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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2003 (24.04.2003)

PCT

(10) International Publication Number
WO 03/034189 A2

(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number: PCT/EP02/11445

(22) International Filing Date: 11 October 2002 (11.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/977,202 16 October 2001 (16.10.2001) US

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

(72) Inventor: CHARBONNEAU, Marc; 23, Terrace Sauve, Casselman, OTTAWA, Ontario KOA 1MO (CA).

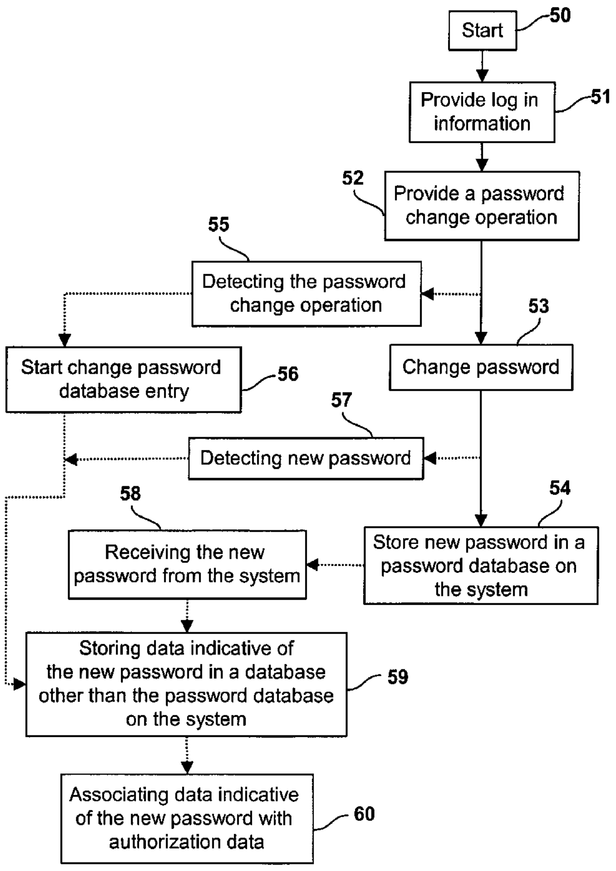
(74) Agent: CABINET JP COLAS; 37, avenue Franklin D. Roosevelt, F-75008 PARIS (FR).

(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, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, 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, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD FOR SUPPORTING SINGLE SIGN ON


Start
50
Provide log in information
51
52
Provide a password change operation
55
Detecting the password change operation
53
Change password
Start change password database entry
56
57
Detecting new password
58
54
Receiving the new password from the system
Store new password in a password database on the system
Storing data indicative of the new password in a database other than the password database on the system
59
Associating data indicative of the new password with authorization data
60

(57) Abstract: A method of securely supporting password change is disclosed. The method comprises the steps of: detecting an occurrence of a password change operation (55) in execution on a system and receiving a new password by the system; detecting the new password when provided (57); storing data indicative (59) of the new password in a database other than the password database of the system for later retrieval, the data indicative of the new password for provision to the system.

Published:

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

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

Method for Supporting Single Sign On

[001] The present invention relates to a method for changing password data, and more particularly, to a method for securely supporting password change for a central database of passwords independent of some processes with which the password is associated.

Background of the invention

[002] Security is fast becoming an important issue. It is well known that 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 is growing. Using passwords is a common method of providing security. Password protection and/or combination type locks are employed for computer network security, automatic teller machines, telephone banking, calling cards, telephone answering services, houses, and safes. These systems generally require the knowledge of an entry code that has been selected by a user or has been preset.

[003] In many large companies, the computer system is organized as a network to reduce the cost of purchasing and installing software on all the stations existing in the company. A main advantage of using a network is to facilitate data accessibility to each employee. However, it is necessary to limit access of a company's network to the company's employees. As such, prior to access the company's network, a password window prompted the company's employees to enter a login identity and an associated password. Usually, a user specifies passwords. Most users, being unsophisticated users of security systems, classically choose as the login identity their first name, and their dog's name as a password for example. Each time a user is prompted to enter his password, the password is always identical to the one previously entered by the user unless the user has modified his password during a previous session. As such, many password systems are easily accessed through a simple trial and error process.

[004] Optionally, to make the system more difficult to break, the network system is organized in such a way that regularly all the employees are prompted to change their

password, or are required to run a specific routine to change their password. Often, the system allows the users to combine a non-determined number of letters, either small or capital, and digits in their passwords. During the time period lasting between two successive modifications of a password, the password remains unchanged. A competent person may rapidly find out the password of a user and access a company's network.

[005] Optionally, a password is stored in a password database and user authorisation information such as biometric information, a digital key, a smart card, or a global password is required to retrieve the password. When the password is retrieved, it is provided to the password window. It is known to those skilled in the art that 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. Fingerprint sensing and matching is a reliable technique for personal identification and/or verification.

[006] The combination of a password and biometric information such as a fingerprint for example is beneficial because it increases the security and limits accessibility to a system. However, an association between a biometric information sample and a password also raises a problem when the password is changed. If an individual changes his password manually using, for example, a change password command of a password protected system, a next time he wants to access the system and provides his fingerprint, his old password is retrieved and provided to the password prompt. The old password is not current and therefore a message indicating that the password is incorrect is provided for the user. Thus, the user has to manually type in the new password. Eventually, the user can run a password change routine wherein the old password is provided along with the fingerprint, the new password typed in and the biometric sample assigned from then to the new password.

Object of the Invention

[007] To overcome such an inconvenience, it is an object of this invention to provide a method for automatically assigning a new password.

[008] It is another object of the present invention to provide a method of detecting a password change operation in a system and prompt for a new password.

