

PORTABLE FINGERPRINT VERIFICATION DEVICE

Field of the Invention

[0001] The present invention relates to fingerprint identification. In particular, the present invention relates to a portable hand-held fingerprint verification device for verifying a person's identity by one's fingerprint.

Background

[0002] The rising concern of national security has led to substantive researches and developments of systems and methods of verifying individuals' identities. In particular, fingerprints have traditionally been used for verifying an individual's identity. In the present age, fingerprints are captured via fingerprint-capturing devices and are then kept in digital fingerprint databases. Such fingerprint databases are kept and managed by the relevant government authorities or trusted institutions, like banks, tax offices and lawyers' offices. The use of digital records in conjunction with the high speed computing systems have increased fingerprints verification and matching throughput. An individual's identity can now be verified through fingerprint in real-time, for example, at a border checkpoint.

[0003] Existing fingerprint capturing sensors or scanners include optical, ultrasonic, passive capacitance and active capacitance sensing. It is usually a design choice for selecting the type of fingerprint capturing sensor/scanner. Usually, fingerprints are captured in live scans to obtain fingerprint images (FPIs). The FPIs are then processed by fingerprint extraction algorithm to extract fingerprint templates (FPTs) that represent the respective FPIs. A FPT contains unique features of ridges and minutiae of each fingerprint; these features of ridges and minutiae are permanent and unchanging. The minutiae are formed by ridge endings, bifurcations and short ridges (or dots). A FPT is then matched with FPTs stored in the relevant fingerprint databases to verify a person's identity. Due to the complexity of FPT extraction and matching, only a probability or score of a match is outputted to a user. The probability/score is then compared with a predetermined threshold to decide whether or not a FPT matches those in the fingerprint databases.

[0004] If the match threshold is set high, the false accept rate (FAR) becomes low and is useful at cross-border checkpoints. At the same time, when the match threshold is set high, the false reject rate (FRR) becomes high and this causes inconvenience. Thus, according to the appropriate security level in verifying a person's identity, a match threshold is predetermined so that there is a balance between the FAR and FRR.

[0005] Fingerprint verification involves many complex processes and these are often performed by large computers. Also, there are various approaches in fingerprint verification. For example, publication no. WO2009/001121 by Warwick Warp Limited discloses a method of aligning fingerprints into a normalized framework for enrolling, matching and storing of fingerprint templates. In addition, sweat pores information is used to distinguish a live finger from an artificial finger.

[0006] In some countries, an adult individual is required to carry his or her own identity card, or similar documentation, issued by the relevant government authority for showing one's identity when demanded. Some of these identity cards or documentations are printed with the respective holders' fingerprints. However, such identification requires trained and experienced officers to carry out appropriate fingerprint verification.

[0007] It can thus be seen that there exists a need to provide a portable or hand-held fingerprint capturing and verifying device.

Summary

[0008] The following presents a simplified summary to provide a basic understanding of the present invention. This summary is not an extensive overview of the invention, and is not intended to identify key features of the invention. Rather, it is to present some of the inventive concepts of this invention in a generalised form as a prelude to the detailed description that is to follow.

[0009] The present invention provides a fingerprint verification device for a user, such as a security officer, to verify identity of an examinee via a card mode or a document mode. In the card mode, the user inserts the examinee's identification card (such as an identity or immigration card) into a card slot. In the document mode, the user places the

device on the examinee's document (such as a passport, a bank book, a tax document or a legal document). The device captures a live fingerprint of the examinee and compares it against the trusted fingerprint on the card or document to verify the examinee's identity.

[0010] In one embodiment, the present invention provides a fingerprint verification device for matching a live fingerprint against a printed fingerprint. The device comprises: a central processing unit (CPU) operable to run a fingerprint template extracting and matching algorithm; a fingerprint scanner operable to capture a live fingerprint image (FPI) of an examinee; and a camera operable to capture the printed FPI from an identity card or a trusted document; wherein the FPI captured by the camera is cropped to obtain a reference FPI, the reference FPI is scaled to a working size and associated pixel resolution is scaled to match the resolution of the fingerprint scanner; the algorithm extracts a fingerprint template (FPT) T1 from the reference FPI and a live FPT from the live FPI, and the algorithm matches the live FPT against the FPT T1 to obtain a score, scaling the FPT T1 over a range of +max% and -min% in steps of p% and repeat matching the live FPT against each scaled FPT T1 during each dynamic iteration, determining the highest score and comparing the highest score against a predetermined threshold to establish pass or fail verification.

