

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
6 February 2003 (06.02.2003)

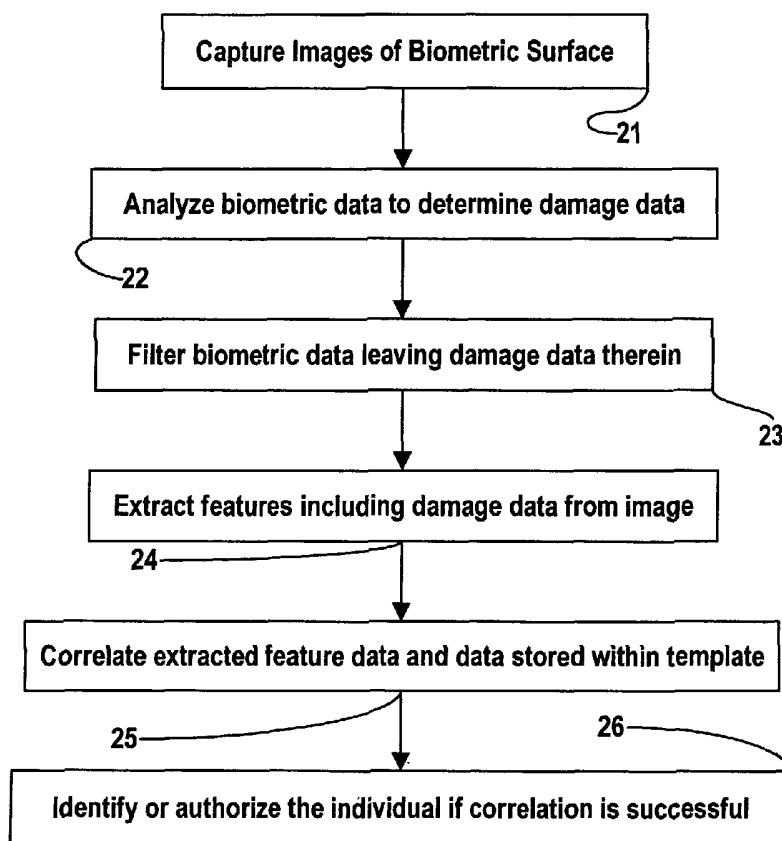
PCT

(10) International Publication Number
WO 03/010706 A1

- (51) International Patent Classification⁷: **G06K 9/00** (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.
- (21) International Application Number: PCT/EP02/08067
- (22) International Filing Date: 18 July 2002 (18.07.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/307,169 24 July 2001 (24.07.2001) 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).
- (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).
- Published:
— with international search report

[Continued on next page]

(54) Title: FINGERPRINT SCAR RECOGNITION METHOD AND APPARATUS



(57) Abstract: A method of recognizing damage to a biometric information source comprises the steps of: sensing biometric information from a biometric information source to provide sensed data (21); extracting features from the sensed data, the features indicative of identifiable content of the sensed data; analyzing the features to determine if some features, when grouped, are characteristic of damage to the biometric information source from which biometric information was sensed (22); and when some of the features are characteristic of damage to the biometric information source, grouping data relating to the some features and to the indicated damage to form damage data (22).

WO 03/010706 A1



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.

Fingerprint Scar Recognition Method and Apparatus

Field of the Invention

[001] The invention relates to biometric identification and more particularly to a method and system for biometric identification of individuals based on identifiable
5 damage to their biometric information source.

Background of the Invention

[002] Security, access control and privacy are important issues in many venues throughout modern society. Government, commercial and private entities continue to seek effective means to control access to either property or information by authorized
10 individuals while excluding access by all others.

[003] Mechanical devices, as simple as a keyed padlock or as robust as the combination lock on a bank vault, have long been used to secure property. Access is allowed to all who possess a matching "key" device or have "knowledge" of the correct combination. Electronic key cards (swipe cards, chip cards and the like) are
15 little more than modern keys and suffer from the same fundamental limitations of all key based security systems: keys can be lost, stolen, and duplicated. Further, keys do not identify the individual possessing and/or using the key.

[004] Modern knowledge based security systems require the correct entry of specific information, into a data entry device, in order to control access. These systems
20 generally require knowledge of an access code that has been selected by a user or has been preset by the system during the user enrollment process. Password protection is commonly employed for computer network security, telephone banking, calling cards, telephone answering services, buildings, and safes. A very effective synergy between key based and knowledge based security systems is typified by the use of swipe cards
25 in combination with passwords in order to provide access to automatic teller machines.

[005] Knowledge based security systems suffer from the same fundamental limitations as combination lock systems: the information that must be provided to the data entry device must be simple; the required knowledge must be concise and easy to remember, and, just as with key systems, knowledge based security systems do not
30 unambiguously identify the individual entering the information.

[006] Complementing the proliferation of computers and computer networks into all aspects of business and daily life is the growing concern over controlled access to information stored in electronic databases.

[007] Short strings of alphanumeric characters, typically less than ten in number, characterize most password protected systems. A word, phrase or number combination familiar to the user is often selected during the user enrollment process. Randomly assigned codes are often forgotten, as users have no reliable method of remembering them. Writing down the codes and storing them in close proximity to an access control device (i.e., the combination lock) results in a secure access control system with a very insecure code. Alternatively, the nuisance of a user making several attempts to enter variations of a complicated code, or lengthy string of characters, renders the access control system more of a problem than a solution.

[008] A security access system that provides substantially secure access control, and is not based on either a key device or user knowledge, is a biometric identification system. A biometric identification system accepts biometric information from a user of the system and attempts to identify and control access by the user by matching the provided information against information belonging to registered users of the system. Biometric information is derived from an anatomic structure of an individual and, as such, is derived from the unique genetic content and the sum of the environmental influences on that individual. One such biometric identification system is a fingerprint recognition system.

Object of the invention

[009] It is an object of the present invention to provide a method of distinguishing scars from other possible factors that might alter an image of a fingerprint. The ability to distinguish scars as a modification of the fingerprint image allows for the scar information to be easily incorporated into the authentication protocol.

Summary of the invention

[0010] In accordance with the present invention, there is provided a method of recognizing damage to a biometric information source comprising the steps of: sensing biometric information from a biometric information source to provide sensed data;

extracting features from the sensed data, the features indicative of identifiable content of the sensed data; analyzing the features to determine if some features, when grouped, are characteristic of damage to the biometric information source from which biometric information was sensed; and, when some of the features are characteristic of damage to the biometric information source, grouping data relating to the some features and to the indicated damage to form damage data.

[0011] According to another aspect of the invention there is provided a storage medium comprising data stored therein and relating to instructions for performing the steps of: sensing biometric information from a biometric information source to provide sensed data; extracting features from the sensed data, the features indicative of identifiable content of the sensed data; analyzing the features to determine if some features, when grouped, are characteristic of damage to the biometric information source from which biometric information was sensed; and, when some of the features are characteristic of damage to the biometric information source, grouping data relating to the some features and to the indicated damage to form damage data.

[0012] According to yet another aspect of the invention there is provided an apparatus comprising: a suitably programmed processor (111) for performing the steps of:

extracting features from the sensed data, the features indicative of identifiable content of the sensed data;

analyzing the features to determine if some features, when grouped, are characteristic of damage to the biometric information source from which biometric information was sensed (22; 32; 42; 48; 52; 58; 63; 802; 812); and,

when some of the features are characteristic of damage to the biometric information source, grouping data relating to the some features and to the indicated damage to form damage data (22; 32; 42; 48; 52; 58; 64; 802; 812).

[0013] According to the invention there is provided a method of recognizing damage to a biometric information source comprising the steps of: providing biometric information to a contact imager to generate an electronic representation thereof; characterizing the electronic representation to identify features associated with an injury within the biometric information; when the features associated with an injury

correspond to stored features associated with an injury, performing one of identifying and authorizing an individual.

Brief description of the drawings

5 [0014] The invention will now be described with reference to the attached drawings in which:

[0015] Fig. 1 is a prior art simplified flow diagram of a method of identifying an individual based on their fingerprint;

[0016] Fig. 2a is a schematic diagram of an imaged fingerprint area;

[0017] Fig. 2b is a representation of the fingerprint area of Fig. 1 having an injury;

10 [0018] Fig. 2c is a representation of the fingerprint area of Fig. 2b wherein the injury is artificially healed;

[0019] Fig. 2d is a representation of the fingerprint area of Fig. 1 having a burn injury;

15 [0020] Fig. 2e is a representation of the fingerprint area of Fig. 2d wherein the injury is artificially healed;

[0021] Referring to Fig. 3, a simplified flow diagram of a method of identifying damage to a biometric information source in analysis thereof in order to preserve the additional information is shown;

20 [0022] Figs. 4a and 4b are simplified flow diagrams of two embodiments of methods of processing fingerprint data to extract damage data relating to cuts;

[0023] Figs. 5a and 5b are simplified flow diagrams of two embodiments of methods of processing fingerprint data to extract damage data relating to cuts and/or burns;

[0024] Fig. 6 is a simplified flow diagram of a method of damage data extraction;

25 [0025] Fig. 7 is a simplified flow diagram of a method of automatically updating template data in response to detected damage data;

[0026] Figs. 8a and 8b are simplified flow diagrams of two embodiments of methods of enrolling individuals to form biometric templates that account for

permanent injury to the biometric information source and the templates including damage data when detected;

[0027] Fig. 9 is a simplified flow diagram of a method of authorizing and/or identifying an individual based on a presence of damage data extracted from their biometric information;

[0028] Fig. 10 is a simplified flow diagram of a method of authorizing and/or identifying an individual based feature data other than feature data in locations corresponding to a presence of damage data extracted from their biometric information; and,

[0029] Fig. 11 is a simplified block diagram of an apparatus according to the invention.

Detailed description of the drawings

[0030] According to the invention temporary or permanent damage to a biometric information source is used as data for authorizing or identifying an individual. Thought the description below refers to fingerprint based biometric authentication systems is also applicable to other biometric identification systems.

[0031] Referring now to Fig. 1, a simplified flow diagram of a prior art method of fingerprint identification is shown. A fingerprint is imaged using a contact sensor at 11. The fingerprint image is then preprocessed at 12. Preprocessing typically begins with adjusting the image for contrast. Preprocessing also includes a step of filtering the image to eliminate noise including image features that are likely caused by the imaging process or conditions and are unlikely to be in the biometric information itself. Of course, in the filtering step image information is typically lost but, since a same filtering process is applied during template generation, the features remaining are sufficient for recognition.

[0032] Once preprocessing of the image is completed, processing of the image is performed at 13. In processing, the image is reoriented to result in a common reference frame. For example, the core of the fingerprint is identified and analysed. The core location and orientation are then used to ensure that the fingerprint image is realigned such that the core location and orientation are a predetermined core location and orientation. Of course, once the core location and orientation are known, a transform is

created to reorient the image. Alternatively, the transform is only applied to extracted feature data obviating a need to realign the image data. Once the image is within a known frame of reference, feature extraction is performed at 14 to determine for each of a plurality of features data for use in registering the fingerprint image against template data. Thus, for example, feature locations, orientations, and feature types are extracted for a predetermined number of features.