[009] It is another object of the present invention to provide a method of detecting a password change command and authorizing a password change operation.

Summary of the invention

[0010] In accordance with the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting at least one of the operations in execution on a system comprising: detecting a password change operation, and detecting a new password storage operation; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored .

[0011] In accordance with another embodiment of the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting a password change operation in execution on a system; displaying to a user a prompt for a new password, the prompt independent of the password change operation; receiving the new password; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored..

[0012] In accordance with another embodiment of the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting a password change operation in execution on a system; displaying to a user a prompt for authentication information, the prompt independent of the password change operation; receiving the authentication information; when the authentication information is indicative of a known user, providing a password associated with the user to the system; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored .

[0013] In accordance with another preferred embodiment of the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting a password change operation in execution on a system; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored; wherein the system has a known user authorized thereon, and wherein the step of performing an operation to change the password comprises the step of automatically generating a new password.

Brief description of the drawings

[0014] Exemplary embodiments of the invention will now be described in conjunction with the following drawings, in which:

[0015] **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;

[0016] **Fig. 2** is an example of a prior art password window dialog display;

[0017] **Fig. 2a** is an example of a filled password window dialog box on a computer screen display;

[0018] **Fig. 3** is a flow diagram of a prior art method of changing password;

[0019] **Fig. 4** is a flow diagram of a prior art method of retrieving the password for provision to the system;

[0020] **Fig. 5** is a flow diagram of a method of securely supporting password change in accordance with a preferred embodiment of the present invention;

[0021] **Fig. 6** is a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention;

[0022] **Fig. 7** is a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention; and,

[0023] **Fig. 8** is a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention wherein a choice is given to the user.

Detailed description of the invention

[0024] In the prior art, many security systems involving imaging fingerprints to allow access for example to a building, to a specific area within a building, to a computer, are described. 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. Following a starting step 10, after a biometric information sample, in a form of a fingerprint for example, has been provided to a system at step 11, in order to generate a fingerprint, a fingertip is imaged to generate an image thereof, which is called a fingerprint or a fingerprint image. The fingerprint is then characterized at step 12. During the process of identification, the characterized fingerprint is compared to stored templates associated with fingerprints of the person at step 13 – for a one-to-one identification system - or of any person registered for access the system – in a one-to-many identification system. 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 14, the system provides at step 15 a password associated with the stored template to, for example, a legacy password based system and the user is identified and authorized at step 16.

[0025] Referring to Fig. 2, an example of a screen display prompting an employee to enter a login identity in 21 and an associated password in 22 to allow the employee to access the network. An example of the display of Figure 1 filled in is shown in Fig. 2a. Classically, the login identity is the user's name, illustrated here, as "Smith" in 23. For security purpose, each character of the password is replaced with a star on the display so that nobody can read it as shown in 24. Each time a user is prompted to enter his password, the password is always identical to the one previously entered by the user unless the user has changed his password during a previous session.

[0026] Optionally, to make the system more difficult to break, the network system is organized in such a way that, regularly, all the employees are prompted to enter a new password in order to change the passwords at regular intervals. Often, the system allows the users to combine a non-predetermined number of letters, either small or capital, and digits in their passwords. Referring to Fig. 3, a prior art method of changing passwords is shown. After a starting step 30, in order to access a system at step 32, the password change window prompts a user to provide an identity and the old password associated with the provided identity at step 31. Once authorized, the user is able to provide the system with a new password at step 33. Typically, the user is prompted to type in a new password two times as shown at step 34. The new password is stored in a password database of an application or operating system related to the password change operation on the system and now replaces the old password at step 35 before an ending session at 36.

[0027] Referring now to Fig. 4, a flow diagram of a method of retrieving the password for provision to the system is shown. For accessing a system after a starting step 40, a user provides authorization data at step 41, in the form of biometric information sample or information stored on a smart card. The authorization data is verified and is used to retrieve data indicative of the user password at step 42. Upon provision of the authorization data, the password is retrieved from a database other than the password database of the system or application at step 43 and provided to the system or application so that the user can gain access thereto.

[0028] The authorization data permits identifying a user based on, for example, biometric information provided therefrom. This provides an indication that the correct person was actually present when the request for changing a password was provided. A major advantage of using biometric information for retrieving a password is that the password does not have to be memorized. Typically, the user provides biometric information from a biometric source. The biometric information is characterized, processed and compared against templates stored in the system. 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 signal is either provided or denied.

[0029] Referring now to Fig. 5, a method for securely supporting password change in accordance with a preferred embodiment is shown. To facilitate the comprehension of the figure, lines are plain for showing a classic password change routine flow, whereas dashed lines show changes in process flow for securely supporting password change. Each individual also has access from its workstation to a password change command. It is understandable that when a user has any doubt concerning the confidentiality of his password, he can change it independently of a network administrator. The user accesses the system at step 50 and provides a command 51 for a password change operation to be performed on the system at step 52. Usually, the user is prompted to type in a new password twice as disclosed with reference to Fig. 3 at step 53, and then the new password is stored in a password database on the system at step 54. Inconveniently, the password is changed independently of the authorization data or log in information when the system supports user authorization and password retrieval as disclosed with reference to Fig. 4. Therefore, the next time the user tries to access the system, his password information will not match with the new password – it has not been updated, and access will be denied.

[0030] According to the present invention, when a change password operation in execution on the system occurs, it is detected at step 55. That said, any password change command options in the form for example of the word "password" or the abbreviation "pwd" typed in are recognized. Of course, though it is preferred that all possible password change operations are detected, the present invention is advantageous if even a single change password operation is detected. The new password is changed at step 53 and the new password is stored in the password database on the system at step 54. Approximately simultaneously, the new password is detected by another process at step 57 that uses the detected data to change the password in another database at step 59. For example, the data indicative of the new password is automatically associated with the authorization data within a system at step 60 such as that of Fig. 4. Therefore, for future accesses to the system, the user just provides his authorization data in a form of a fingerprint for example, the system retrieves the data indicative of the new password associated with the authorization data and the user is authorized to access the system.

