other than stored on said computer system,

reversibly encoding said key data using said first data value to produce said first information sample.

24. A method according to claim 23 further comprising before the step of encoding said key data, the step of encoding irreversibly said first data value to produce a first encoded data value that is used to encode said key data.

25. A method according to claim 24 further comprising the step of

providing at least a second biometric sample to retrieve said encoded security data (24),

providing a second data value (23),

irreversibly encoding said second data value to produce a second encoded data value,

using said second encoded data value to decode said encoded key value and produce a decoded key value,

using said decoded key value to decode said encoded security data (26).

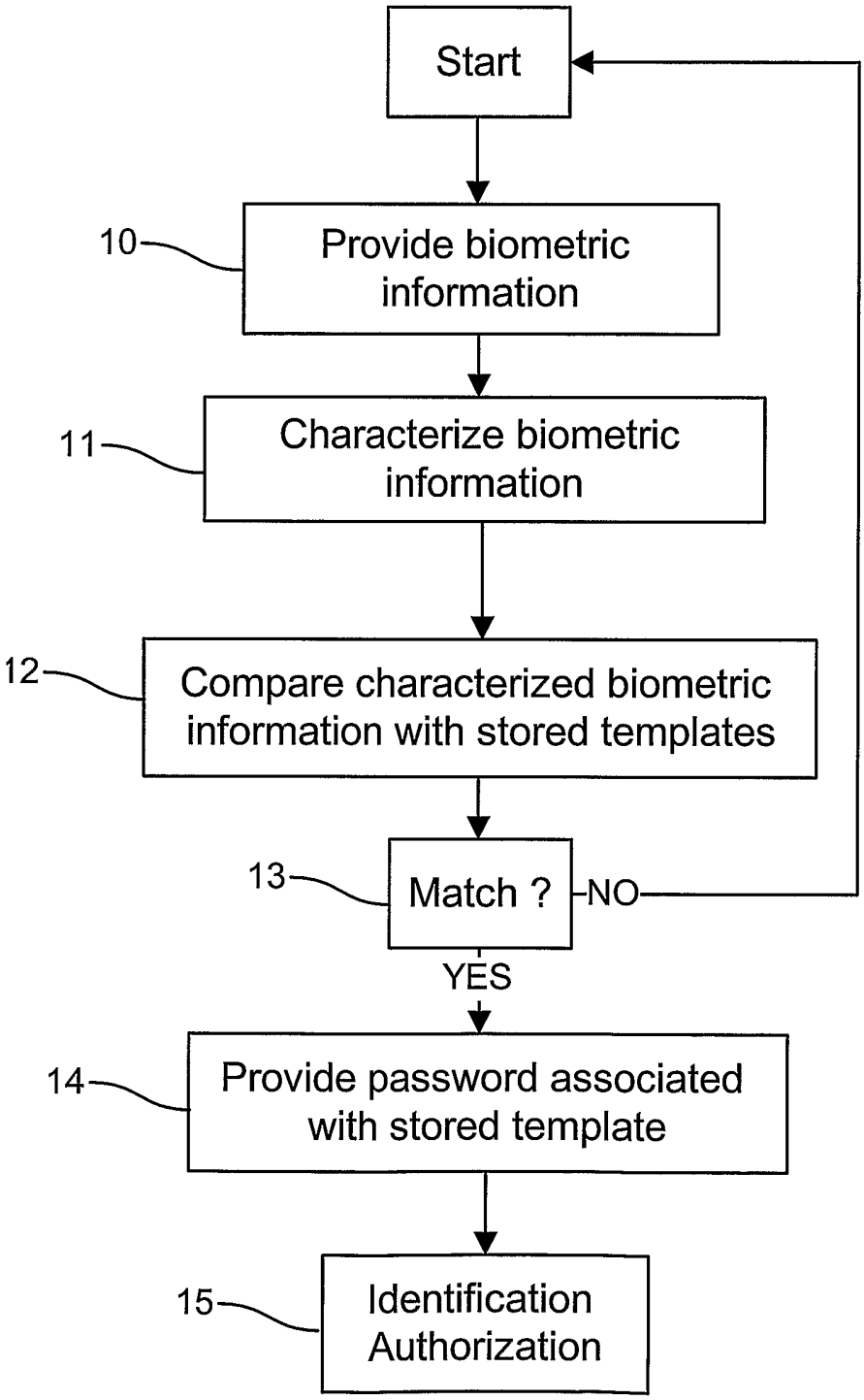


FIG. 1
(Prior Art)