[0033] Once the feature data is determined, it is correlated with data within the template at 15 to determine a likelihood of a match. Depending on the determined likelihood, the individual providing the biometric information source to the imager is either identified, authorized, or neither at 16. As is evident to those of skill in the art, image processing is the step during which the most variation in a quality of the biometric identification process is achievable. Thus, the step of processing is adjusted to try to enhance the process by reducing false acceptance and false rejection.

[0034] Alternatively, feature data is extracted within a known reference frame relative to a known feature such that it need not be transformed itself. For example, each feature location is identified by an angle relative to the core direction and an offset from the core location.

[0035] Referring now to Fig. 2a, a representation of a portion of fingerprint image is provided for a healthy fingertip having no damage thereto. As is evident, there is a plurality of features including minutia where bifurcation occurs within a ridge or where a ridge ends abruptly.

[0036] Fingers often show injuries. Typically, these injuries heal and disappear completely. Sometimes, however, when an injury is of a certain type, for example a very deep cut, scarring occurs. Macroscopically, a most probable shape of such a scar resulting from a cut is a line substantially straight across a fingertip in some arbitrary direction. In Fig. 2b, a representation of the fingerprint of Fig. 2a and having a cut therein is shown. In Fig. 2c, a representation of the fingerprint of Fig. 2a and having a scar resulting from the cut of Fig. 2b is shown. At the level of the fingerprint, consistent interruption of the natural lines is observable. This kind of injury shows a regular pattern and, of course, once the skin has scarred the scar is always present on subsequent images of the fingertip.

[0037] The regularity of a typical cut injury on a fingertip and the dimensions of the wound allow a processor characterizing the imaged fingerprint to recognize the wound pattern and identify same as a wound. Whereas prior art fingerprint recognition systems eliminate the features resulting from the cut shown in Fig. 2b, in order to allow recognition, this involves discarding valuable identification related information and reconstruct the missing part of the fingerprint image.

[0038] Referring to Fig. 3a, a simplified flow diagram of a method of identifying damage to a biometric information source in analysis thereof in order to preserve the additional information is shown. A biometric information source is sensed at 21 to provide biometric data. The biometric data is then analysed to extract damage data at 22 relating to damage to the biometric information source. The biometric data is then adjusted and filtered leaving the damage data therein at 23. The biometric information is then analysed to extract features therefrom including the damage data at 24 for use in registration of the biometric data against template data previously stored within memory at 25. In dependence upon the registration result, the individual is one of identified, authorized, and neither identified nor authorized at 26.

[0039] Referring to Fig. 3b, a simplified flow diagram of a method of identifying damage to a biometric information source in analysis thereof in order to preserve the additional information is shown. A biometric information source is sensed at 31 to provide biometric data. The biometric data is then analysed to extract damage data at 32 relating to damage to the biometric information source. The biometric data is then adjusted and filtered to remove noise artifacts and to remove the damage data therein at 33. The biometric information is then analysed to extract features therefrom at 34, which, along with the damage data, are for use in registration of the biometric data against template data previously stored within memory at 35. In dependence upon the registration result, the individual is one of identified, authorized, and neither identified nor authorized at 36.

[0040] By identifying the damage data separately from the remaining feature data, the registration process performed against the template data can account for the damage data both in terms of features absent from the extracted feature data and in terms of updating the template should damage data be determined to be scar data.

[0041] Referring to Figs. 4a and 4b, flow diagrams similar to those of Figs. 3a and 3b are shown but specific to fingerprint registration. Referring to Fig. 4a, a fingertip is imaged to provide biometric data at 41. The biometric data is then analysed to extract damage data relating to damage to the fingertip at 42. The damage data is in the form of lines across the fingerprint image in any direction that are other than ridges. These lines are determined and are extracted in the form of a position, length and direction. Alternatively, they are identified as a plurality of minutia each indicative of a ridge ending and each lying along the line of the fingertip damage. The biometric data is then adjusted and filtered leaving the damage data therein at 43. The biometric information is then analysed to extract features therefrom including the damage data at 44 for use in registration of the biometric data against template data previously stored within memory. Data relating to each feature is determined within a known frame of reference and are provided for use in registration. The data is registered against stored template data at 45 to determine registration results. In dependence upon the registration result, the individual is one of identified, authorized, and neither identified nor authorized at 46.

[0042] Referring to Fig. 4b, a fingertip is imaged to provide biometric data at 47. The biometric data is then analysed to extract damage data relating to damage to the fingertip at 48. The damage data is in the form of lines across the fingerprint image in any direction that are other than ridges. These lines are determined and are extracted in the form of a position, length and direction. Alternatively, they are identified as a plurality of minutia each indicative of a ridge ending and each lying along the line of the fingertip damage. The biometric data is then adjusted and filtered to remove noise artifacts and to remove the damage data therein at 49. The biometric information is then analysed to extract features therefrom at 401. Data relating to each feature is determined within a known frame of reference and are provided for use in registration. The data is registered against stored template data at 402 to determine registration results along with the damage data. In dependence upon the registration result, the individual is one of identified, authorized, and neither identified nor authorized at 403.

[0043] In the methods of Figs. 4a and 4b, the damage data is indicative of a cut or approximately linear scar. Thus, as shown in Figs. 2b and 2c, the damage data relates to a pattern formed within the fingerprint indicating a line therein of ridge endings that

are unlikely to occur naturally. This line, once identified, is likely indicative of damage to the fingertip.

[0044] Of course, fingertips also may suffer burns or other damage. In Fig. 2d, a representation of the fingerprint of Fig. 2a and having a burn thereon is shown. In Fig. 2e, a representation of the fingerprint of Fig. 2a and having a scar resulting from the burn of Fig. 2d is shown.

[0045] Referring to Fig. 5a, a similar method to that of Fig. 4a wherein the damage includes cuts and burns is shown. A fingertip is imaged to provide biometric data at 51. The biometric data is then analysed to extract damage data relating to damage to the fingertip at 52. The damage data is in the form of one of a line across the fingerprint image in any direction that is other than ridges and an area within the fingerprint image absent ridge and trough patterns but surrounded by ridge and trough patterns on all peripheral edges thereof. The line is determined and extracted in the form of a position, length and direction. Alternatively, it is identified as a plurality of minutia each indicative of a ridge ending and each lying along the line of the fingertip damage. The area within the fingerprint image is either identified as a plurality of minutia about the area or as an area definition. In either case, the resulting data is sufficient to uniquely identify the damage from the damage data. The biometric data is then adjusted and filtered leaving the damage data therein at 53. The biometric information is then analysed to extract features therefrom including the damage data at 54 for use in registration of the biometric data against template data previously stored within memory. Data relating to each feature is determined within a known frame of reference and are provided for use in registration. The data is registered against stored template data at 55 to determine registration results. In dependence upon the registration result, the individual is one of identified, authorized, and neither identified nor authorized at 56.

[0046] Referring to Fig. 5b, a fingertip is imaged to provide biometric data at 57. The biometric data is then analysed to extract damage data relating to damage to the fingertip at 58. The damage data is in the form of one of a line across the fingerprint image in any direction that is other than ridges and an area within the fingerprint image absent ridge and trough patterns but surrounded by ridge and trough patterns on all peripheral edges thereof. The line is determined and extracted in the form of a

position, length and direction. Alternatively, it is identified as a plurality of minutia each indicative of a ridge ending and each lying along the line of the fingertip damage. The area within the fingerprint image is either identified as a plurality of minutia about the area or as an area definition. In either case, the resulting data is sufficient to uniquely identify the damage from the damage data. The biometric data is then adjusted and filtered to remove noise artifacts and to remove the damage data therein at 59. The biometric information is then analysed to extract features therefrom at 501. Data relating to each feature is determined within a known frame of reference and are provided for use in registration. The data is registered against stored template data at 502 to determine registration results along with the damage data. In dependence upon the registration result, the individual is one of identified, authorized, and neither identified nor authorized at 503.

[0047] Once scar tissue is permanently present on the fingerprint, prior art filtering operations ignore valuable identification data from the image. Advantageously, a method according to the invention supports dynamic recognition of an injury pattern in order to dynamically update a template.

[0048] Referring to Fig. 6, a simplified flow diagram of a method of identifying and extracting damage data is shown. The method is explained with reference to a fingerprint though it may be applied to other biometric data. A fingerprint is provided to a processor for processing thereof at 61. Contrast within the fingerprint image is adjusted to highlight ridge and trough patterns therein and to make feature extraction more easily performed at 62. The fingerprint is then examined to identify an injury pattern in the form of a pattern of features that is indicative of an injury at 63. For example, two rows of minutia facing each other and each representative of a ridge termination and following two approximately consistently spaced apart lines is indicative of a cut or a scar resulting from a cut. An area having little or no contrast therein and surrounded by a plurality of minutia each indicative of a ridge ending and forming a closed boundary about the area is indicative of tissue damage within the fingerprint. Of course, this latter pattern may also be indicative of dirt, plaster, glue and so forth deposited on the fingertip and therefore preventing accurate imaging of an area thereof.

[0049] When an injury pattern is identified, the processor determines damage data relating thereto at 64. For example, for a cut, a line length, direction, location and type are determined. The line type includes data relating to jaggedness and/or a straightness of the line.

5 [0050] In the event the dimensions and pattern of the wound are such that a substantial portion of the fingerprint image is disrupted, a recognition process may lack the required sophistication or may have insufficient data with which to identify or authenticate the individual. Thus, the invention preferably requires the damage data to be evaluated in conjunction with other biometric data to identify an individual. When
10 other biometric data is insufficient for authentication and identification purposes, authentication of the individual must proceed by different means. Alternatively, authorization or identification proceeds merely based on the damage data.

[0051] Referring to Fig. 7, a method of automatically updating a template in dependence upon damage data is presented. Though specific parameters are presented
15 therein, it is evident to those of skill in the art that experimentation and testing will allow selection of parameters on a case-by-case basis. If a wound lasts for a long period of time, more than ten days for example, the registration process must each time ignore the wound data in identifying the individual. After several years, for example, ignoring the wound data is still performed. This is problematic since the
20 wound data has now become part of the individual's biometric information source. As such, the method shown in Fig. 7 allows for automated updating of a template to accommodate permanent and semi-permanent changes to biometric information sources.

[0052] A fingerprint is captured, preprocessed, and processed in accordance with
25 any of the preceding inventive methods at 71. The damage data is stored within the template or in association therewith at 72. At 73 associated with the damage data is time data indicative of the time when the damaged biometric information source was sensed. On a subsequent access attempt, the registration process confirms a consistency between the damage data and the newly acquired biometric data. For
30 example, if a cut is determined to exist within the five previous sensed fingerprints over the past hour, a sixth fingerprint absent a cut detected therein is highly suspect. Further, after six (6) months, if the cut remains within the fingerprint, the template is

adjusted to add the cut as a scar being a permanent feature within the fingerprint. Thus, damage data stored within a template or associated therewith is either indicative of a temporary damage or permanent damage. Further, some damage data is indicative of potential damage. A potential burn, if it disappears a few hours later was likely just
5 dirt or something stuck to the fingertip sensed. If it remains for a very long time, then is determined to be a scar and the template is automatically updated.