[0011] In another embodiment, the present invention provides a method of verifying a person's identity against a printed fingerprint obtained from a trusted card or document. The method comprises: scanning the printed fingerprint to obtain a reference fingerprint image (FPI); scanning a live finger at a fingerprint scanner to obtain a live FPI; extracting a fingerprint template T1 from the reference FPI and a live fingerprint template T2 from the live FPI; matching the live fingerprint template T2 against the fingerprint template T1 to obtain a matching score; and comparing the matching score with a predetermined threshold to establish pass or fail verification.

[0012] In another embodiment, the method further comprises: scaling a resolution of the reference FPI to substantially that or near that of the fingerprint scanner prior to extracting the fingerprint template T1; scaling the fingerprint template T1 from +max% to -min% in each step of p% prior to comparing the live fingerprint template T2 to obtain

a matching score during each scaling step; and the highest matching score is used to establish the pass or fail verification.

Brief Description of the Drawings

[0013] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0014] **FIG. 1A** illustrates a top perspective view of a fingerprint verification device according to an embodiment of the present invention;

[0015] **FIG. 1B** illustrates a bottom perspective view of the fingerprint verification device shown in **FIG. 1A**;

[0016] **FIG. 2** illustrates a schematic diagram showing components used in the fingerprint verification device shown in **FIG. 1A**;

[0017] **FIG. 3** illustrates a process flow when the fingerprint verification device is used in a card mode according to another embodiment of the present invention;

FIG. 3A illustrates a process flow when the fingerprint verification device matches a fingerprint with fingerprints of wanted/missing persons;

[0018] **FIG. 4** illustrates a process flow when the fingerprint verification device is used in a document mode according to yet another embodiment of the present invention; and

FIG. 4A illustrates a process flow when the fingerprint verification device matches a fingerprint with fingerprints of wanted/missing persons.

Detailed Description

[0019] One or more specific and alternative embodiments will now be described with reference to the attached drawings. It shall be apparent to one skilled in the art, however, that this invention may be practised without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference,

common reference numerals will be used throughout the figures when referring to the same or similar features common to the figures.

[0020] FIG. 1A shows a top perspective view of a fingerprint verification device **100** according to one embodiment of the present invention. The fingerprint verification device **100** has a housing **110**. The housing **110** is sized and dimensioned for a user to hold or grip in one's hand. The housing **110** is generally a rectangular box and has an upper surface **112**, a lower surface **114** and side/end surfaces **116**. The upper surface **112** is made up of two inclined surfaces **112a,112b**. These two inclined surfaces **112a,112b** give the upper surface **112** a generally convex shape. The first inclined surface **112a** is ergonomically orientated to a user, for example, a security officer whilst the second inclined surface **112b** is ergonomically orientated for a thumb, for example, of a person or examinee whose identity is to be verified.

[0021] On the first inclined surface **112a**, there is a display screen **124**. On the second inclined surface **112b**, there is a window for a fingerprint scanner **122**. On the left hand side of the display screen **124**, with respect to the user, is a green START button **126**. The green START button **126** is used to start the fingerprint verification process when the reference fingerprint is on a document; the verification process will be described later. A red STOP button **127** for canceling the verification process is located on the right hand side of the display screen **124**. The display screen **124** is a liquid crystal display (LCD) panel and provides a visual interface to the user. Near the apex of the generally convex upper surface **112** and near the left hand edge of the housing **110** is a power indicator **132** and a processing indicator **134**. Additionally, on the side surface **116** adjacent to the indicators **132,134** is an ON/OFF power switch **130** for turning power on or off to the fingerprint verification device **100** and a USB socket **140**.

[0022] FIG. 1B shows a bottom perspective view of the fingerprint verification device **100** shown in **FIG. 1A**. The bottom surface **114** is generally planar and it includes a battery cover **150**, an optical window **160**, a card slot **170** and four anti-slip pads **180**. The battery cover **150** conceals a rechargeable battery **152** (shown in **FIG. 2**) for powering the fingerprint verification device **100**. In one embodiment, the rechargeable battery **152** is a Lithium-ion battery; in another embodiment, the rechargeable battery is a metal hydride battery. The optical window **160** has a clear glass window; behind the