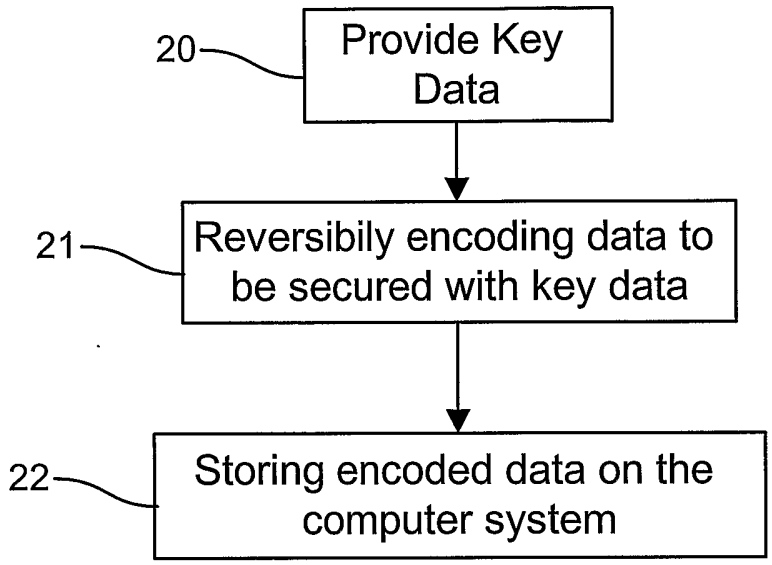

20
Provide Key Data
21
Reversibily encoding data to be secured with key data
22
Storing encoded data on the computer system

FIG. 2a

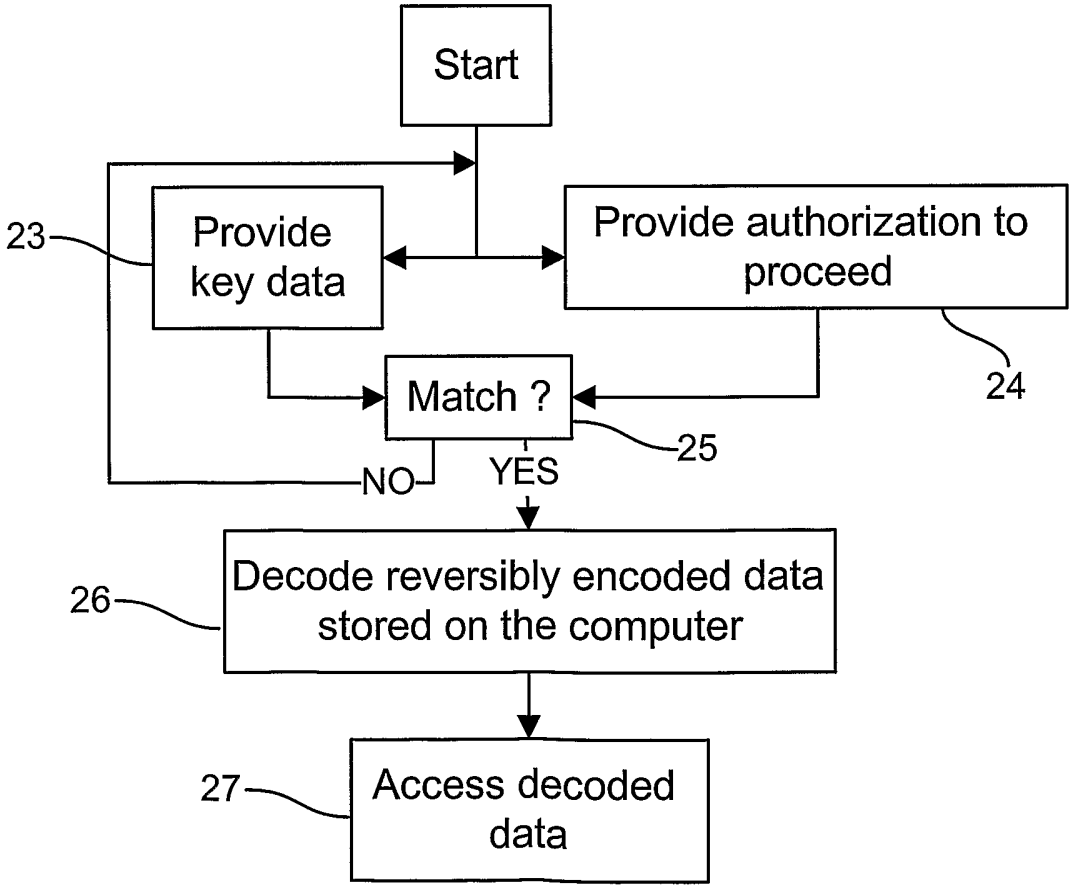

Start
23
Provide key data
Provide authorization to proceed
24
Match ?
25
NO
YES
26
Decode reversibly encoded data stored on the computer
27
Access decoded data