[0053] Referring to Figs. 8a and 8b, a damage sensitive template generation process for use during enrollment is shown in simplified flow diagram. Though the process is described with reference to fingerprints and linear cuts detected therein, it is
10 applicable to other forms of damage as well. Referring to Fig. 8a, biometric information in the form of a fingertip is sensed by imaging same to provide biometric data at 801. The biometric data is then analysed to extract damage data relating to damage to the fingertip at 802. The damage data is in the form of lines across the fingerprint image in any direction that are other than ridges. These lines are
15 determined and are extracted in the form of a position, length and direction. Alternatively, they are identified as a plurality of minutia each indicative of a ridge ending and each lying along the line of the fingertip damage. The biometric data is then adjusted and filtered leaving the damage data therein at 803. The biometric information is then analysed to extract features therefrom including the damage data at
20 804 for use in generating a template thereof.

[0054] In such a case, the features of the fingerprint include the features about the scar and, as such, no data relating to the scar damage is necessary in the registration process so long as the scar features are included within the feature data.

[0055] Referring to Fig. 8b, a fingertip is imaged to provide biometric data at 811.
25 The biometric data is then analysed to extract damage data relating to damage to the fingertip at 812. The damage data is in the form of lines across the fingerprint image in any direction that are other than ridges. These lines are determined and are extracted in the form of a position, length and direction. Alternatively, they are identified as a plurality of minutia each indicative of a ridge ending and each lying along the line of
30 the fingertip damage. The biometric data is then adjusted and filtered to remove noise artifacts and to remove the damage data therein at 813. The biometric information is then analysed to extract features therefrom at 814. Data relating to each feature is

determined within a known frame of reference and are provided along with the extracted damage data for use in generating a template thereof at 815.

[0056] Alternatively, instead of automatically updating template data as described with reference to Fig. 7, users are prompted to re-enroll with the system in order to regenerate a new template when damage data is detected to have become scar data. Using the template generation technique described with reference to Fig. 7, allows for a damage sensitive template generation process during the re-enrollment in order to most accurately characterize the biometric data during the enrollment process.

[0057] Since injuries are typically medium term modifications of biometric information, it is also possible in accordance with the invention to modify the user template in accordance with injuries to indicate that the injury is there. Changes to the injury are then restricted to those that may occur within the timeframe between image capture steps. For example, a cut on a user's fingertip today cannot completely vanish by tomorrow. Therefore, the appearance and disappearance of injuries is a valuable marker in identifying individuals. Of course, once the injury is no longer detected, information relating thereto is removed from the template.

[0058] Referring to Fig. 9, a flow diagram of a method of identifying or authorizing an individual based on damage data present within their biometric information is shown. A biometric information source is sensed at 91 to provide biometric data. The biometric data is then analysed to extract damage data at 92 relating to damage to the biometric information source. The damage data is for use in registration of the biometric data against template data including template damage data previously stored within memory at 95. In dependence upon the registration result, the individual is one of identified, authorized, and neither identified nor authorized at 96.

[0059] Referring to Fig. 10, a flow diagram of a method of identifying or authorizing an individual based on damage data present within their biometric information is shown. A biometric information source is sensed at 101 to provide biometric data. The biometric data is then analysed to extract damage data at 102 relating to damage to the biometric information source. The biometric data is then filtered to extract the damage data therefrom at 103. The template is analysed to determine whether or not damage data was stored therein at 104. If damage data is not

known, then the features extracted from the sensed data are registered against features within the template accounting for the location of the damage data at 105. As such, features in locations corresponding to where the damage data is determined are ignored in feature registration because those features are not likely present within the sensed data. In dependence upon the registration result, the individual is one of identified, authorized, and neither identified nor authorized at 106.

[0060] Referring to Fig. 11, an apparatus is shown. The apparatus includes a sensor for sensing biometric information 110 and a processor 111. The processor is suitably programmed for performing one or more of the above described methods.

10 [0061] The damage data is for use in improving registration of the biometric data against template data at 105. In dependence upon the registration result, the individual is one of identified, authorized, and neither identified nor authorized at 106.

[0062] Alternatively, damage data includes damage data relating to a plurality of different causes of damage such as, for example, lacerations and abrasions with irregular patterns, substantial loss of tissue, blisters, holes, insect bites, bites in general, swelling, frost bite, substantial bruising, etc.

15 [0063] Numerous other embodiments may be envisaged without departing from the spirit or scope of the invention.

Claims

What is claimed is:

1. A method of recognizing damage to a biometric information source comprising the steps of:

5 sensing biometric information from a biometric information source to provide sensed data (21; 31; 41; 47; 51; 57; 61; 801; 811; 101);

extracting features from the sensed data, the features indicative of identifiable content of the sensed data;

analyzing the features to determine if some features, when grouped, are characteristic
10 of damage to the biometric information source from which biometric information was sensed (22; 32; 42; 48; 52; 58; 63; 802; 812; 102); and,

when some of the features are characteristic of damage to the biometric information source, grouping data relating to the some features and to the indicated damage to form damage data (22; 32; 42; 48; 52; 58; 64; 802; 812; 102).

15

2. A method according to claim 1 comprising the steps of:

providing a template;

extracting feature data relating to at least other features than the some features (24; 34; 44; 401; 54; 501);

20 registering the extracted feature data against data within the template to determine a likelihood of a match (25; 35; 45; 402; 55; 502); and,

when a match is likely, performing one of identifying and authorizing the biometric information source (26; 36; 46; 403; 56; 503).

25 3. A method according to claim 2, wherein the step of correlating is performed in dependence upon only feature data other than the damage data.

4. A method according to claim 2, wherein the step of correlating accounts for features missing from the extracted feature data in dependence upon the damage data.

30

5. A method according to claim 2 wherein the step of registering includes a step of registering the damage data against further data within the template to determine a likelihood of a damage match; and,
wherein the step of when a match is likely, performing one of identifying and
5 authorizing the biometric information source is performed when a match and a damage match are both likely.
6. A method according to claim 1 comprising the steps of:
providing a template;
10 registering the damage data against data within the template to determine a likelihood of a match (95); and,
when a match is likely, performing one of identifying and authorizing the biometric information source (96).
- 15 7. A method according to claim 1 comprising the steps of:
providing a template;
determining from the template whether damage data is known for the biometric information source;
when damage data is other than known (104), performing the steps of:
20 extracting feature data relating to at least other features than the some features,
registering the extracted feature data against data within the template to determine a likelihood of a match (105), and
when a match is likely, performing one of identifying and authorizing the biometric information source (106); and
25 when damage data is known, performing the steps of:
extracting feature data relating to at least other features than the some features,
registering the extracted feature data against data within the template to determine a likelihood of a match,
registering the damage data against further data within the template to
30 determine a likelihood of a damage match, and
when a match and a damage match are both likely, performing one of identifying and authorizing the biometric information source.

8. A method according to any of claims 6 and 7 wherein the step of when damage data is other than known includes the step of:

storing in association with the provided template data indicative of the damage data (72).

5

9. A method according to claim 8 wherein the step of when damage data is other than known includes the step of:

storing in association with the provided template data indicative of the time the biometric information source from which the damage data was extracted was sensed (73).

10

10. A method according to claim 1 wherein the biometric data includes image data.

11. A method according to claim 10 wherein the biometric information is a fingertip and wherein the image data relates to a fingerprint.

15

12. A method according to claim 11 wherein the damage data includes data relating to minutia within the fingerprint, the minutia arranged in a pattern indicative of damage.

13. A method according to claim 11 wherein the damage data includes data relating to the type, size and location of the damage.

20

14. A method according to claim 13 wherein the damage is one of a cut and a scar resulting from a cut and wherein the damage data includes data relating to a length of the cut, a location of the cut, and an orientation of the cut.

25

15. A method according to claim 14 wherein the damage is identifiable from data comprises a plurality of features along two approximately equally spaced lines within the image.

30

16. A method according to claim 13 wherein the damage is one of a burn and a scar resulting from a burn and wherein the damage data includes data relating to a shape of the burn and a location of the burn.

17. A method according to claim 16 wherein the damage is identifiable from data comprising a plurality of features forming a boundary about a region having no features or expected and identifiable patterns therein.

- 5 18. A method according to claim 1 comprising the steps of:
providing a template;
determining from the template whether damage data is known for the biometric
information source (71);
when damage data is other than known, performing the step of storing in association
10 with the provided template data indicative of the damage data (72).

19. A method according to claim 18 wherein the step of when damage data is other
than known includes the step of:
storing in association with the provided template data indicative of the time the
15 biometric information source from which the damage data was extracted was sensed
(73).

20. A method according to claim 1 comprising the steps of:
providing a template;
20 determining from the template whether template damage data is known for the
biometric information source;
when template damage data is known, performing the steps of:
determining if the template damage data is relating to permanent damage to the
biometric information source; and
25 if the template damage data relates to permanent damage then verifying that
the damage data and the known damage data are consistent damage data.

21. A method according to claim 20 wherein the template includes data relating to a
period during which the damage data has been detected and wherein the step of
30 determining is performed in dependence upon the data relating to the period.

22. A method according to claim 21 wherein the step of determining is performed in
dependence upon a known present time.

23. A method according to claim 1 comprising the steps of:

providing a template;

determining from the template whether template damage data is known for the biometric information source;

5 when template damage data is known, performing the steps of:

determining if the template damage data is relating to permanent damage to the biometric information source and

if the template damage data relates to other than permanent damage then comparing the damage data to the template damage data to determine a change
10 therebetween.

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

when no change, determining a period during which no change has occurred; and

if the period is greater than a threshold period, storing an indication that the damage
15 data relates to permanent damage to the biometric information source.

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

when no change, determining a period during which no change has occurred; and

if the period is greater than a threshold period, providing an indication to the biometric
20 information source to re-enroll their biometric information.

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

when no change, determining a period during which no change has occurred; and

if the period is less than a threshold period, storing an indication of the period during
25 which no change has occurred.

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

when change, determining an amount of change; and

in dependence upon the amount of change determining a likelihood of consistency for
30 the damage data.

28. A method according to claim 1 comprising the steps of:

storing, within a template, data indicative of the damage data and data indicative of features other than the some features.

29. A method according to claim 28 wherein the step of storing data indicative of the damage data includes the step of storing the damage data.

30. A method according to claim 29 wherein the step of storing data indicative of the damage data includes the step of storing data indicative of the grouped features.

31. A method according to claim 29 wherein the step of storing data indicative of the damage data includes the step of storing data relating to the type of damage.

32. A method according to claim according to any of claims 18, 20, and 28 wherein the sensed data is an image of a biometric surface.

33. A method according to claim 32 wherein the damage is one of a cut and a scar resulting from a cut and wherein the damage data includes data relating to a length of the cut, a location of the cut, and an orientation of the cut.

34. A method according to claim 33 wherein the damage is identifiable from data comprises a plurality of features along two approximately equally spaced lines within the image.

35. A method according to claim 32 wherein the damage is one of a burn and a scar resulting from a burn and wherein the damage data includes data relating to a shape of the burn and a location of the burn.

36. A method according to claim 35 wherein the damage is identifiable from data comprising a plurality of features forming a boundary about a region having no features or expected and identifiable patterns therein.