optical window **160**, a camera **230** (shown in FIG. 2) is mounted for recording a printed FPI, for example, on a document that is placed near the optical window **160**. The card slot **170** is located at the end of the bottom surface **114** near to the user. The card slot **170** is dimensioned to accept an identity card or any personal identification card of an examinee. The identity card is inserted into the card slot **170** with the face of the card substantially parallel to the bottom surface **114** such that the area on the card imprinted with the examinee's FPI is substantially in register with the optical window **160**. In one embodiment, the optical window **160** is offset to one side of the fingerprint verification device **100** such that the camera **230** is operable to capture substantially a FPI on the identity card and the document. The mouth of the card slot **170** has a recessed edge **172**. The recessed edge **172** allows a user to insert an identity card into or remove it from the card slot **170** more easily. When the card slot **170** is not in use, a dust cover **174** is inserted therein. The dust cover **174** helps to minimize dust from entering the card slot **170**. The dust cover **174** is slightly smaller than the size of the identity card.

[0023] In one embodiment, the fingerprint scanner **122** is made of an active capacitance sensor type. The fingerprint scanner **122** is operable to acquire a live scan, for example, at a pixel resolution of about 500 ppi, of a thumb of the examinee. An advantage of this active capacitance type sensor is that it only responds a live finger but not to an artificial finger. In another embodiment, the fingerprint scanner **122** uses an optical, ultrasonic, thermal or passive capacitance sensor type.

[0024] In another embodiment, the fingerprint scanner **122** includes a finger guide **123** to help the examinee place one's thumb centrally on the fingerprint scanner **122**. The finger guide **123** also minimizes translational and rotational mis-placements of an examinee's thumb on the fingerprint scanner **122**.

[0025] In another embodiment, the display screen **124** is a color LCD that has sufficient pixel density to display a FPI. In use, the display screen **124** provides a live preview of a FPI when a thumb is placed on the fingerprint scanner **122**. Preview of a FPI provides visual feedback to a user so that fingerprint on the ball of the thumb is captured.

[0026] The optical window **160** and card slot **170** thus provide two modes, i.e. document mode or card mode of inputting the printed FPI against which a live FPI is to be verified.

These two modes provide flexibility for scanning fingerprints printed on different trusted documents. In another embodiment, the FPI captured through the optical window **160** is a fingerprint to be verified, for example, a FPI lifted up or located at a crime scene or on an object.

[0027] **FIG. 2** shows a schematic block diagram of the fingerprint verification device **100**. The fingerprint verification device **100** includes a central processing unit (CPU) **210**, a memory unit **220**, the camera **230**, LEDs **240**, the fingerprint scanner **122**, the display screen **124**, the START button **126**, the STOP button **127**, a card trigger switch **128**, the USB socket **130**, the power indicator **132**, the processing indicator **134** and battery **152**. Whilst not shown, the optical path of the camera **230** is bent by a front-face reflecting mirror; this mirror allows the housing **100** to attain a low height profile yet the depth of field is sufficient to capture the printed FPI on a card inserted in the card slot or a document placed near the optical window **160**.

[0028] The CPU **210** is a microprocessor that is suitable for a portable hand-held device and runs on the battery **152**. For example, the CPU **210** may be a 400 MHz micro-processor and executes a fingerprint template extracting and matching algorithm. The memory unit **220** includes a volatile memory, such as RAM **222**, and non-volatile memory, such as a flash memory **224** and an optional removeable data storage **226**. The card trigger switch **128** is an internal limit switch for initiating a fingerprint scan when an identity card is fully inserted into the card slot **170**. The USB socket **140** provides a communication link with other devices, such as a computer. The USB socket **140** may also be used for charging the battery **152**.

[0029] The power indicator **132** emits a green indicating light when the battery power is sufficient for the device **100** to operate for a reasonable period of time. The indicating light changes to amber when the battery power is low, and the amber light blinks when the battery power is very low. When the battery **152** is being charged, the power indicator **132** emits a blinking green indicating light.

[0030] **FIG. 3** shows a process **300** of verifying fingerprint using the fingerprint verification device **100** according to the card mode. The process **300** is illustrated with reference to **FIGs. 1A, 1B** and **2**. The process **300** starts at step **305**, in which power to

the device **100** is turned ON and the power indicator **132** is lighted up in green, showing that the device **100** is ready for use. In the following step, i.e. step **310**, the user inserts the examinee's identity card into the card slot **170**; in one embodiment, the identity card is an immigration card, such as a work-permit card. Once the identity card is fully inserted, in step **315**, the card trigger switch **128** is activated and the LEDs **240** are turned on. In step **320**, a time delay, for example, 0.5 seconds is initiated before process **300** continues further.