[0031] Alternatively, the storage of the new password in a password database on the system is detected and data indicative of the new password are also detected for storing in a database other than the password database on the system as shown at step 58.

[0032] Interestingly, the user is not aware of the detection procedure and of the automatic assignment of the authorization data to the data indicative of the new password. Therefore, the user types in a new password twice for storing the new password in a password database on the system, data indicative of the new password is saved in a database other than the password database on the system at step 59 and the password is changed on the system, and the user does not have to retype this new password for further access. However, because of the transparency of such a system, the user does not know whether his new password has effectively been changed or not.

[0033] Referring now to Fig. 6, a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention is shown. When a password change operation is provided at step 61, the password change operation is detected at step 61 and a secure password change process prompts the user for a new password at step 63 to allow the change password operation to proceed at step 64. The new password is provided to the process at step 65 to allow changing of the password, which is stored in an independent database at step 66. The data indicative of the new password is automatically associated with the authorization data in replacement of the data indicative of the old password. From the independent database, the new password is provided to a password database on the system at step 67 to change the password there. The prompt for a new password by the secure password change process instead of by the process associated with the system or application notifies the user that the password change operation has been detected and that the new password is accurately stored.

[0034] Advantageously, the above process is implemented with no apparent change to the users of the system. In other words, a user is completely unaffected by the method of Fig. 6, since it is transparent to the user and does not affect any existing change password processes.

[0035] Referring now to Fig. 7, a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention is shown. When a password change operation is provided at step 70, the password change operation is detected at step 71 and a secure user authorization process prompts the user for an authorization data at step 72. Once authorized at step 73, the system allows the change password operation to proceed at step 74. The new password is provided to allow changing of the password, which is stored in an independent database at step 75. The data indicative of the new password is automatically associated with the user identity in replacement of the data indicative of the old password. From the independent database, the new password is provided to a password database on the system at step 76 to change the password there. The prompt for user authorization data by the secure authorization process instead of by the process associated with the system or application notifies the user that the password change operation has been detected and that the new password is accurately stored.

[0036] The above process is highly advantageous. It provides a single password change process and as such a single ergonomic interface for changing passwords. Therefore, design and implementation of the secure change password process replaces all legacy change password processes allowing for better information for the users and a more modern and ergonomic process.

[0037] Further advantageously, the above process allows for changing of passwords of several systems/files/applications simultaneously. Thus, a single change password operation is used where before several or several hundred processes would have been required. This is most applicable when changing a password used to protect a single file such as a Microsoft ® Word® file or the like.

[0038] Of course, it is evident to those of skill in the art that a password entered in accordance with the above described process is optionally long and complex since there is no need to remember the password. Because of the automatic password retrieval, a user never needs to know their password so an arbitrary string of characters such as "efkjhgbshgdxfbkj#$$JHYT$kjsfd*(&REW^kvhgfd)(*^*&^%C^Tvc hbjhf86%(%(ffgf nm.b.nm.,mn.vb2609" is usable as a password allowing for greatly increased security.

[0039] Another advantage to the present method is that it allows tracking of old passwords to provide for access to older system restorations or old files that were saved using earlier passwords.

[0040] Of course, the process also supports different passwords for different systems, files and applications without substantial user inconvenience. This is achieved by storing each password in association with data indicative of the user identity or authorization and the system, file, or application with which the password is to be used. Of course, more complex associations are also possible when desired.

[0041] Referring now to Fig. 8, a flow diagram of a method of securely supporting password change for use with the method of Figure 7 wherein a choice is given to the user is shown. During the password change operation of step 80 and after user authorization at step 82 due to the detection of the password change operation at step 81, the user is given the opportunity to either enter a password or to have the process automatically generate a new password at step 83. Therefore, in the case of a computer-generated password, the user does not have to invent and remember the new password because it is automatically assigned to his authorization data and automatically retrieved for access to the system. Consequently, choosing a computer-generated password means that the new password is never typed in which decreases the possibilities of a Trojan Horse application from detecting same.

[0042] Advantageously, when a password is automatically generated, it is unknown to the user. This makes the password impossible to ascertain except by breaching security of password database. For example, when automatic password generation is used, an encryption key may form each password allowing for security relating to access and for encryption of file data to prevent mining of file data.

[0043] Numerous other embodiments may be envisaged without departing from the spirit and scope of the invention.

Claims

What is claimed is:

1. A method of securely supporting password change comprising the steps of:

detecting at least one of the operations in execution on a system comprising:

(i) detecting a password change operation (55; 62; 71; 81),

(ii) and detecting a new password storage operation (57);

performing an operation to change the password of a user to a new password in the system (53, 64, 74);

storing the new password in a password database on the system (54; 67; 76); and,

storing data indicative (59, 66; 75) of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored.

2. A method of securely supporting password change according to claim 1 wherein the step of detecting a password change operation (55; 62; 71; 81) in execution on a system comprises the step of detecting a new password prompt.

3. A method of securely supporting password change according to claim 1 comprising the steps of:

prompting a user to provide authorization data (72); and,

associating the authorization data with the password.

4. A method of securely supporting password change according to claim 1, wherein the step of detecting the new password comprises the step of detecting the new password at least two separate times.

5. A method of securely supporting password change according to claim1 wherein the operation detected is a password change operation and further comprising the steps of:

displaying to a user a prompt for a new password (63), the prompt independent of the password change operation;

receiving the new password (65);

6. A method of securely supporting password change according to claim 5 wherein the step of detecting the change password operation in execution on a system comprises the step of detecting password change command options.