37. A storage medium comprising data stored therein and relating to instructions for performing the steps of:

sensing biometric information from a biometric information source to provide sensed data (21; 31; 41; 47; 51; 57; 61; 801; 811);

extracting features from the sensed data, the features indicative of identifiable content of the sensed data;

- 5 analyzing the features to determine if some features, when grouped, are characteristic of damage to the biometric information source from which biometric information was sensed (22; 32; 42; 48; 52; 58; 63; 802; 812); and,
- when some of the features are characteristic of damage to the biometric information source, grouping data relating to the some features and to the indicated damage to
- 10 form damage data (22; 32; 42; 48; 52; 58; 64; 802; 812).

38. A storage medium according to claim 37 wherein the stored data relates to instructions for performing the steps of:

providing a template;

- 15 extracting feature data relating to at least other features than the some features (24; 34; 44; 401; 54; 501);
- registering the extracted feature data against data within the template to determine a likelihood of a match (25; 35; 45; 402; 55; 502); and,
- when a match is likely, performing one of identifying and authorizing the biometric
- 20 information source (26; 36; 46; 403; 56; 503).

39. A storage medium according to claim 38, wherein the stored data relating to the step of correlating relates to performing the step in dependence upon only feature data other than the damage data.

25

40. A storage medium according to claim 38, wherein the stored data relating to the step of correlating account for features missing from the extracted feature data in dependence upon the damage data.

- 30 41. A storage medium according to claim 38 wherein the stored data relating to performing the step of registering includes data relating to a step of registering the damage data against further data within the template to determine a likelihood of a damage match; and,

relating to a step of when a match is likely, performing one of identifying and authorizing the biometric information source is performed when a match and a damage match are both likely.

- 5 42. A storage medium according to claim 37 comprising wherein the stored data relates to instructions for performing the steps of:

providing a template;

registering the damage data against data within the template to determine a likelihood of a match (95); and,

- 10 when a match is likely, performing one of identifying and authorizing the biometric information source (96).

43. A storage medium according to claim 37 wherein the stored data relates to instructions for performing the steps of:

- 15 providing a template;

determining from the template whether damage data is known for the biometric information source;

when damage data is other than known, performing the steps of:

- 20 extracting feature data relating to at least other features than the some features, registering the extracted feature data against data within the template to determine a likelihood of a match, and

when a match is likely, performing one of identifying and authorizing the biometric information source; and

when damage data is known, performing the steps of:

- 25 extracting feature data relating to at least other features than the some features, registering the extracted feature data against data within the template to determine a likelihood of a match,

registering the damage data against further data within the template to determine a likelihood of a damage match, and

- 30 when a match and a damage match are both likely, performing one of identifying and authorizing the biometric information source.

44. A storage medium according to any of claims 42 and 43 wherein the stored data relating to instructions for performing the step of when damage data is other than known includes data relating to performing the step of:
storing in association with the provided template data indicative of the damage data
5 (72).

45. A storage medium according to claim 44 wherein the stored data relating to instructions for performing the step of when damage data is other than known includes data relating to performing the step of:
10 storing in association with the provided template data indicative of the time the biometric information source from which the damage data was extracted was sensed
(73).

46. A storage medium according to claim 45 wherein the damage data includes data
15 relating to minutia within the fingerprint, the minutia arranged in a pattern indicative of damage.

47. A storage medium according to claim 45 wherein the damage data includes data relating to the type, size and location of the damage.
20

48. A storage medium according to claim 47 wherein the damage is one of a cut and a scar resulting from a cut and wherein the damage data includes data relating to a length of the cut, a location of the cut, and an orientation of the cut.

25 49. A storage medium according to claim 48 wherein the damage is identifiable from data comprises a plurality of features along two approximately equally spaced lines within the image.

30 50. A storage medium according to claim 47 wherein the damage data relates to one of a burn and a scar resulting from a burn and wherein the damage data includes data relating to a shape of the burn and a location of the burn.

51. A storage medium according to claim 50 wherein the damage data relates to damage identifiable from data comprising a plurality of features forming a boundary about a region having no features or expected and identifiable patterns therein.

- 5 52. A storage medium according to claim 37 wherein the stored data relates to instructions for performing the steps of:
providing a template;
determining from the template whether damage data is known for the biometric information source;
10 when damage data is other than known, performing the step of storing in association with the provided template data indicative of the damage data.

53. A storage medium according to claim 52 wherein the stored data relating to instructions for performing the step of when damage data is other than known includes
15 data relating to the step of:
storing in association with the provided template data indicative of the time the biometric information source from which the damage data was extracted was sensed.

54. A storage medium according to claim 37 wherein the stored data relates to
20 instructions for performing the steps of:
providing a template;
determining from the template whether template damage data is known for the biometric information source;
when template damage data is known, performing the steps of:
25 determining if the template damage data is relating to permanent damage to the biometric information source; and
if the template damage data relates to permanent damage then verifying that the damage data and the known damage data are consistent damage data.

- 30 55. A storage medium according to claim 54 wherein the template includes data relating to a period during which the damage data has been detected and wherein the step of determining is performed in dependence upon the data relating to the period.

56. A storage medium according to claim 55 wherein the stored data relating to instructions for performing the step of determining includes data relating to performing the step in dependence upon a known present time.

- 5 57. A storage medium according to claim 37 wherein the stored data relates to instructions for performing the steps of:
providing a template;
determining from the template whether template damage data is known for the biometric information source;
10 when template damage data is known, performing the steps of:
determining if the template damage data is relating to permanent damage to the biometric information source and
if the template damage data relates to other than permanent damage then
comparing the damage data to the template damage data to determine a change
15 therebetween.

58. A storage medium according to claim 57 wherein the stored data relates to instructions for performing the steps of:
when no change, determining a period during which no change has occurred; and
20 if the period is greater than a threshold period, storing an indication that the damage data relates to permanent damage to the biometric information source.

59. A storage medium according to claim 57 wherein the stored data relates to instructions for performing the steps of:
25 when no change, determining a period during which no change has occurred; and
if the period is greater than a threshold period, providing an indication to the biometric information source to re-enroll their biometric information.

60. A storage medium according to claim 57 wherein the stored data relates to
30 instructions for performing the steps of:
when no change, determining a period during which no change has occurred; and
if the period is less than a threshold period, storing an indication of the period during which no change has occurred.

61. A storage medium according to claim 57 wherein the stored data relates to instructions for performing the steps of:
when change, determining an amount of change; and
in dependence upon the amount of change determining a likelihood of consistency for
5 the damage data.

62. A storage medium according to claim 37 wherein the stored data relates to instructions for performing the steps of:
storing, within a template, data indicative of the damage data and data indicative of
10 features other than the some features.

63. A storage medium according to claim 62 wherein the stored data relating to instructions for performing the step of storing data indicative of the damage data includes data relating to the step of storing the damage data.
15

64. A storage medium according to claim 63 wherein the stored data relating to instructions for performing the step of storing data indicative of the damage data includes data relating to the step of storing data indicative of the grouped features.

20 65. A storage medium according to claim 63 wherein the stored data relating to instructions for performing the step of storing data indicative of the damage data includes data relating to the step of storing data relating to the type of damage.

25 66. A storage medium according to any of claims 52, 54, and 62 wherein the sensed data is an image of a biometric surface.

67. A storage medium according to claim 66 wherein the damage data relates to one of a cut and a scar resulting from a cut and wherein the damage data includes data relating to a length of the cut, a location of the cut, and an orientation of the cut.
30

68. A storage medium according to claim 67 wherein the damage data relates to damage identifiable from data comprises a plurality of features along two approximately equally spaced lines within the image.

69. A storage medium according to claim 66 wherein the damage data relates to one of a burn and a scar resulting from a burn and wherein the damage data includes data relating to a shape of the burn and a location of the burn.
- 5 70. A storage medium according to claim 69 wherein the damage data relates to damage identifiable from data comprising a plurality of features forming a boundary about a region having no features or expected and identifiable patterns therein.
71. An apparatus comprising:
- 10 a suitably programmed processor (111) for performing the steps of:
- extracting features from sensed data, the features indicative of identifiable content of the sensed data;
- analyzing the features to determine if some features, when grouped, are characteristic of damage to the biometric information source from which
- 15 biometric information was sensed (22; 32; 42; 48; 52; 58; 63; 802; 812); and,
- when some of the features are characteristic of damage to the biometric information source, grouping data relating to the some features and to the indicated damage to form damage data (22; 32; 42; 48; 52; 58; 64; 802; 812).
- 20 72. An apparatus according to claim 71 comprising an imaging device (110).
73. An apparatus according to claim 72 wherein the imaging device is a contact imager.
- 25 74. An apparatus according to claim 71 comprising a communication circuit for communicating with another processor, the communication circuit for receiving template data from the other processor.
75. A method of recognizing damage to a biometric information source comprising
- 30 the steps of: providing biometric information to a contact imager to generate an electronic representation thereof; characterizing the electronic representation to

identify features associated with an injury within the biometric information; when the features associated with an injury correspond to stored features associated with an injury, performing one of identifying and authorizing an individual.

- 5 76. A method according to claim 75 wherein the electronic representation is of a fingerprint.

1/11

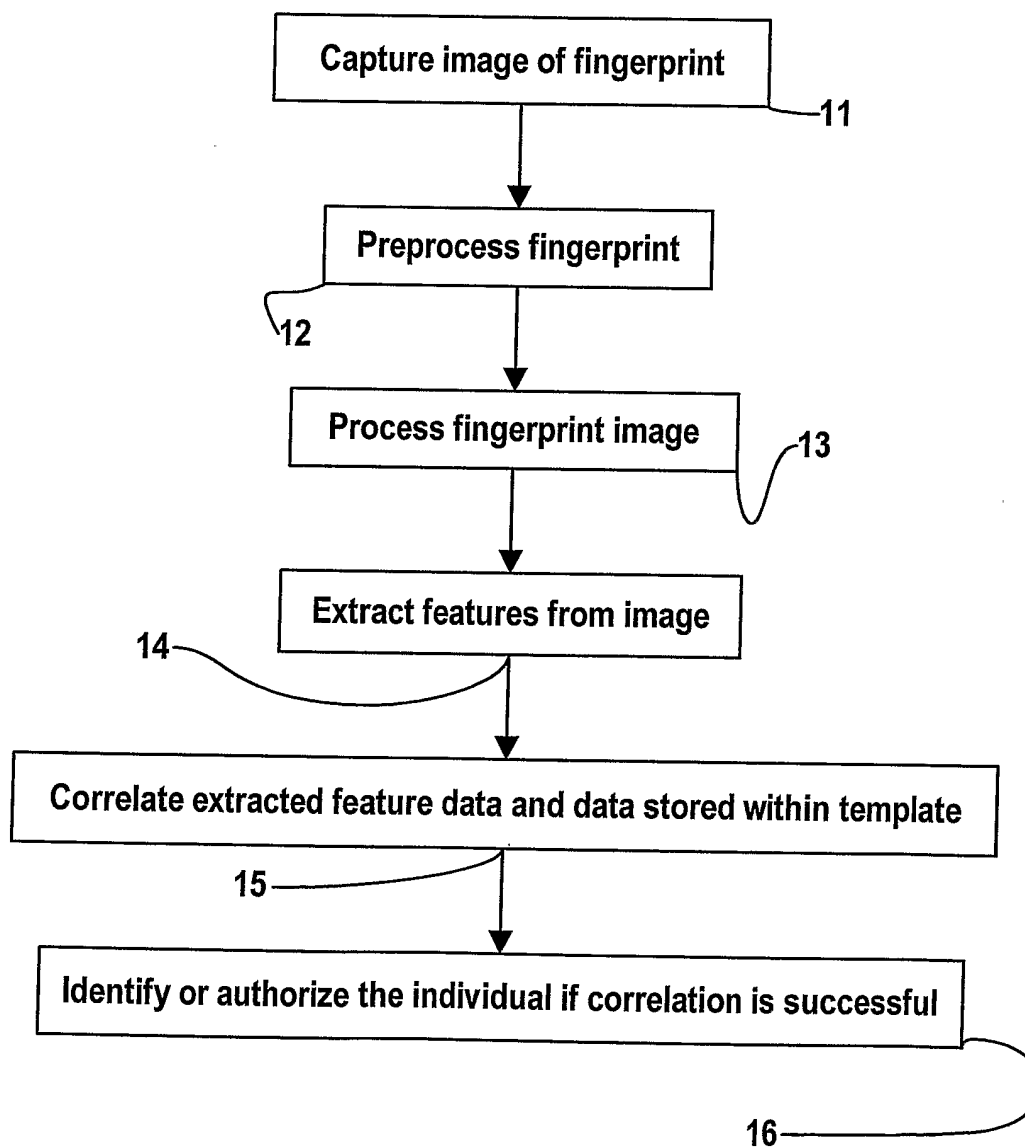


Fig. 1
(Prior Art)

