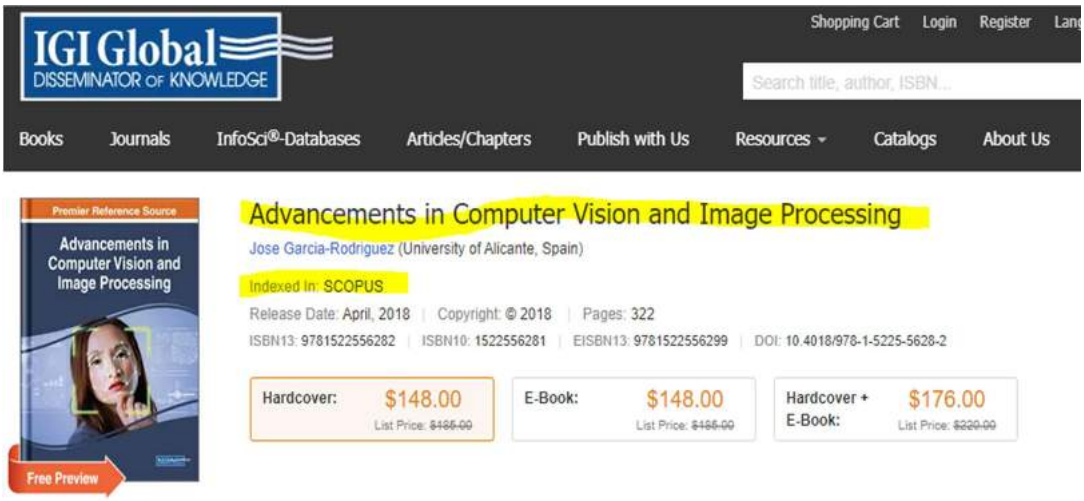
Advancements in Computer Vision and Image Processing



Description

Interest in computer vision and image processing has grown in recent years with the advancement of everyday technologies such as smartphones, computer games, and social robotics. These advancements have allowed for advanced algorithms that have improved the processing capabilities of these technologies.

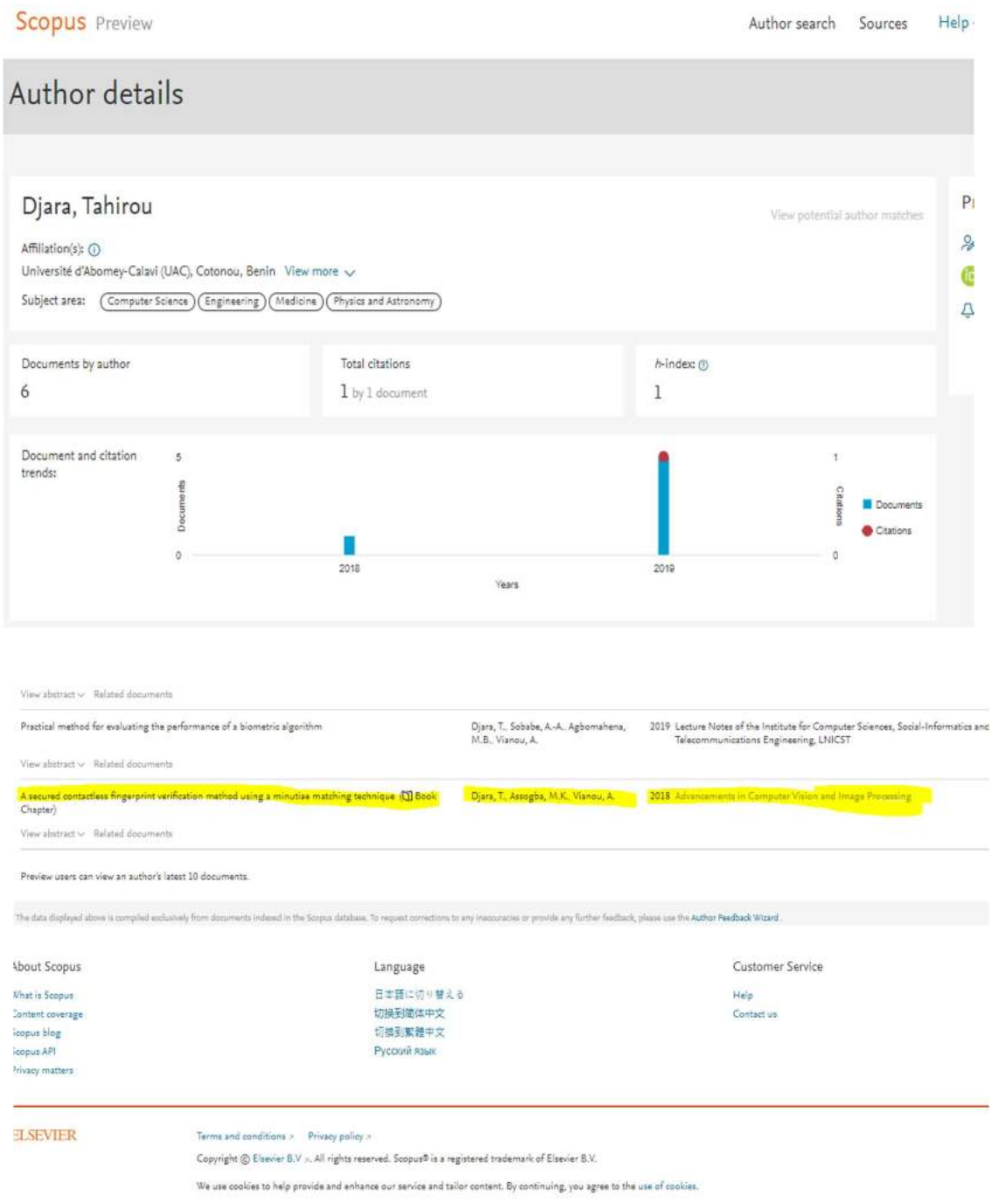
Advancements in Computer Vision and Image Processing is a critical scholarly resource that explores the impact of new technologies on computer vision and image processing methods in everyday life. Featuring coverage on a wide range of topics including 3D visual localization, cellular automata-based structures, and eye and face recognition, this book is geared toward academicians, technology professionals, engineers, students, and researchers seeking current research on the development of sophisticated algorithms to process images and videos in real time.