[0031] The camera **230** then proceeds to capture the printed FPI from the identity card in step **325**. Once, the printed FPI is captured, the LEDs **240** are turned off. Next, in step **327**, the FPI captured by the camera **230** is cropped to obtain a card FPI. By cropping the FPI captured by the camera, any letters, numbers and barcode, etc. that may be captured with the FPI are removed, leaving only the FPI for verification. In step **330**, the size of the card FPI is scaled to a working size by applying an average card fingerprint size factor (card-avg) on the card FPI. In step **335**, the working size card FPI obtained in step **330** is then scaled by a pixel resolution factor (Pr) so that resolution of the card FPI is about or near to the resolution of the live FPI captured by the fingerprint scanner **122**. For example, the card FPI captured by the camera **230** is about 750 ppi whilst the live FPI captured by the fingerprint scanner **122** is about 500 ppi. Next, in step **340**, a reference FPT **T1** is extracted from the FPI obtained in step **335**. When the template extracting algorithm is extracting the reference FPT **T1**, the processing indicator **134** emits a blue indicating light.

[0032] When the template extraction is completed and the processing indicator **134** is extinguished, the examinee is then prompted, in step **350**, to place a thumb on the fingerprint scanner **122** and a live FPI is then captured in step **355**. In step **360**, the display screen **124** provides a preview of the FPI captured by the fingerprint scanner **122**. A decision is then made by the user whether the live FPI is near the centre of the thumb of the examinee. If the live FPI is not an image near the centre of the thumb, the user prompts the examinee to place one's thumb on the fingerprint scanner **122** again and steps **355** and **360** are executed again. Next, a live FPT **T2** is extracted in step **375**.

[0033] Following step **375**, the FPT **T1** obtained in step **340** is scaled to +max% in step **380** and the live FPT **T2** is compared with the scaled FPT **T1**. A score is generated by

the matching algorithm running in the CPU **210** and the score is then stored in the RAM **222**. When a matching activity in step **380** is taking place, the processing indicator **134** emits a blinking blue indicating light. Scaling of the FPT **T1** is then reduced in steps of $p\%$ in each matching process in step **380** until the FPT **T1** is reduced to $-\text{min}\%$. After each matching process in step **380**, the respective scores are stored in the RAM **222**. At the end of step **380**, the highest score is then compared with a predetermined threshold. A decision is then made whether **T2** substantially matches **T1**. If the highest score is greater than the predetermined threshold, there is a certainty that the printed FPI belongs to the examinee and a “pass” indication, in step **390**, is shown on the display screen **124**. If the highest score is less than the predetermined threshold, the printed FPI is determined not to belong to the examinee and the process **300** executes step **385**. Step **385** allows the examinee three chances to position one’s thumb on the fingerprint scanner **122**, i.e. re-execute steps **350**, **355**, **360**, **375** and **380** two more times. If **T2** does not substantially match **T1** in the third try, a “fail” indication is shown on the display screen **124** and the process **300** proceeds to step **395**. After the identity of the examinee is determined, the identity card is removed, in step **395**, and the user deals appropriately with the examinee. At the same time, a power save and/or power off feature in the device **100** may then be initiated if there is a long waiting time to verify identity of another examinee. For example, the power save is initiated after 5 minutes and the power off is initiated after 15 minutes of inactivity.

[0034] In step **380**, the FPT **T1** is scaled from $+\text{max}\%$ to $-\text{min}\%$ in steps of $p\%$. The $+\text{max}\%$ is chosen so that it is generally larger than the average card fingerprint size factor (card-avg). In one embodiment, $+\text{max}$ is $+20$ and $-\text{min}$ is -20 ; in another embodiment, p ranges from 1 to 5.

[0035] In the above verification process **300**, the process is described with steps being carried out in a sequential manner. If the CPU **210** has sufficient capacity, some of the process steps can be carried out in parallel. For example, steps **325** to **340** may be carried in parallel with steps **350** to **375**. The parallel branching points in **FIG. 3** are indicated by nodes **W**, **X** and **Y**.

[0036] **FIG. 3A** shows step **382** for matching of the live FPT **T2** of an examinee against pre-stored FPTs of wanted or missing persons and step **384** for displaying results of

identity verification. Steps **382** and **384** may be carried after step **380** or in parallel with steps **380** and **390**. The parallel branching points in **FIG. 3** are indicated by nodes **Y** and **Z**.