FIG. 2b

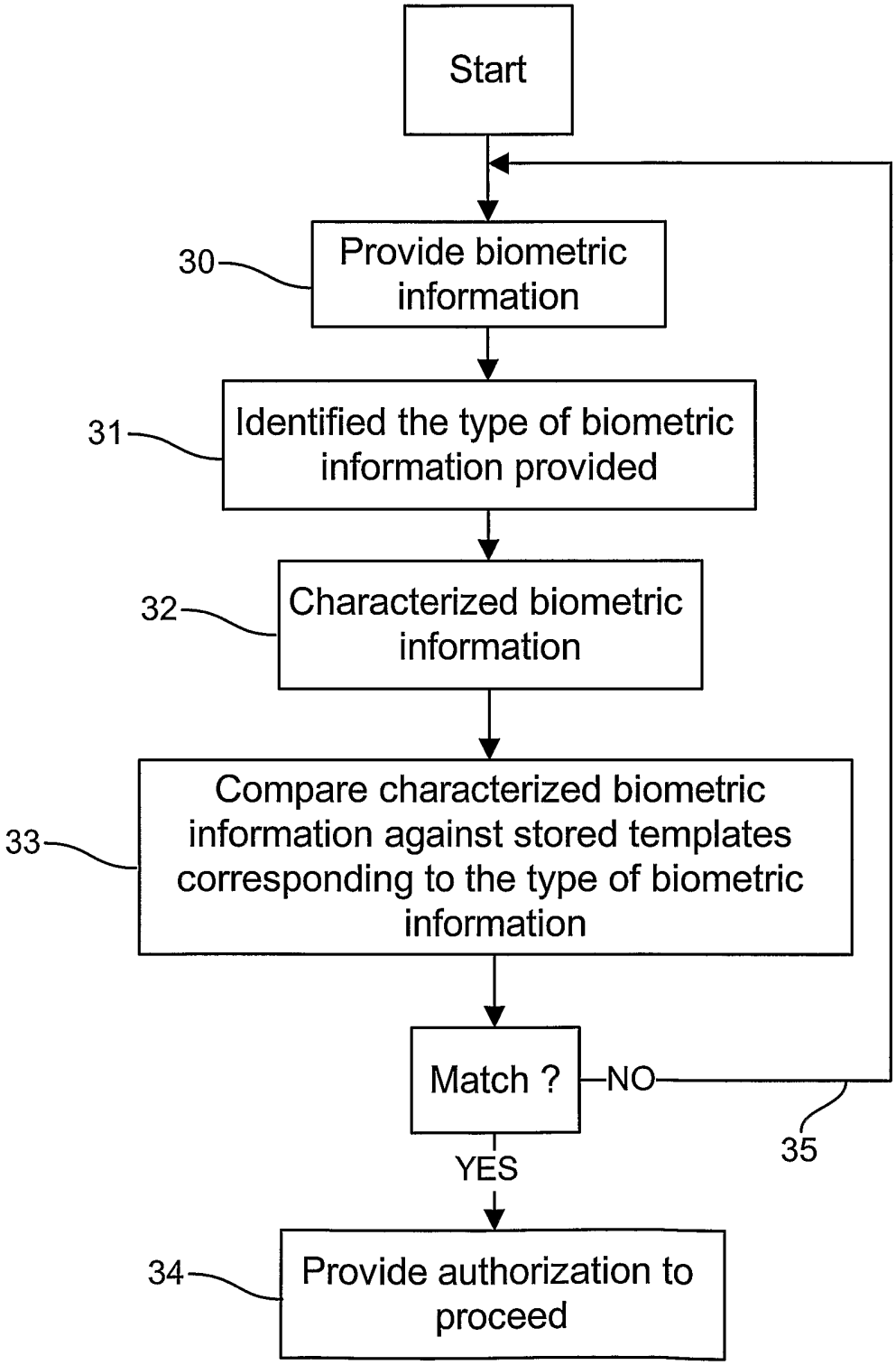

Start
30
Provide biometric information
31
Identified the type of biometric information provided
32
Characterized biometric information
33
Compare characterized biometric information against stored templates corresponding to the type of biometric information
Match ?
NO
35
YES
34
Provide authorization to proceed

FIG. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/01120

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

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)
IPC 7 G06F H04L G06K

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, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 052 468 A (HILLHOUSE ROBERT D) 18 April 2000 (2000-04-18) column 6, line 20 - line 41 column 7, line 65 -column 8, line 15 column 8, line 44 - line 64	1-25
A	US 6 170 058 B1 (KAUSIK BALAS NATARAJAN) 2 January 2001 (2001-01-02) figure 2	5,11, 14-16, 21,24,25
A	US 6 230 272 B1 (LOCKHART ROLAND T ET AL) 8 May 2001 (2001-05-08) abstract	1-25
A	EP 1 176 489 A (DEW ENGINEERING AND DEV LTD) 30 January 2002 (2002-01-30) abstract; figures 1-4	1-25

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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
25 April 2003	13. 05. 2003

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	JENNY FORSS/JA A

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 03/01120

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6052468 A	18-04-2000	NONE	
US 6170058 B1	02-01-2001	AU 746966 B2	09-05-2002
		AU 2097399 A	12-07-1999
		CA 2314349 A1	01-07-1999
		EP 1048143 A1	02-11-2000
		JP 2001527325 T	25-12-2001
		NO 20003310 A	22-08-2000
		WO 9933222 A1	01-07-1999
		WO 0030285 A1	25-05-2000
		US 6263446 B1	17-07-2001
		US 2001008012 A1	12-07-2001
		US 2001034837 A1	25-10-2001
US 6230272 B1	08-05-2001	NONE	
EP 1176489 A	30-01-2002	CA 2317259 A1	25-01-2002
		EP 1176489 A2	30-01-2002