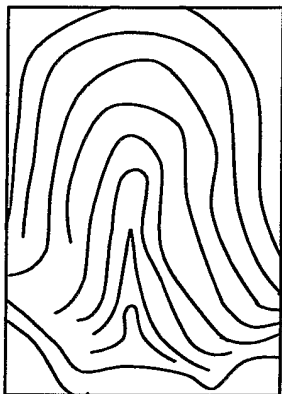


Fig. 2a

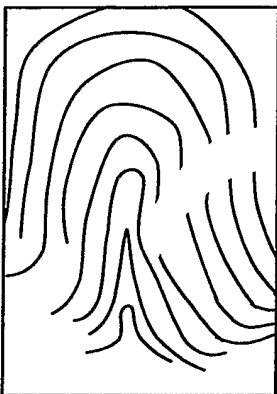


Fig. 2b

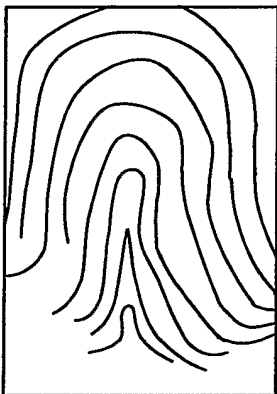


Fig. 2c

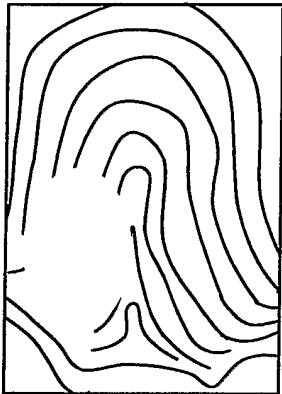


Fig. 2d

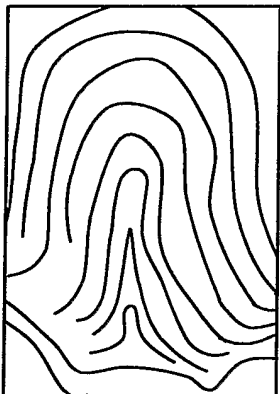


Fig. 2e

3/11

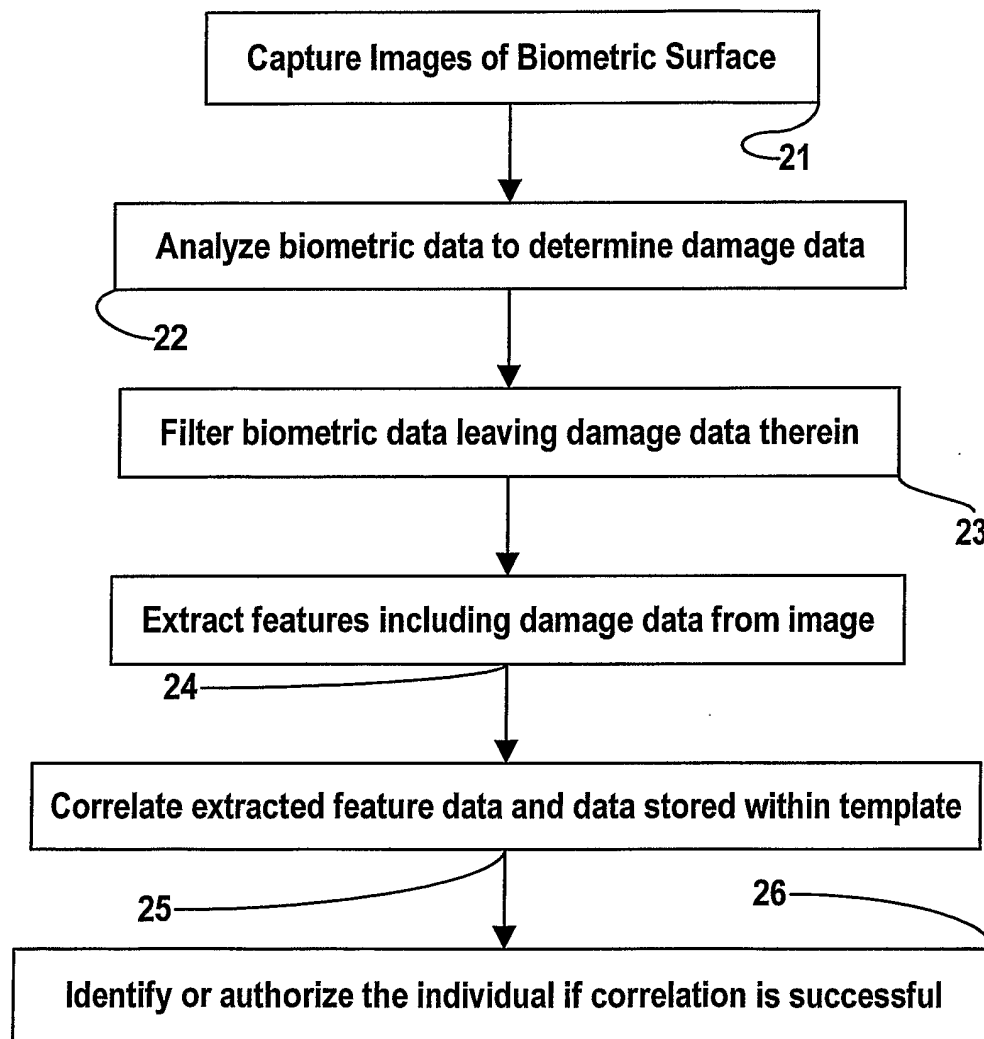