[0037] **FIG. 4** shows a verification process **400** of verifying fingerprint using the fingerprint verification device **100** according to the document mode. If the device is not already power up, the device **100** is started by turning ON the power switch **130** in step **405**. Once the device is ready and the power indicator **132** is green, the user places, in step **410**, the device **100** over a trusted document that carries a printed FPI. The trusted document may be a bank book, a passport, a tax document, a legal document, etc. With the preview from the display screen **124**, the user re-positions the device on the trusted document so that the optical window **160** is in register with the printed FPI and the camera **230** is operable to capture the printed FPI. The user then presses the START button **126**, in step **415**, to start the verification process **400**.

[0038] Following step **415**, the LEDs **240** are turned on and the camera **230** captures the printed FPI in step **425**, , scales the pixel resolution of the FPI captured by the camera **230** to substantially that of the fingerprint scanner **122** in step **435** and extracts a reference FPT **T1** in step **440**; steps **435** and **440** are similar to steps **335** and **340** described in the previous process **300**. Similarly, steps **450** to **475** corresponding to steps **350** to **375** in the previous process **300** are carried out in this process **400** and identity of the examinee is matched by comparing the live FPT **T2** against the reference FPT **T1** in step **480**. Like in the previous step **380**, the reference FPT **T1** is scaled to +max% in step **480** and a matching score is then stored in the RAM **222**. Scaling of the reference FPT **T1** is reduced in steps of p% in each matching process in step **480** until the printed FPT **T1** is reduced to -min%. A decision is then made whether **T2** substantially matches **T1**. The highest matching score that is greater than a predetermined threshold indicates that the printed FPI belongs to the examinee and a “pass” indication, in step **490**, is shown on the display screen **124**. If the highest matching score is less than the predetermined threshold, the printed FPI is determined not to belong to the examinee and the process **400** proceeds to step **485**. Step **485** allows the examinee three chances to position one’s thumb on the fingerprint scanner **122** and re-executes steps **450**, **455**, **460**, **475** and **480** two more times. If **T2** does not substantially match **T1** in the third try, a “fail” indication

is shown on the display screen **124** and the process 400 proceeds to step 495. After the identity of an examinee is determined, the device **100** and document are removed, in step **495**, and the user deals appropriately with the examinee. At the same time, a power save and/or power off feature in the device **100** may then be initiated if there is a long wait to verify identity of another examinee. If the printed FPI on the trusted document is not the same size as the live FPI, scaling of the FPI captured by the camera 230 will need to be executed before step 435.

[0039] Again as in the previous process 300, some of the steps in the process **400** can be carried out in parallel. For example, steps **425** to **440** can be carried out in parallel with steps **450** to **475**. The parallel branching points in **FIG. 4** are indicated by nodes **W1**, **X1** and **Y1**.

[0040] **FIG. 4A** shows step **482** for matching of the live FPT **T2** of an examinee against pre-stored FPTs of wanted or missing persons and step **484** for displaying results of identity verification. Steps **482** and **484** may be carried after step **480** or in parallel with steps **480** and **490**. The parallel branching points in **FIG. 4** are indicated by nodes **Y1** and **Z1**.

[0041] In the present invention, it is possible that the images of the printed fingerprint and the live fingerprint and associated templates are stored in a non-volatile memory **224** according to another embodiment of the present invention. These FPIs and FPTs can then be transferred to a computer via the USB socket **140**. The FPTs of wanted/missing persons can also be updated through the USB socket **140**. In addition, data logging activity of the device **100** can also be transferred from the USB socket **140** to a computer/server for recording purposes.

[0042] In another embodiment, the scaling of the entire fingerprint images is carried out instead of scaling the fingerprint templates. Such scaling also affects the sizes and pixel resolutions of the FPIs and FPTs.

[0043] In another embodiment, the fingerprint verification device **100** includes a touch screen instead of the display screen **124**. A touch screen may allow a user to manually select areas on a captured PFI for cropping.

[0044] In another embodiment, instead of determining whether the fingerprint verification processes 300,400 pass tests by checking the highest matching scores against a predetermined threshold, the verification processes 300, 400 is configurable to compare the matching score against the predetermined threshold as step 380,480 is dynamically iterating and matching scores are being generated. When a matching score is found to be higher than the predetermined threshold, the fingerprint verification is considered affirmative and the fingerprint verification process is then concluded before the entire iteration in step 380, 480 is completed.