Indices

Filter by indice name

Scopus®
SCOPUS

PREUVE D'INDEXATION



Scopus Preview

Author search Sources Help

Author details

Djara, Tahirou

View potential author matches

Affiliation(s):

Université d'Abomey-Calavi (UAC), Cotonou, Benin View more

Subject area: Computer Science Engineering Medicine Physics and Astronomy

Documents by author
6

Total citations
1 by 1 document

h-index:
1

Document and citation trends:

View abstract Related documents

Practical method for evaluating the performance of a biometric algorithm — Djara, T., Sobabe, A.-A., Agbomahena, M.B., Vianou, A. — 2019 Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST

View abstract Related documents

A secured contactless fingerprint verification method using a minutiae matching technique (Book Chapter) — Djara, T., Assogba, M.K., Vianou, A. — 2018 Advancements in Computer Vision and Image Processing

View abstract Related documents

Preview users can view an author's latest 10 documents.

The data displayed above is compiled exclusively from documents indexed in the Scopus database. To request corrections to any inaccuracies or provide any further feedback, please use the Author Feedback Wizard.

About Scopus
What is Scopus
Content coverage
Scopus blog
Scopus API
Privacy matters

Language
日本語に切り替える
切换到简体中文
切換到繁體中文
Русский язык

Customer Service
Help
Contact us

ELSEVIER

Terms and conditions Privacy policy

Copyright © Elsevier B.V. All rights reserved. Scopus® is a registered trademark of Elsevier B.V.

We use cookies to help provide and enhance our service and tailor content. By continuing, you agree to the use of cookies.

Chapter 9
A Secured Contactless Fingerprint Verification Method Using a Minutiae Matching Technique

Tahirou Djara
Université d'Abomey-Calavi, Benin

Marc Kokou Assogba
Université d'Abomey-Calavi, Benin

Antoine Vianou
Université d'Abomey-Calavi, Benin

ABSTRACT

Most matching or verification phases of fingerprint systems use minutiae types and orientation angle to find matched minutiae pairs from the input and template fingerprints. Unfortunately, due to some non-linear distortions, like excessive pressure and fingers twisting during enrollment, this process can cause the minutiae features to be distorted from the original. The authors are interested in a fingerprint matching method using contactless images for fingerprint verification. After features extraction, they compute Euclidean distances between template minutiae (bifurcation and ending points) and input image minutiae. They compute then after bifurcation ridges orientation angles and ending point orientations. In the decision stage, they analyze the similarity between templates. The proposed algorithm has been tested on a set of 420 fingerprint images. The verification accuracy is found to be acceptable and the experimental results are promising. Future work will enhance the proposed verification method by a new template protection technique.