Fig. 3a

4/11

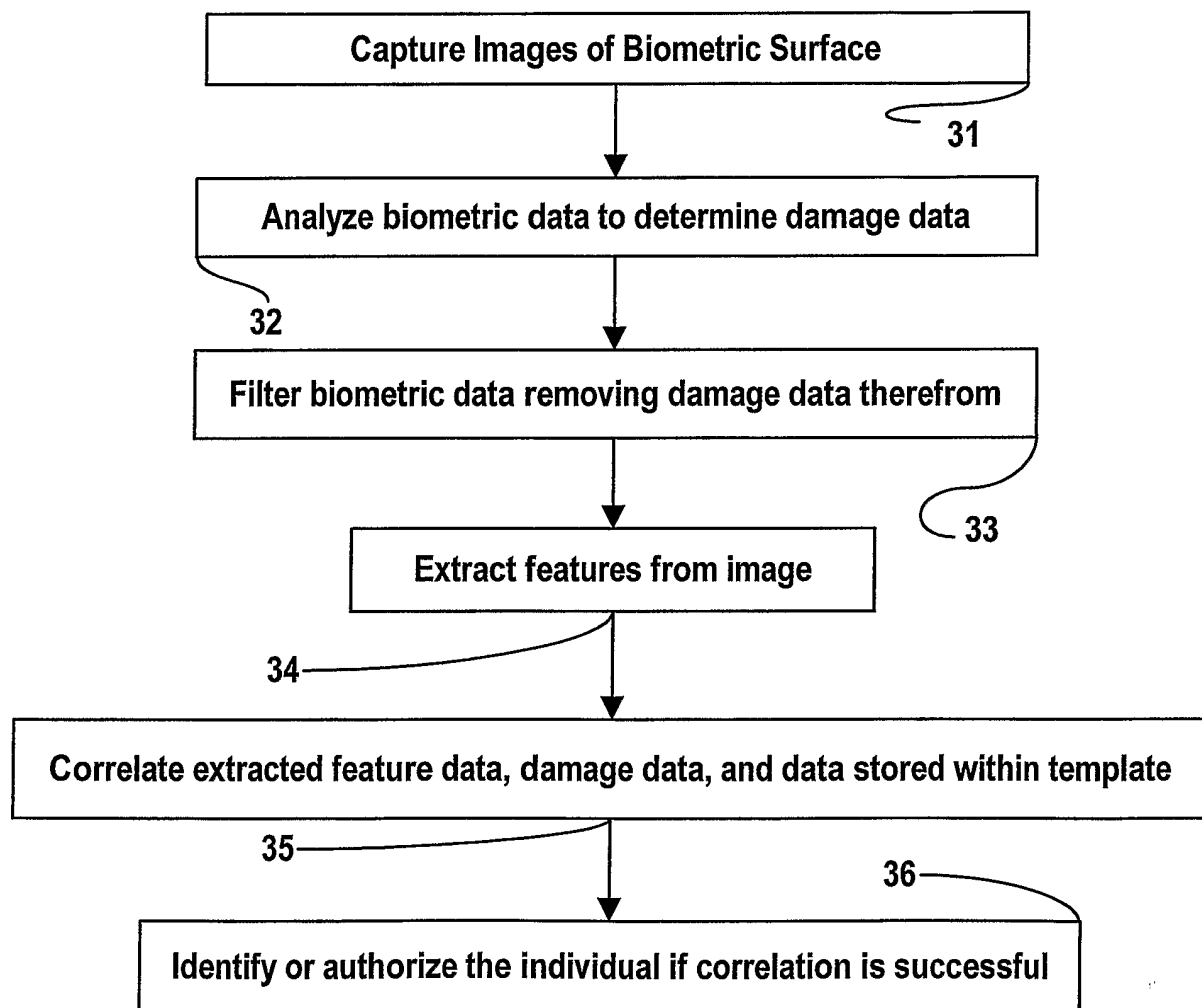


Fig. 3b

5/11

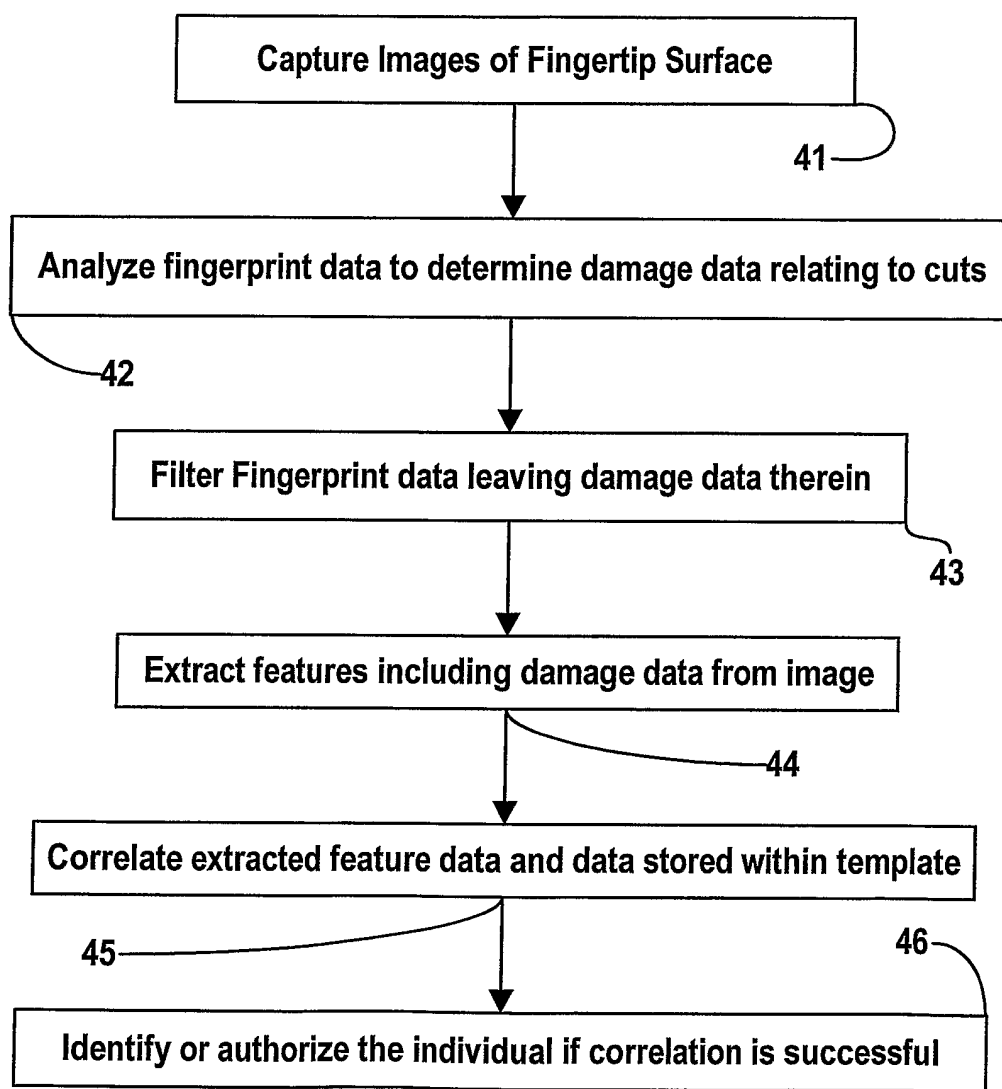


Fig. 4a

6/11

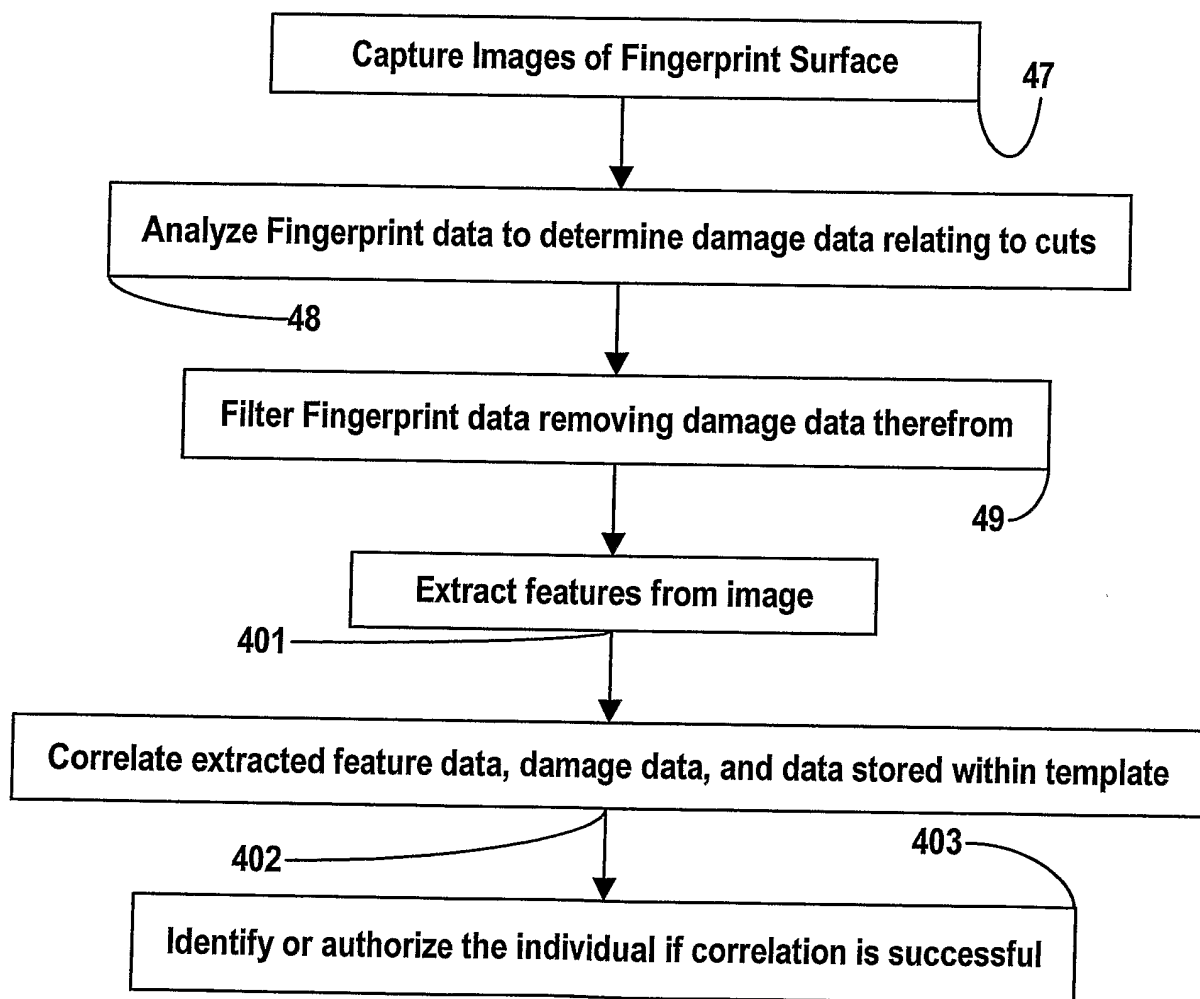


Fig. 4b

7/11

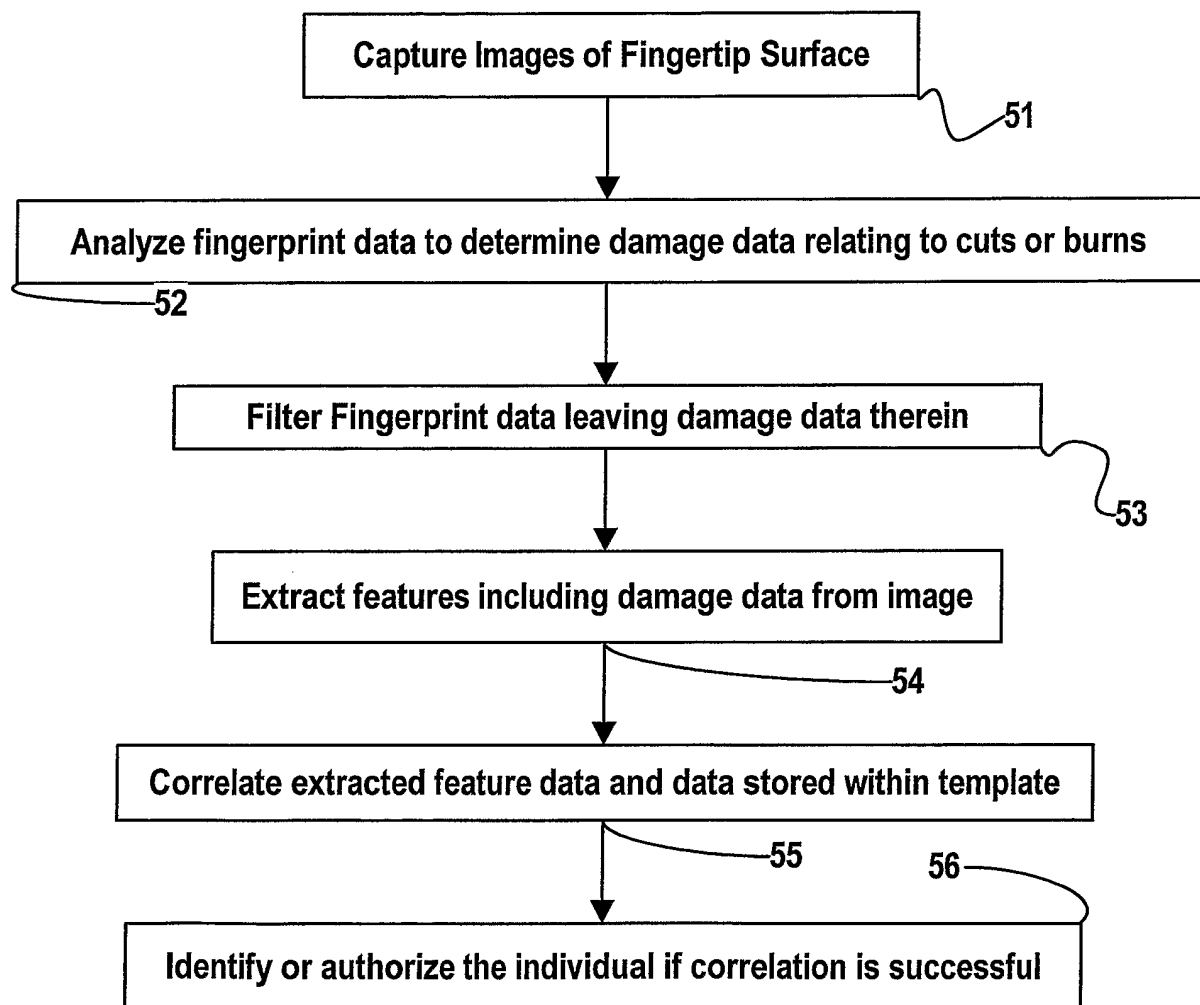


Fig. 5a

8/11

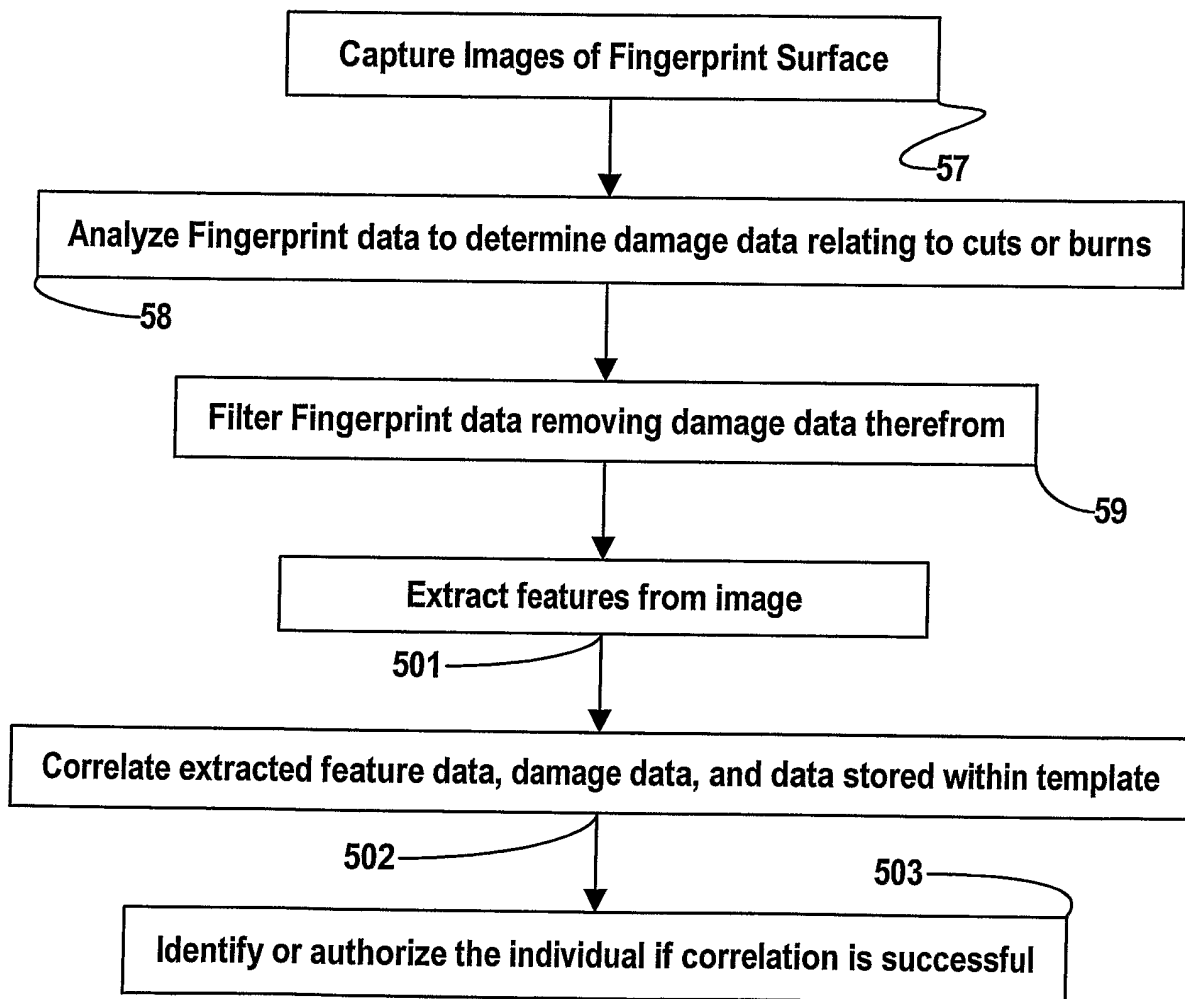


Fig. 5b