7. A method of securely supporting password change according to claim 1 wherein the operation detected is a password change operation and further comprising the steps of:

displaying to a user a prompt for authentication information (72), the prompt independent of the password change operation;

receiving the authentication information (73);

when the authentication information is indicative of a known user, performing said operation to change the password (74) of the known user to a new password in the system; and;

8. A method of securely supporting password change according to claim 7 wherein the prompt for authentication information is a prompt for biometric information.

9. A method of securely supporting password change according to claim 8 comprising the step of:

providing biometric information;

processing the provided biometric information to provide biometric data;

comparing the biometric data with a stored template; and

in dependence upon a comparison result retrieving a user password from a database.

10. A method of securely supporting password change according to claim 7 wherein the prompt for authentication information is a prompt for information stored on a smart card.

11. A method of securely supporting password change according to claim 7 wherein the step of performing an operation to change the password comprises the step of providing the new password to the system.

12. A method of securely supporting password change according to claim 7 wherein the step of performing an operation to change the password comprises the step of prompting the user to select between provision of the new password and automatic generation of the new password (83).

13. A method of securely supporting password change according to any of claims 7 and 12, characterized in that the step of performing an operation to change the password comprises the step of automatically generating the new password.

14. A method of securely supporting password change according to claim 13 wherein data secured with the new password is encrypted using an encryption key.

15. A method of securely supporting password change according to claim 7 comprising the step of performing another operation to change another password of the known user to the new password.

16. A method of securely supporting password change according to claim 7 comprising the step of determining all passwords identical to the password being changed and automatically performing at least another operation to change each identical password of the known user to the new password.

17. A method of securely supporting password change according to claim 1

wherein the operation detected is a password change operation;

wherein the system has a known user authorized thereon; and,

wherein the step of performing an operation to change the password comprises the step of automatically generating a new password .

18. A method of securely supporting password change according to any of claims 13 and 17, characterized in that the automatically generated new password is unknown to the user.

19. A method of securely supporting password change according to any of claims 13 and 18, characterized in that the automatically generated new password is an encryption key.

20. A method of securely supporting password change according to any of claims 13 and 19, characterized in that the data secured with the new password is encrypted using an encryption key.

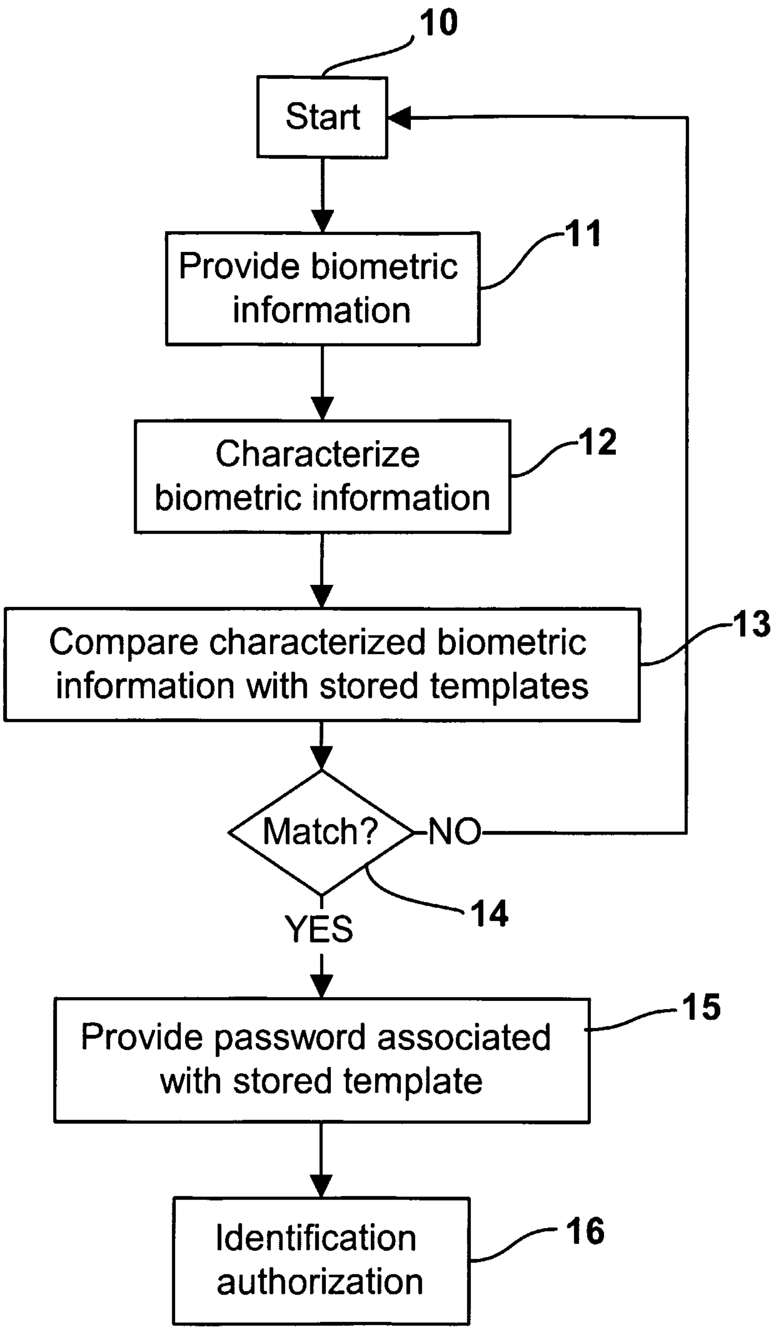

10
Start
11
Provide biometric information
12
Characterize biometric information
13
Compare characterized biometric information with stored templates
Match?
NO
14
YES
15
Provide password associated with stored template
16
Identification authorization