[0045] While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the invention. For example, an additional vertical card slot may be provided on the right hand side of the fingerprint verification device 100 to input a trusted FPI or FPT from a smart card. In another example, instead of using LEDs to provide illumination for the camera, another light source may be used.

CLAIMS:

1. A fingerprint verification device for matching a live fingerprint against a printed fingerprint, the fingerprint verification device comprising:

a central processing unit (CPU) operable to run a fingerprint template extracting and matching algorithm;

a fingerprint scanner operable to capture a live fingerprint image (FPI) of an examinee; and

a camera operable to capture the printed FPI from an identity card or a trusted document;

wherein the FPI captured by the camera is cropped to obtain a reference FPI, the reference FPI is scaled to a working size and associated pixel resolution is scaled to match the resolution of the fingerprint scanner; the algorithm extracts a fingerprint template (FPT) T1 from the reference FPI and a live FPT from the live FPI, and the algorithm matches the live FPT against the FPT T1 to obtain a score, scaling the FPT T1 over a range of +max% and -min% in steps of p% and repeat matching the live FPT against each scaled FPT T1 during each dynamic iteration, determining the highest score and comparing the highest score against a predetermined threshold to establish pass or fail verification.

2. A device according to claim 1, further comprising a housing, which is dimensioned to fit in a user's hand, said housing having two inclined surfaces to form a generally convex upper surface and a planar lower surface.

3. A device according to claim 2, further comprising a display screen disposed on the inclined upper surface that is orientated to the user.

4. A device according to claim 2 or 3, wherein the fingerprint scanner is disposed on the inclined upper surface that is orientated opposite the user.

5. A device according to any one of claims 2 to 4, further comprising a card slot disposed at an end near to the user but parallel to the planar lower surface.

6. A device according to any one of claims 2 to 5, wherein the planar lower surface has an optical window, inside which is disposed the camera.
7. A device according to claim 6, wherein the camera is operable to capture the printed FPI from an identity card inserted into the card slot or to capture the printed FPI on a trusted document through the optical window.
8. A device according to any one of claims 1 to 7, wherein prior to scaling the FPI captured by the camera, an average size of the printed FPI is determined and a size scaling factor (card-avg, D-avg) is applied on the FPI captured by the camera to obtain the working size of the FPI.
9. A device according to any one of claims 2 to 8, further comprising a slot to receive a smart card, wherein the slot is disposed on a side surface of the housing.
10. A device according to any one of claims 1 to 9, further comprising a pre-stored database of FPTs belonging to wanted or missing persons, so that the live FPT is verified with the pre-stored FPTs.
11. A device according to any one of claims 1 to 10, wherein the identity card is an immigration card or trusted document is a bank book, a tax document and a legal document.
12. A device according to any one of claims 1 to 11, wherein the printed FPI is a forensic fingerprint at a crime scene or on an object.
13. A device according to any one of claims 1 to 12, wherein +max% is +20% and -min% is -20%.
14. A device according to claim 13, wherein p ranges from 1 to 5.
15. A method of verifying a person's identity against a printed fingerprint obtained from a trusted card or document, the method comprising:

scanning the printed fingerprint to obtain a reference fingerprint image (FPI);
scanning a live finger at a fingerprint scanner to obtain a live FPI;
extracting a fingerprint template T1 from the reference FPI and a live fingerprint template T2 from the live FPI;
matching the live fingerprint template T2 against the fingerprint template T1 to obtain a matching score; and
comparing the matching score with a predetermined threshold to establish pass or fail verification.

16. A method according to claim 15, further comprising cropping the reference FPI at a predefined area prior to extracting the fingerprint template T1.

17. A method according to claim 15 or 16, further scaling the size of the reference FPI by an average fingerprint size factor (card-avg) of the printed fingerprint prior to extracting the fingerprint template T1.

18. A method according to any one of claims 15 to 17, further comprises scaling a resolution of the reference FPI to substantially that or near that of the fingerprint scanner prior to extracting the fingerprint template T1.

19. A method according to any one of claims 15 to 18, further comprising scaling the fingerprint template T1 from +max% to -min% in each step of p% prior to comparing the live fingerprint template T2 to obtain a matching score during each scaling step.

20. A method according to claim 19, wherein the highest matching score is used to establish the pass or fail verification.

21. A method according to claim 19 or 20, wherein max% and min% is greater than the average fingerprint size factor (card-avg).

22. A method according to any one of claims 19 to 21, wherein +max is +20%, -min is -20% and p ranges from 1 to 5.