9/11

Fig. 6

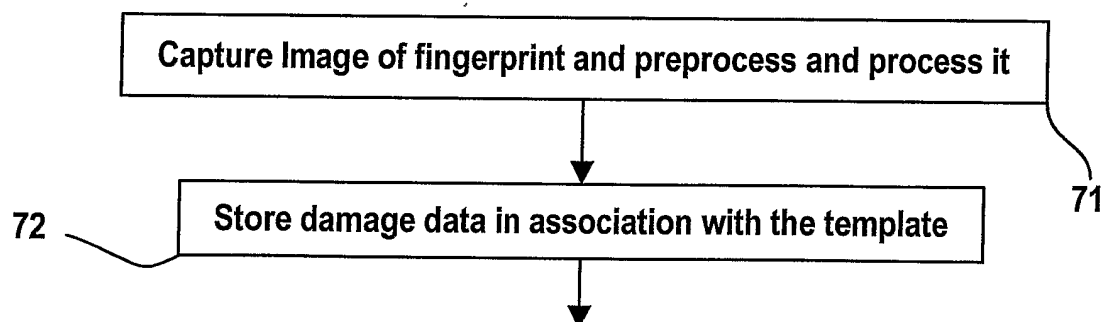
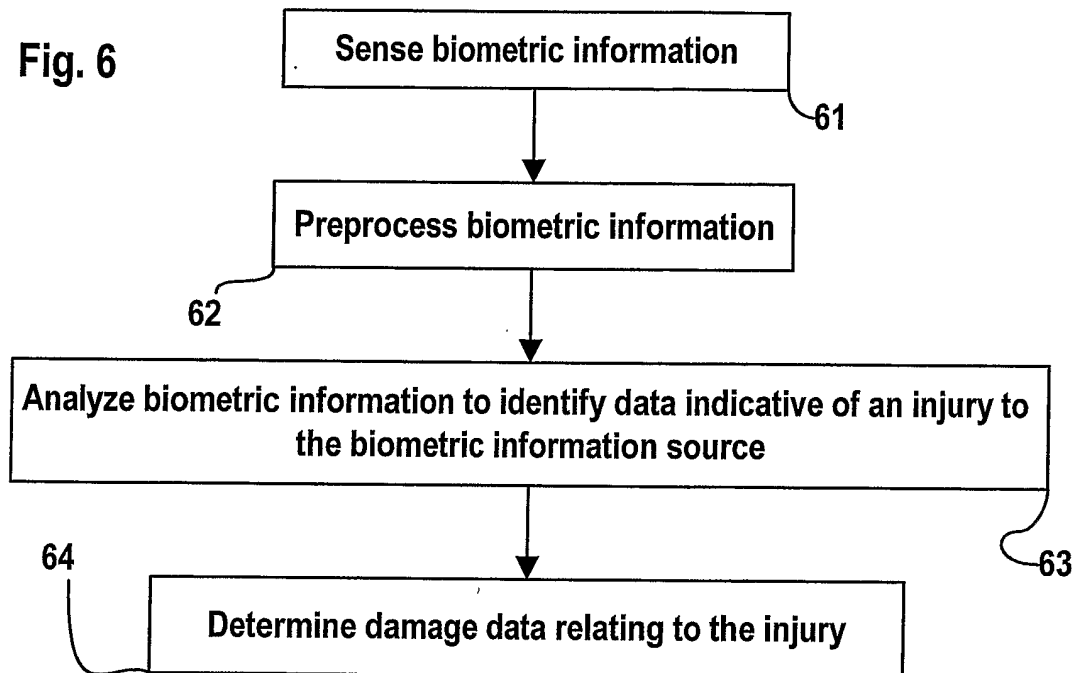


Fig. 7

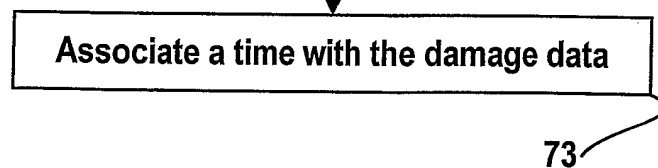
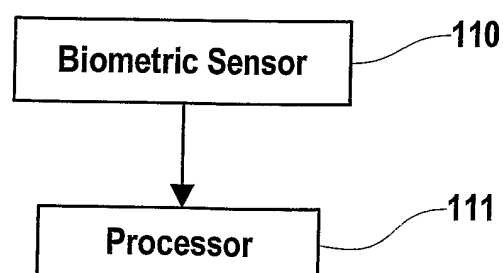


Fig. 11



10/11

Fig. 8a

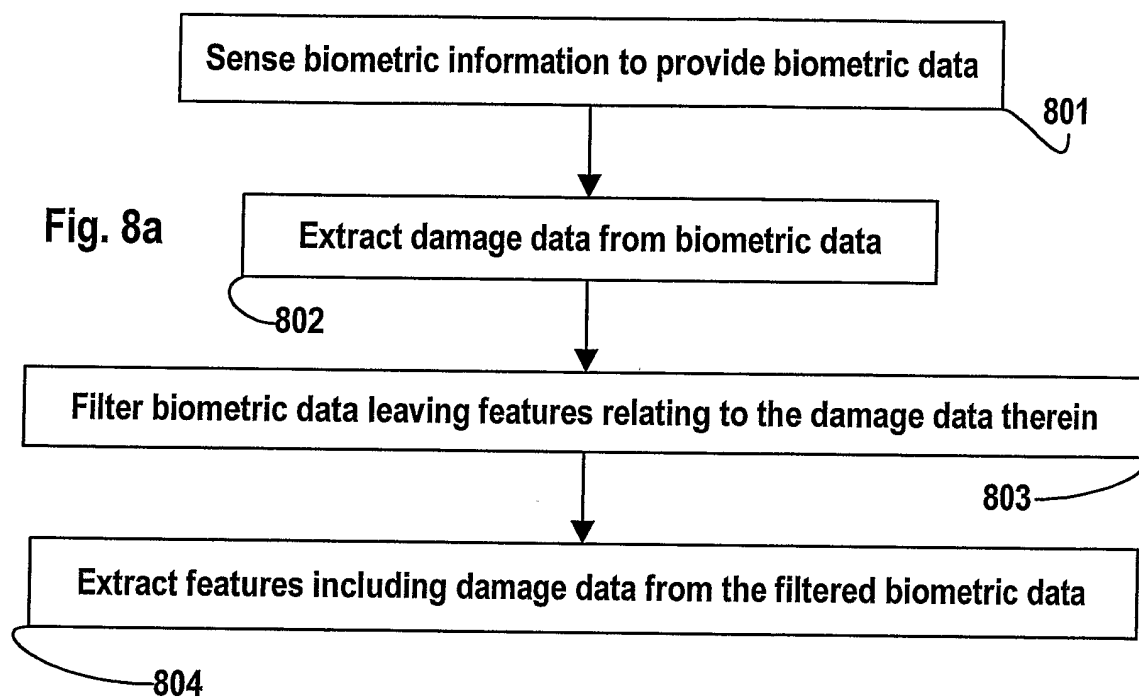
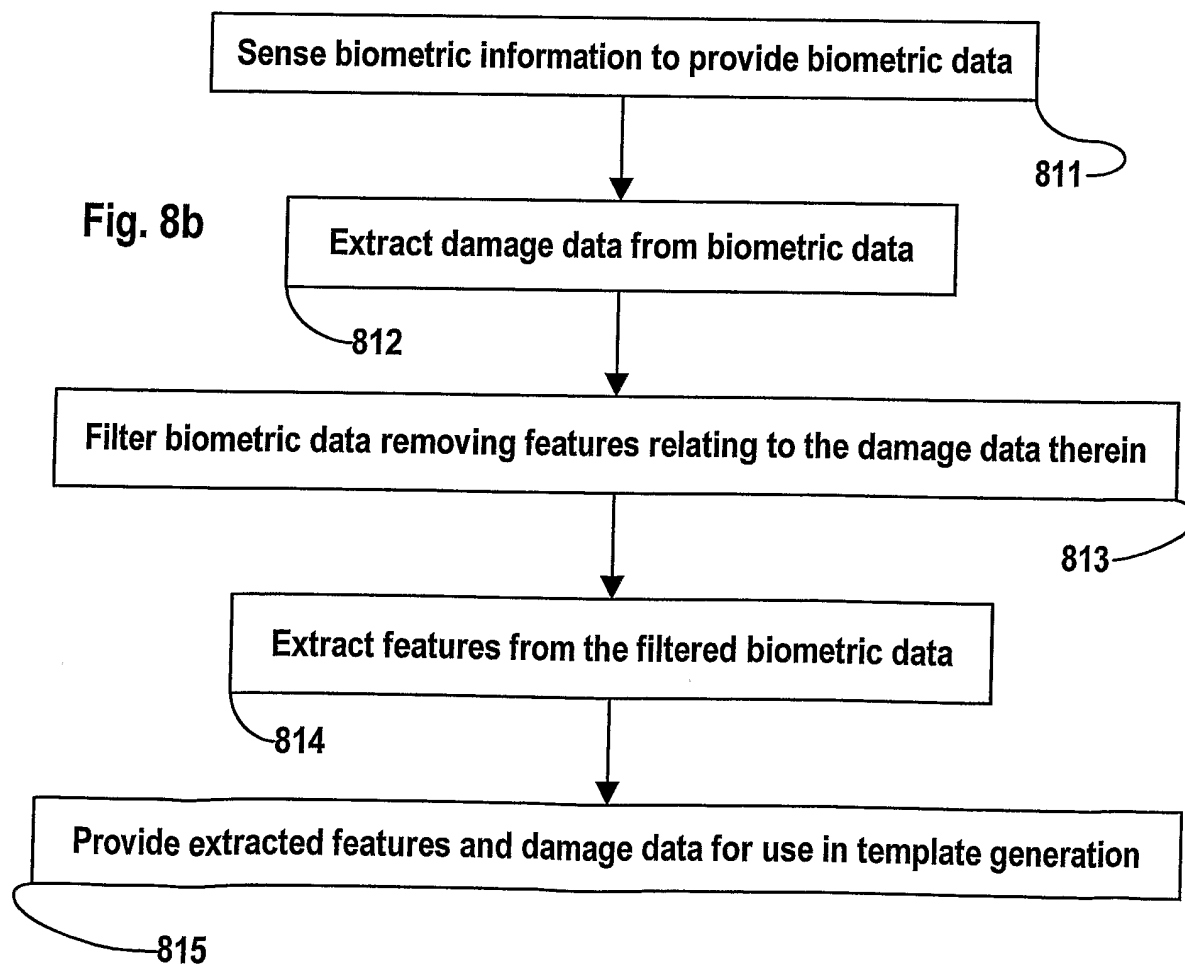