Fig. 1
(PRIOR ART)

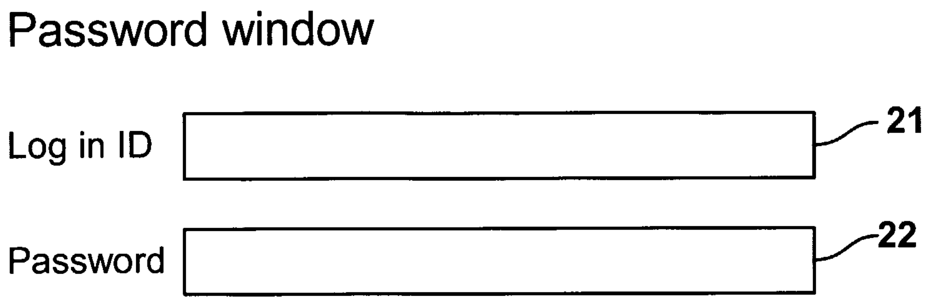
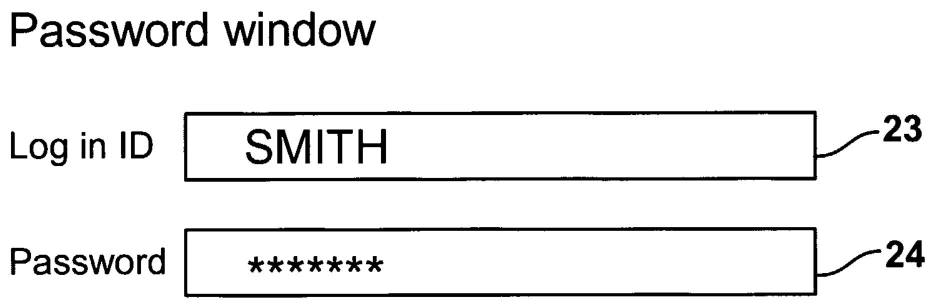


Fig. 2
(PRIOR ART)



Log in ID SMITH

Password *******

Fig. 2a
(PRIOR ART)

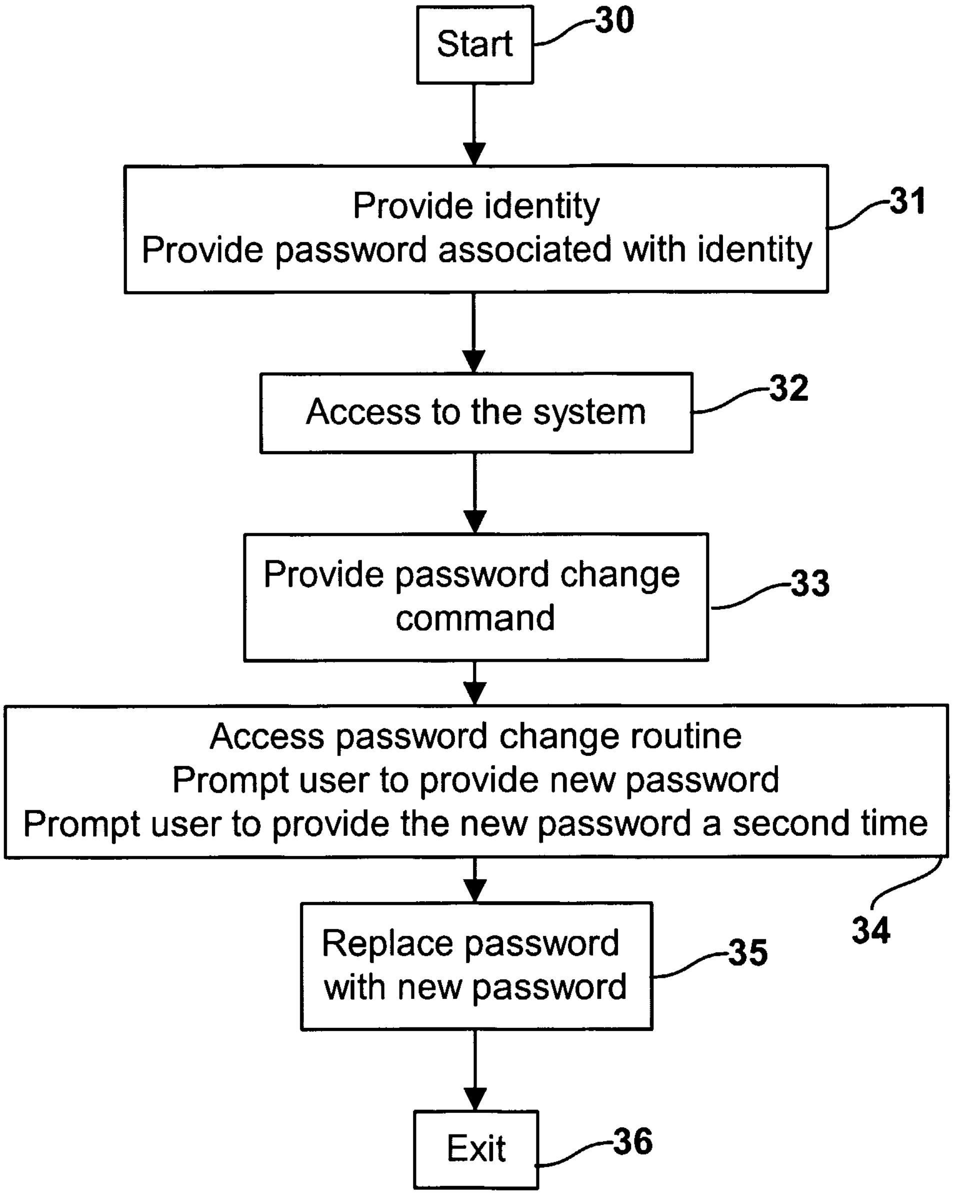

Start
30
Provide identity
Provide password associated with identity
31
Access to the system
32
Provide password change command
33
Access password change routine
Prompt user to provide new password
Prompt user to provide the new password a second time
34
Replace password with new password
35
Exit
36