DOI: 10.4018/978-1-5225-5628-2.ch009

INTRODUCTION

Biometric authentication has received extensive attention over the past decade with increasing demands in automated personal identification as fingerprints are assumed to be unique across individuals, and fingers of the same individual (Pankanti et al., 2002). However, contact based fingerprint systems have some drawbacks due to skin elasticity, inconsistent finger placement, contact pressure, small sensing area, environment conditions and sensor noise. Additionally, problems like skin conditions (e.g. dirty or wet) and contagious diseases spreading make the use of contact based scanners not very safe (Yin et al., 2016). Another major risk in the contact-based systems is the possibility of chemical or bacteriological attacks. This risk is increasingly increased with the development of international terrorism nowadays. We are then interested in a fingerprint matching method using contactless images for fingerprint verification.

Depending on the application context, a biometric system may be called either a verification system or an identification system (Maltoni et al., 2003; AlMahafzah et al., 2012). A verification system authenticates a person's identity by comparing the captured biometric reference template pre-stored in the system. It conducts one-to-one comparison to confirm whether the claim of identity by the individual is true. An identification system recognizes an individual by searching the entire enrollment template database for a match. It conducts one-to-many comparisons to establish if the individual is present in the database and if so, returns the identifier of the enrollment reference that matched.

Fingerprint matching techniques can be coarsely classified into three categories, namely minutiae-based matching (Jain et al., 1997; Medina-pérez et al., 2012), image-based matching (A. Qader et al.,2006; Ito et al., 2009; Jain et al., 2000, Sha et al., 2003) and hybrid matching technique (Khalila et al., 2010; Kumar et al., 2012). Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae feature sets that result in the maximum number of minutiae pairings.

In this paper, we present a contactless fingerprint verification method using a minutiae matching technique, based on the alignment between template images acquired by a contactless system and input images acquired by the same way. Contactless images have been acquired and stored in a database during an enrollment step. The first stage in an Automatic Fingerprint Verification procedure is to extract minutiae from fingerprints. In our contactless fingerprint verification system, we have implemented a minutia extraction algorithm which has been presented in (Djara et al., 2010). The extracted features are ridge bifurcation, ridge ending and ridges orientations. Authors in (Kumar et al., 2012;He et al., 2002; Virk&Maini, 2012) determine orientations using horizontal axis.

Most of the matching or verification of the fingerprint verification systems use minutiae types and orientation angle to find matched minutiae pairs from the input and template fingerprints (Tiko&Kuosmanen, 2003). Thus, accuracy of the verification stage largely depends on the minutiae extraction process. Unfortunately, due to some non-linear distortion, like excessive pressure and twisting of fingers during enrollment, this process can cause the minutiae features to be distorted from the original. Some authors have used the Smallest Minimum Sum of Closest Euclidean Distance of bifurcation points to improve the accuracy of fingerprint verification (Bhowmik et al., 2009).

To overcome those drawbacks, we work on contactless fingerprint images. After features extraction, we compute Euclidean distances between template minutiae and input image minutiae. We compute then after ridges bifurcation orientations and the ridgesending orientations. In the decision stage, we analyze the similarity between templates. Our algorithm has been tested by computing various similarity scores.

In section 2 we present a literature review oriented on the biometric systems security in general and the special case of contactless fingerprint systems. In section 3 the experimental condition i.e. the contactless enrollment. Feature representation is presented in section 4. Ridge bifurcation and Ridge ending similarity are described in Section 5. Section 6 presents our minutiae matching algorithm. Section 7 presents the experimental results. Section 8 presents our outlook for the future and section 9 concludes the paper.

BACKGROUND

Biometric verification systems in general are subject to spoofing attacks in order to bypass them. These attacks are perfect from day to day and require appropriate measures. Several techniques are proposed to deal with these attacks and to secure the biometric systems. The proposed solutions can be divided into two main categories, palliative solutions and preventive solutions (Marasco et al., 2015). Each category can be divided into two types (hardware types and software types). There are two main methods of spoofing (Mojtaba M, 2010): Co-operative spoofing and non-Cooperative spoofing. Attacks are made by exploiting vulnerability points located at five levels of the biometric system (Javier G, 2014). It is:

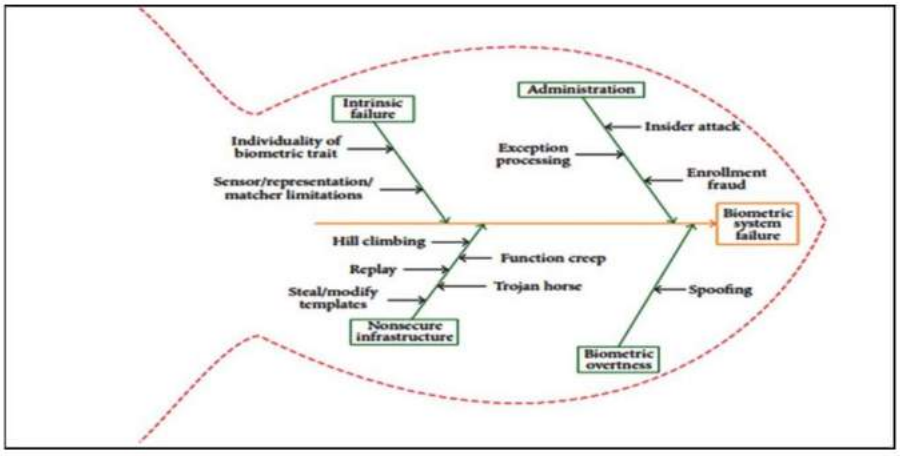
1. **Presentation Attacks:** Reproduction of biometric modality is presented at the inputs.
2. Sensor is bypassed and previously stored data is hacked and used.
3. The set of extracted features are replaced with the false sets.

4. The matcher is corrupted and sample is matched with the false set.
5. The final match is altered by an attacker.

Indeed, security holes have been identified in all biometric systems. Thus Jain et al. in September 2007 have listed the vulnerabilities in the form of fishbone.

The contactless verification system presented in this paper makes it possible to limit the possibilities of reproduction of the fingerprint because the system avoids leaving traces at the image acquisition step. In addition, the contactless system allows the implementation of the 3D technique which offers better security. The 3D technique allows the sensor to differentiate between a finger and an image of the finger. This technique also improves the recognition algorithm (Kumar&Kwong, 2015; Yin et al., 2016) and offers good resistance to software level attacks. The finger vivacity recognition techniques also make it possible to fight against the reproduction (Matsumoto et al., 2002). One of the major challenges of fingerprint verification is the improvement of recognition accuracy. Several works have been carried out in this direction. In 2013, (Labati et al., 2013) proposed a neural network-based approach for the rotation effects reduction. This approach has reduced the ERR of existing biometric systems from 3.04% to 2.20%. In the fingerprint recognition process, the minutiae detection phase is very important for the overall performance of the system. Thus, (Liu et al., 2016) proposed a 3-step approach to improving image quality in the detection of minutiae of the contactless fingerprint. In addition, contactless fingerprint images often contain noises and have low contrast. To solve this problem, (Yin et al., 2016) proposed a method for intrinsic image decomposition and guided image

Figure 1. List of fishbone vulnerabilities (Jain et al, 2007)



filtering. All that techniques can contribute to improve the contactless systems. In this paper we focus on the minutiae matching technique.

CONTACTLESS ENROLLMENT

After the tragic attacks of September 11, 2001, the need for improved and reliable fingerprint recognition technology drastically increased. Despite the known deficiencies and drawbacks of contact-based fingerprinting, this method is still deployed. Although contactless methods are known for producing distortion free fingerprints, this is a rather new technological development, and very few universities are involved in their development. Among authors interested by contactless fingerprint development, we have (Parziale et al., 2006; Hiew et al.,2007;Mil'shtein et al., 2008). Other authors present in an academic work, recent applications in contactless fingerprint (Milshtein et al., 2011; Pillai&Milshtein, 2012; Labati et al., 2013; Liu et al., 2016; Yin et al., 2016; Arora et al., 2016).