Fig. 8b



11/11

Fig. 9

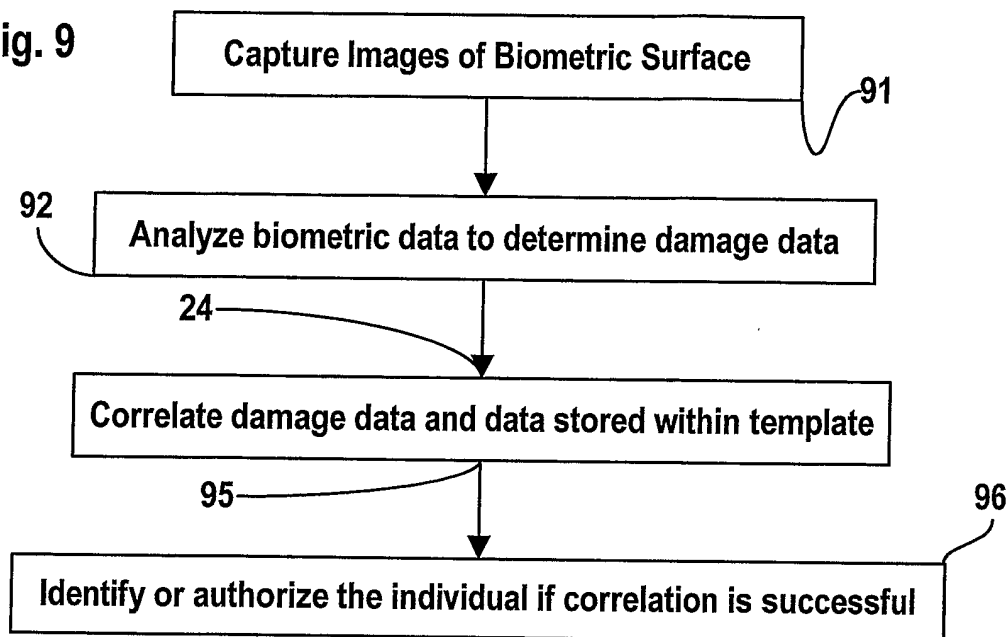
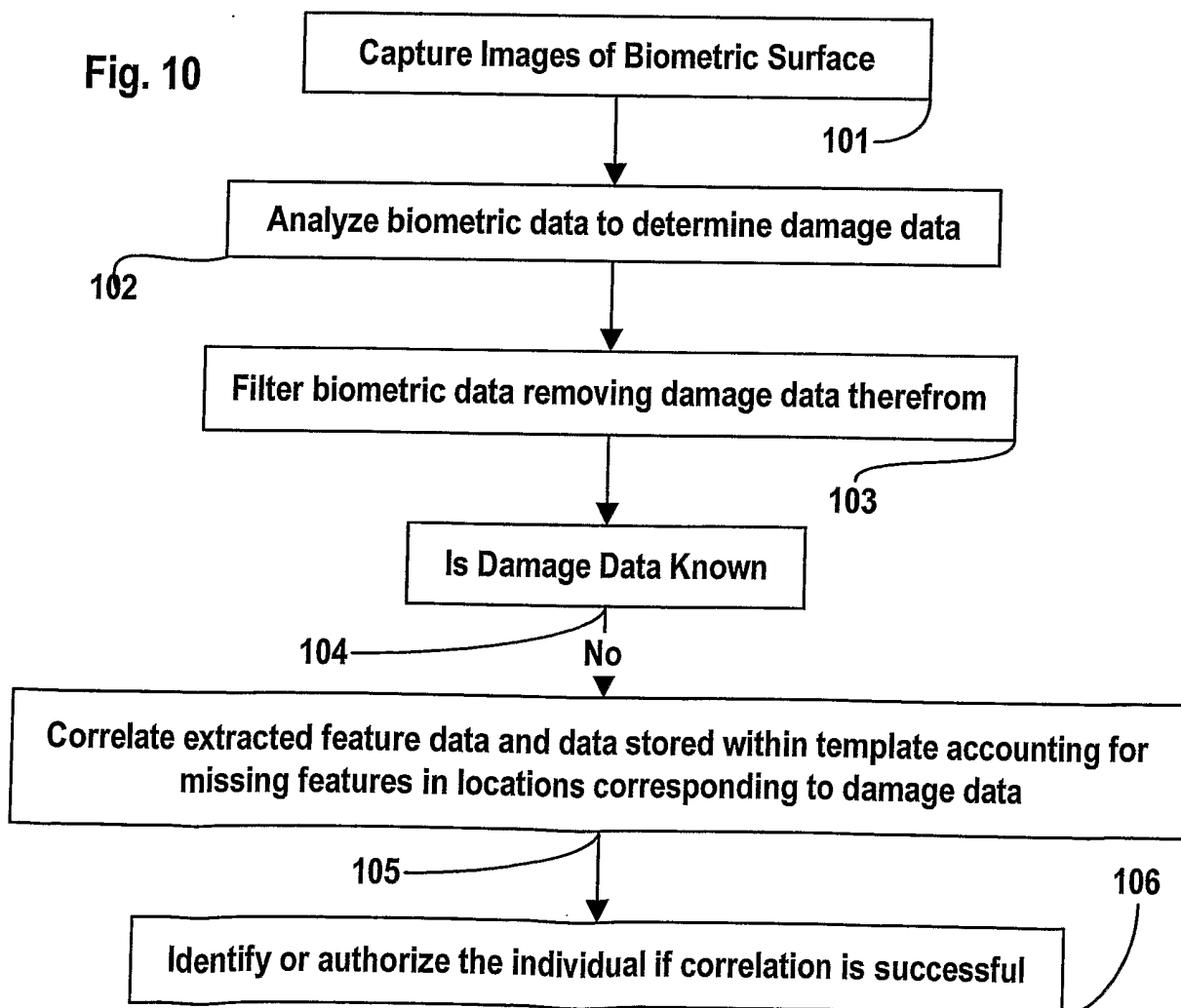


Fig. 10



INTERNATIONAL SEARCH REPORT

Internat Application No
PCT/EP 02/08067

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K9/00

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 G06K A61B G07C

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	VERNON D: "AUTOMATIC DETECTION OF SECONDARY CREASES IN FINGERPRINTS" OPTICAL ENGINEERING, SOC. OF PHOTO-OPTICAL INSTRUMENTATION ENGINEERS. BELLINGHAM, US, vol. 32, no. 10, 1 October 1993 (1993-10-01), pages 2616-2623, XP000402553 ISSN: 0091-3286	1, 10-13, 18, 19, 28-30, 32, 37
Y	abstract; figures 1, 2, 5-9 page 2618, left-hand column, paragraph 5 -page 2619, right-hand column, paragraph 1 page 2620, right-hand column, paragraph 2 -page 2621, left-hand column, paragraph 1 --- -/--	2, 3, 38, 39

☒ 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

1 October 2002

Date of mailing of the international search report

09/10/2002

Name and mailing address of the ISA

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

Authorized officer

Müller, M

INTERNATIONAL SEARCH REPORT

Internati Application No

PCT/EP 02/08067

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WAHAB A ET AL: "Novel approach to automated fingerprint recognition" IEE PROCEEDINGS: VISION, IMAGE AND SIGNAL PROCESSING, INSTITUTION OF ELECTRICAL ENGINEERS, GB, vol. 145, no. 3, 24 June 1998 (1998-06-24), pages 160-166, XP006011563 ISSN: 1350-245X	2, 3, 38, 39
A	abstract; figures 1, 3 page 161, left-hand column -----	1-76
A	GUNAWARDENA C A ET AL: "Coincident sequencing for fingerprint verification" CIRCUITS AND SYSTEMS, 1990., PROCEEDINGS OF THE 33RD MIDWEST SYMPOSIUM ON CALGARY, ALTA., CANADA 12-14 AUG. 1990, NEW YORK, NY, USA, IEEE, US, 12 August 1990 (1990-08-12), pages 845-848, XP010047970 ISBN: 0-7803-0081-5 abstract page 848, left-hand column, line 1-14 -----	1-76
A	FUNADA J ET AL: "Feature extraction method for palmpoint considering elimination of creases" PATTERN RECOGNITION, 1998. PROCEEDINGS. FOURTEENTH INTERNATIONAL CONFERENCE ON BRISBANE, QLD., AUSTRALIA 16-20 AUG. 1998, LOS ALAMITOS, CA, USA, IEEE COMPUT. SOC, US, 16 August 1998 (1998-08-16), pages 1849-1854, XP010297909 ISBN: 0-8186-8512-3 abstract; figures 1, 5-7 page 1849, right-hand column, paragraph 2 -----	1-76