Fig. 3
(PRIOR ART)

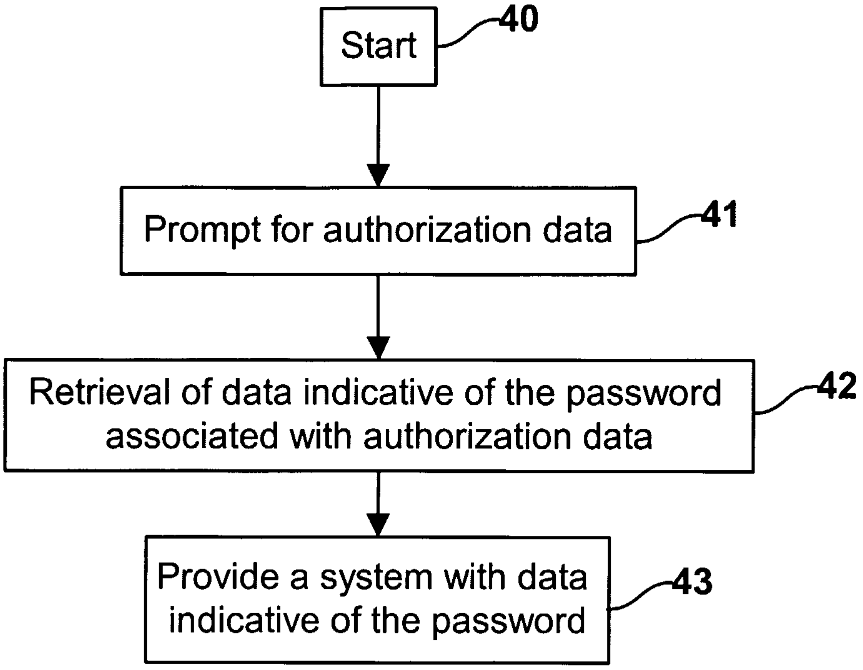

Start
40
Prompt for authorization data
41
Retrieval of data indicative of the password associated with authorization data
42
Provide a system with data indicative of the password
43

Fig. 4
(PRIOR ART)