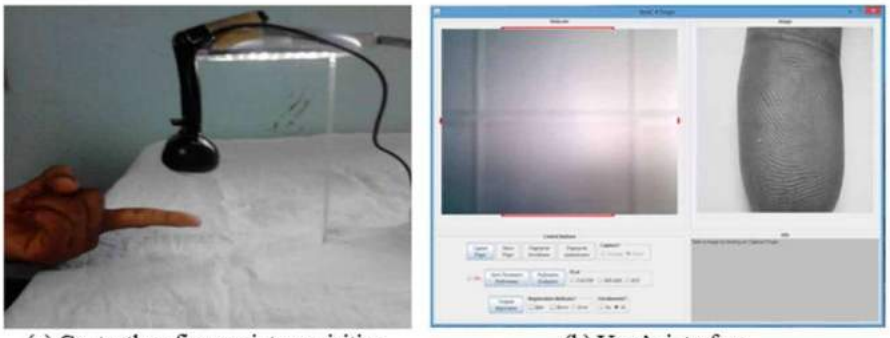
Acquisition Protocol

We have developed a Contactless Biometric Fingerprint Software (CBFS) for the acquisition and processing of our images. The contactless fingerprint acquisition system consists of this CBFS to visualize the sharpness of the finger before capture, a webcam for taking digital photo, and lighting equipment. The user is asked to put his finger in a fixed position, the reverse of his finger on the indicated place and his palm faces the camera. We use a medium-resolution webcam (Logitech Pro9000), driven by an interface as shown in Figure 2. In order to limit travel, a rectangular area is defined on the interface of the camera which will contain the finger before capture (area marked "1"). The acquired images are PNG format and have a size of 640x640. Figure 2-(a) shows the system and Figure 2-(b) shows a screenshot of the user's interface.

In acquisition stage, it is important to acquire images but also to represent them in a proper format. For that, we use the following soft wares:

- ij.process, an ImageJ package for image processing,
- Jama, (Java Matrix) package for linear algebra methods implementation,
- DSJ (Direct Show Java), a Microsoft API for the Webcam management,
- Java programming language,
- SQL language for database management.

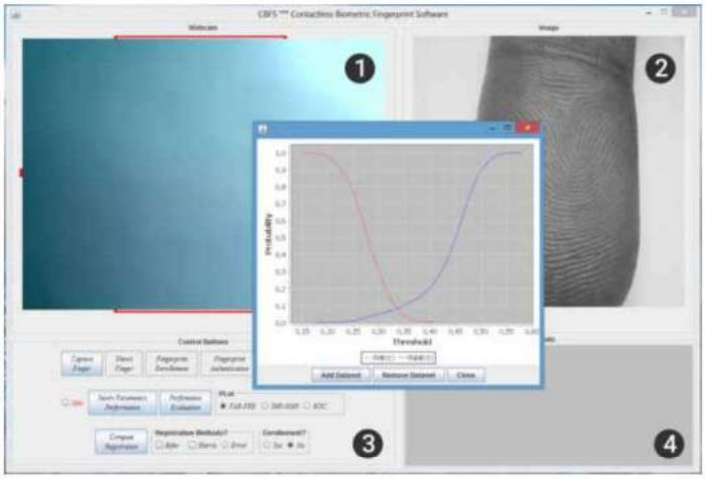
Figure 2. Contactless fingerprint acquisition system and Screenshot of CBFS



(a) Contactless fingerprint acquisition system

(b) User's interface

Figure 3. User's interface

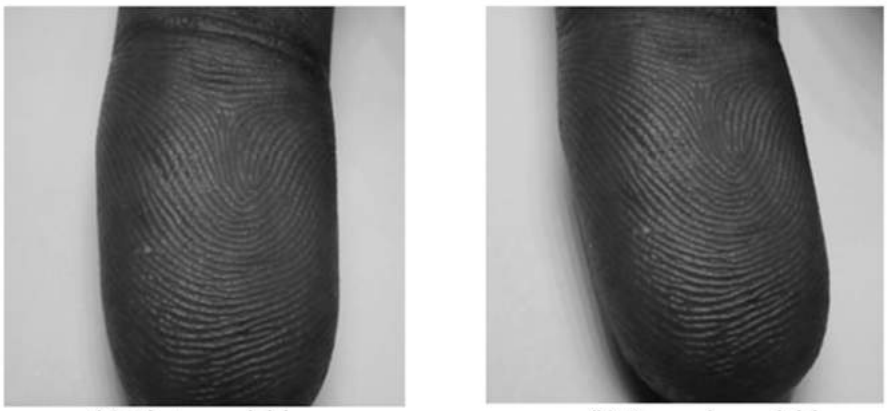


In the previous figure, the area marked "1" is used to present the finger for capture while the area marked "2" is used to show the captured image. The button "Insert Parameters Performances" is used to extract and save image signatures.

The distance between the camera and the finger, and the resolution of the output image are two important parameters in contactless image acquisition. In fact, many distances have been tested, and we find the optimum one is 8cm between the camera and the finger. In our experiment, the camera ensures a resolution of 360 dpi.

Figure 5 shows in (a) and (b) two fingerprints images acquired by a contact of sensor, while Figure 4 shows in (a) and (b) two images obtained using our camera. We notice that, a paramount advantage of contactless image acquisition is that a large image area can be captured quickly compared touch based systems.

Figure 4. Two different acquisitions of the same finger obtained by our webcam



(a) First acquisition (b) Second acquisition

Figure 5. Two different acquisitions of the same finger obtained by contact-based system (FVC2004 DB1)

(a) First acquisition (b) Second acquisition

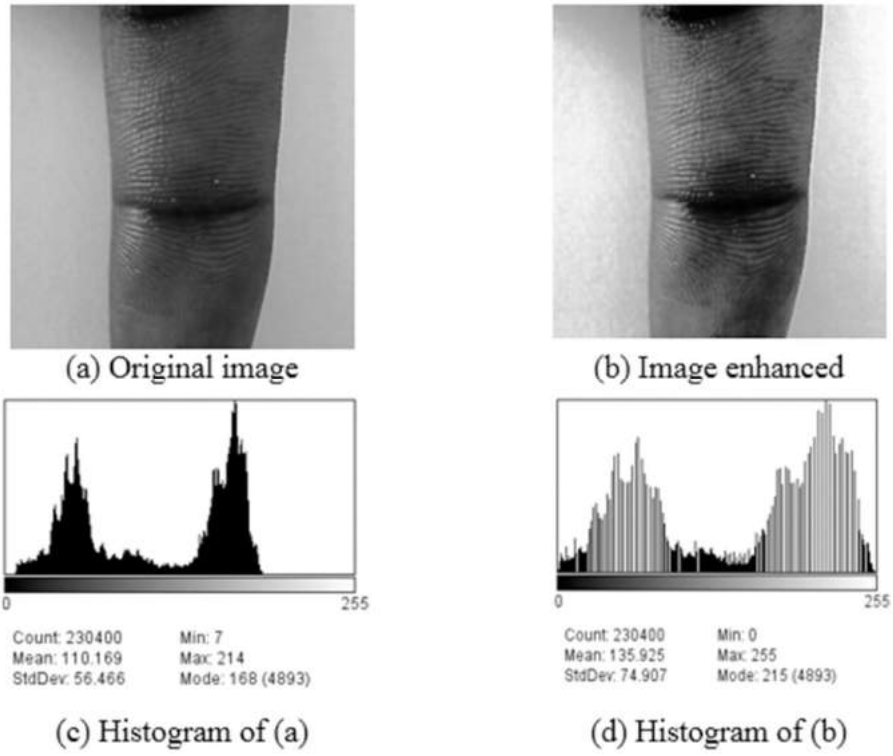
Pre-Processing Phase

Pre-processing plays a significant role in improving image contrast. We have used histogram equalization for image enhancement. Figure 6.a shows a contactless acquisition fingerprint image while Figure 6.b shows the enhanced image of Figure 6.a. Figure 6.c and 6.d show respectively the histogram of Figure 6.a and Figure 6.b. Images from webcam experiments are Red-Green-Blue color images. The image is converted to grey scale image using the CBFS.

FEATURE CHARACTERISATION

The used features are bifurcation points and ending points (Figures 8 and 9). In order to get the streaks in the image of fingerprint, a photometric adaptive threshold

Figure 6. Images and histograms



method has been developed and presented in (Djara et al., 2010). Two thresholds are defined i.e. S_s .and S_h corresponding to the mean of a square framework and the mean of a hexagonal framework. A pixel P is deleted or not by comparing its value with S_s .and S_h . Here we introduce the foreground regions extraction before streaks extraction. The extraction phase of the streaks is linked to the extraction foreground regions. For this purpose, we have applied a filter to the image in order to define its contour. Then a binary mask is subsequently applied to the image filter, which allows to have an image defining the contour of the fingerprint. This contour image is used for the extraction of foreground regions (see Figure 7).

The image from the photometric adaptive threshold is skeletonized in order to get minutiae (bifurcation points and ending points). The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3×3 window of Table 1. The crossing number (CN) is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood as presented in (Arcelli & Baja, 1984; Mehtre, 1993). We have:

$$CN = \frac{1}{2}\sum_{i=1}^{8}\left|P_i - P_{i-1}\right|, \quad P_8 = P_0. \tag{1}$$

Figure 7. Main steps of the extraction of the foreground regions

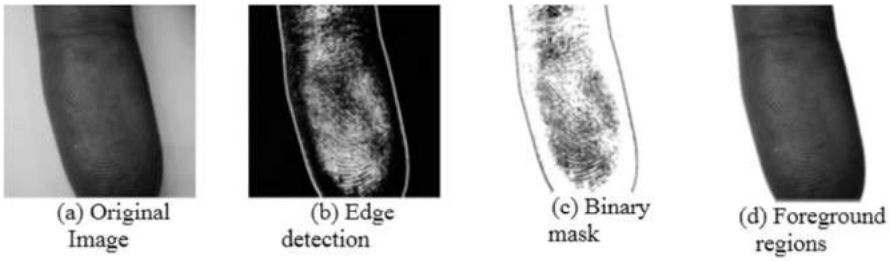


Table 1. 3×3 *operation window*

P_1	P_2	P_3
P_8	P	P_4
P_7	P_6	P_5

If $CN = 1$ then the ridge pixel is a ridge ending, while if $CN = 3$ the ridge pixel is a ridge bifurcation otherwise it is a non-minutiae point.