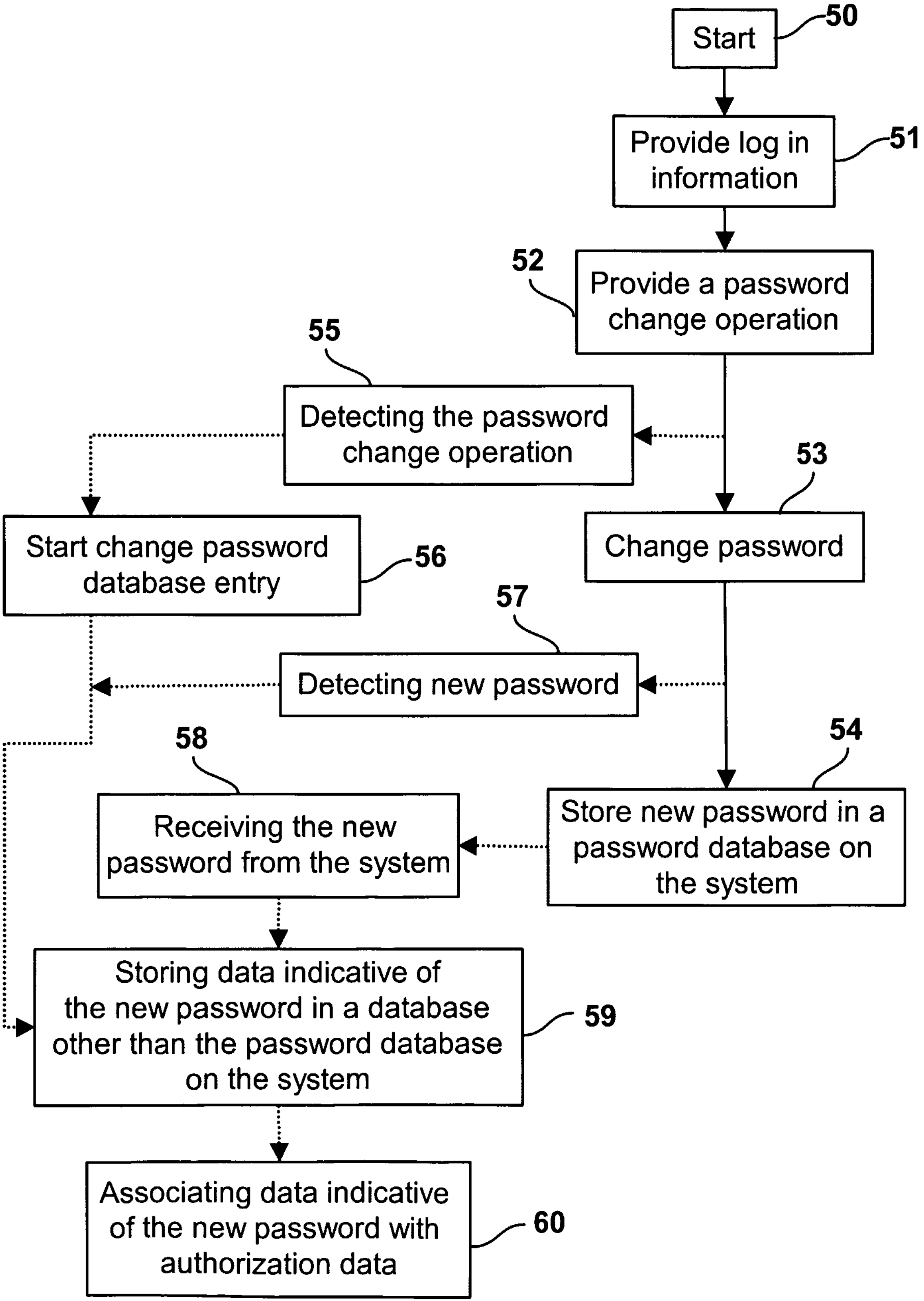

Start
50
Provide log in information
51
52
Provide a password change operation
55
Detecting the password change operation
53
Change password
Start change password database entry
56
57
Detecting new password
58
54
Receiving the new password from the system
Store new password in a password database on the system
Storing data indicative of the new password in a database other than the password database on the system
59
Associating data indicative of the new password with authorization data
60

Fig. 5

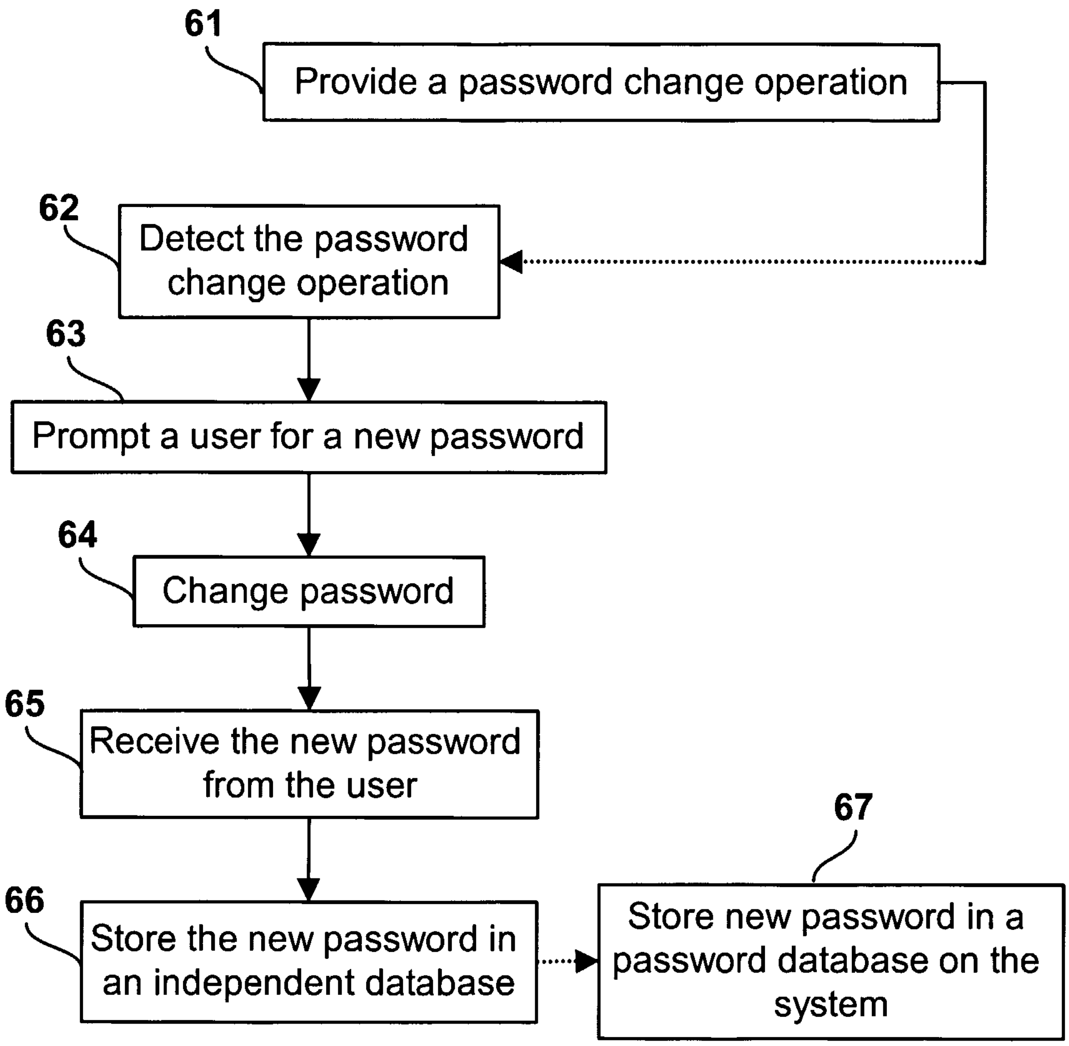

61
Provide a password change operation
62
Detect the password change operation
63
Prompt a user for a new password
64
Change password
65
Receive the new password from the user
66
Store the new password in an independent database
67
Store new password in a password database on the system