Ridge Bifurcation Orientation Characterization

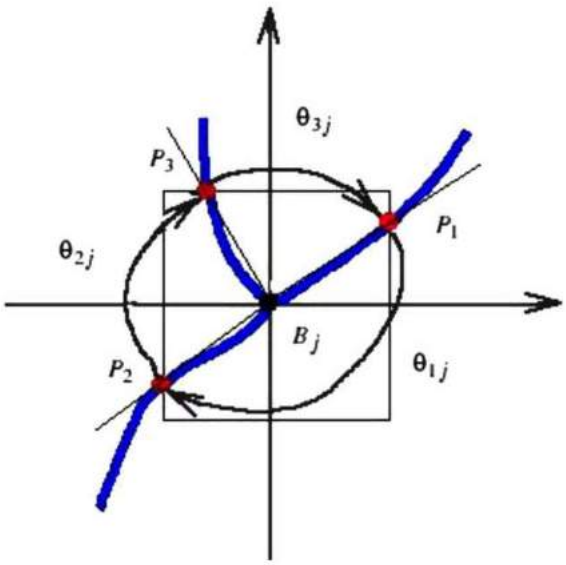
In our approach, for bifurcation points we define a window W of size S*S and of central pixel the minutiae points. We count 3 points P_1, P_2, and P_3 around the perimeter of the window as shown in Figure 8.

For a given bifurcation point B_j, we compute the orientations as being (Equations 2, 3 and 4):

$$\theta_{1j} = Arccos\left(\frac{\overrightarrow{B_jP_1}.\overrightarrow{B_jP_2}}{B_jP_1 \times B_jP_2}\right) \tag{2}$$

$$\theta_{2j} = Arccos\left(\frac{\overrightarrow{B_jP_2}.\overrightarrow{B_jP_3}}{B_jP_2 \times B_jP_3}\right) \tag{3}$$

Figure 8. Orientations of bifurcation points



$$\theta_{3j} = Arccos\left(\frac{\overrightarrow{B_jP_3}.\overrightarrow{B_jP_1}}{B_jP_3 \times B_jP_1}\right) \tag{4}$$

(.) stands for the scalar product.
(×) stands for the ordinary multiplication.

For an image with M validated bifurcation points, we build a matrix of M rows and 5 columns. Each point is represented by a row in the matrix. The columns represent the coordinates and the angles between them are the branches.

$$\begin{pmatrix} x_1 & y_1 & \theta_{11} & \theta_{21} & \theta_{31} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_M & y_M & \theta_{1M} & \theta_{2M} & \theta_{3M} \end{pmatrix} \tag{5}$$

Ridge Ending Orientation Characterization

We define two concentric windows W_1F_0 and W_2F_1 of central point the ridge ending point and for size S_1 and S_2. On the perimeter of F_1 W_1 we have a point P_1 and on the perimeter of W_2F_0 we have a point P_2P_0 as shown on figure 9. For a given ending point T_i, the orientation is defined as the angle between vectors.

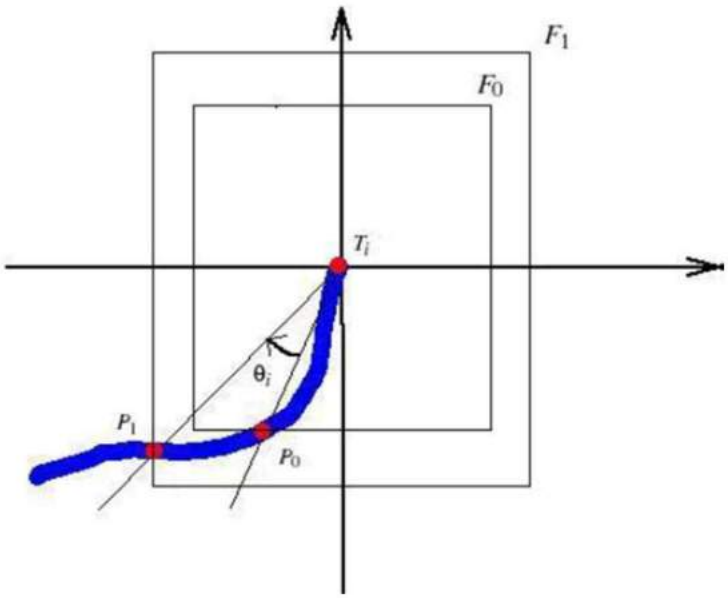
$$\theta_i = \text{Arccos}\left(\frac{\overrightarrow{T_iP_0}.\overrightarrow{T_iP_1}}{T_iP_0 \times T_iP_1}\right) \tag{6}$$