Fig. 6

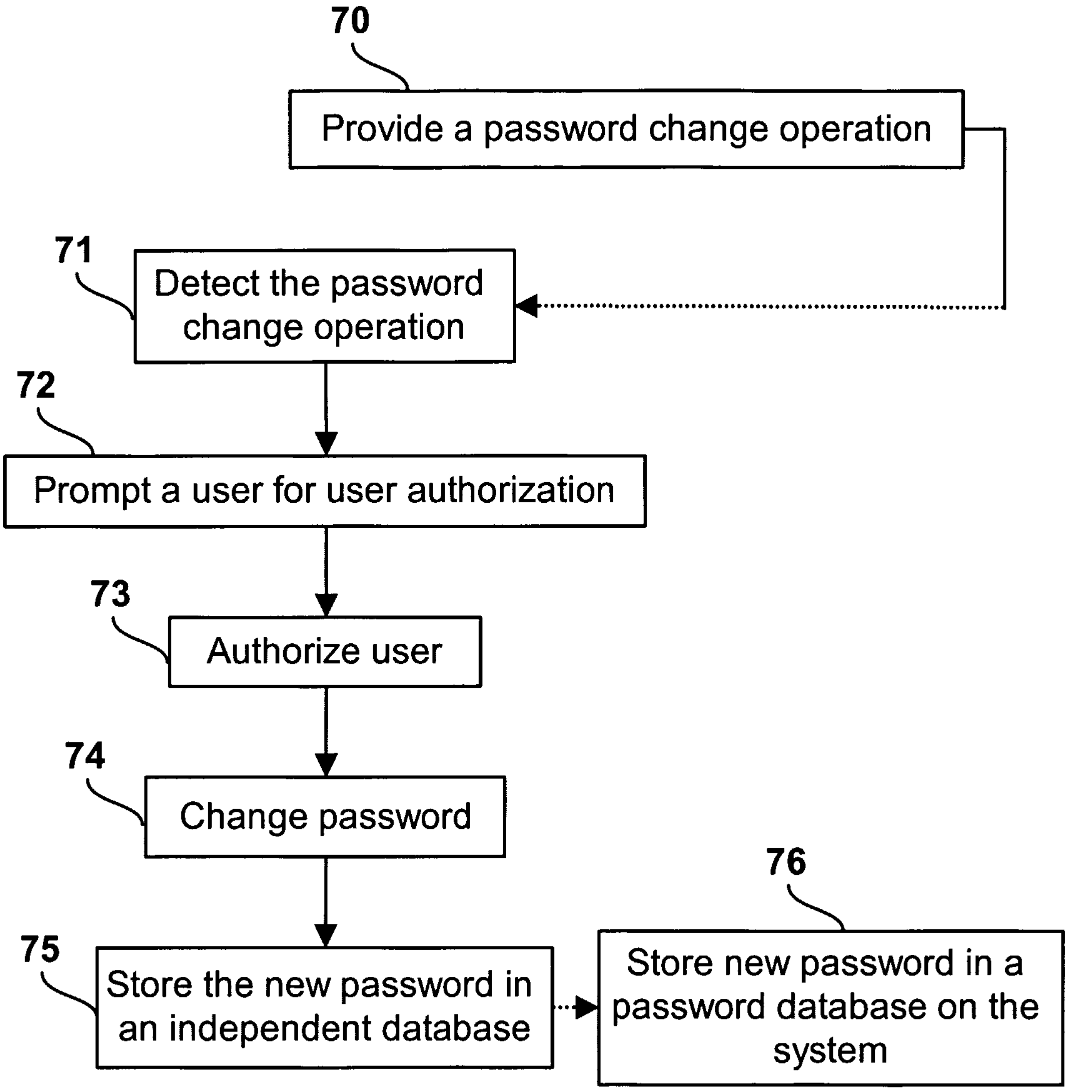

70
Provide a password change operation
71
Detect the password change operation
72
Prompt a user for user authorization
73
Authorize user
74
Change password
75
Store the new password in an independent database
76
Store new password in a password database on the system

Fig. 7

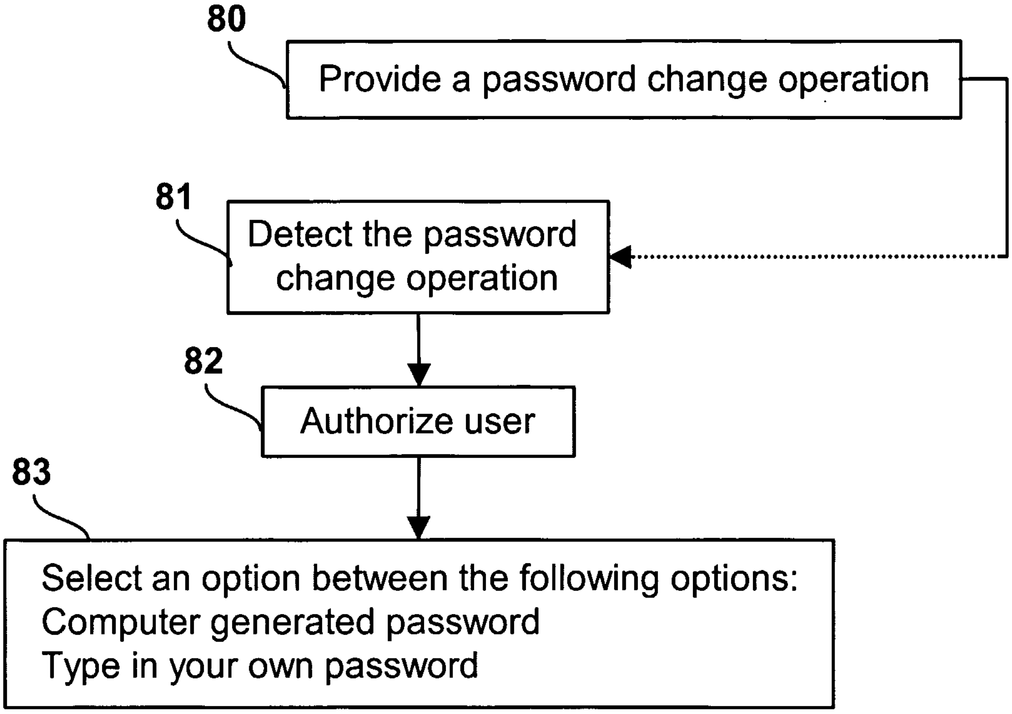

80
Provide a password change operation
81
Detect the password change operation
82
Authorize user
83
Select an option between the following options:
Computer generated password
Type in your own password

Fig. 8