(.) stands for the scalar product.
(×) stands for the ordinary multiplication.

For an image with N validated ending points, we build a matrix of N rows and 3 columns. Each row of the matrix represents an ending points. The columns represent the coordinates of the point and the angle of the branch.

$$\begin{pmatrix} x_1 & y_1 & \theta_1 \\ \cdots & \cdots & \cdots \\ x_N & y_N & \theta_{1N} \end{pmatrix} \tag{7}$$

Figure 9. Orientation of ridge ending points



RIDGE BIFURCATION AND RIDGE ENDING SIMILARITY

In this section, we introduce the ridge bifurcation (Rb) and the ridge ending points (Re) similarity (Rb-Re Similarity). Let $I_t\left(Rb\right)$ and $I_{t+d}\left(Rb\right)$ be the template and query fingerprint Rb sets respectively. Let $I_t\left(Re\right)$ and $I_{t+d}\left(Re\right)$ be the template and query fingerprint Re sets respectively. We have:

$$I_t\left(b\right)=\left\{b_1,b_2,\ldots,b_M\right\}b_j=\left(\mathrm{x_j},\mathrm{y_j},\theta_{1j},\theta_{2j},\theta_{3j}\right);\quad \mathrm{j}\in\left[1\ldots\mathrm{M}\right] \tag{8}$$

$$I_{t+d}\left(b\right)=\left\{b'_1,b'_2,\ldots,b'_{M'}\right\}b'_P=\left(\mathrm{x'_p},\mathrm{y'_p},\theta'_{1p},\theta'_{2p},\theta'_{3p}\right);\quad \mathrm{p}\in\left[1\ldots\mathrm{M'}\right] \tag{9}$$

$$I_t\left(t\right)=\left\{t_1,t_2,\ldots,t_N\right\}t_i=\left(\mathrm{x_i},\mathrm{y_i},\theta_i\right);\quad \mathrm{i}\in\left[1\ldots\mathrm{N}\right] \tag{10}$$

$$I_{t+d}\left(t\right)=\left\{t'_1,t'_2,\ldots,t'_{N'}\right\}t'_q=\left(\mathrm{x}'_q,\mathrm{y}'_q,\theta'_q\right);\quad \mathrm{q}\in\left[1\ldots\mathrm{N}'\right] \tag{11}$$

where b_j and b'_p represent respectively the j^{th} and the p^{th} row of matrix of the Rb. t_i and t'_q represent respectively the i^{th} and q^{th} row of matrix of the Re. It is assumed, that there is correspondence between b_j and b'_q if the Euclidean distance (ed) between them is smaller than a given tolerance d_0 and orientation differences (od) of their respective angles are smaller than angular tolerances $\theta_0,\alpha_0,\beta_0$:

$$ed\left(b_j,b'_p\right)=\sqrt{\left(x_j-x'_p\right)^2+\left(y_j-y'_p\right)^2}\le d_0\ \ and \tag{12}$$

$$\begin{cases} od\left(b_j,b'_p\right)_1=min\left(\left|\theta_{1j}-\theta'_{1j}\right|,360-\left|\theta_{1j}-\theta'_{1j}\right|\right)\le\theta_0 \\ and \\ \begin{cases} od\left(b_j,b'_p\right)_2=min\left(\left|\theta_{2j}-\theta'_{2j}\right|,360-\left|\theta_{2j}-\theta'_{2j}\right|\right)\le\alpha_0 \\ or \\ od\left(b_j,b'_p\right)_3=min\left(\left|\theta_{3j}-\theta'_{3j}\right|,360-\left|\theta_{3j}-\theta'_{3j}\right|\right)\le\beta_0 \end{cases} \end{cases} \tag{13}$$

By the same way, we assume that there is a correspondence between t_i and t'_q if the euclidean distance (ed) between them is smaller than a given tolerance d_0 and the orientation difference (od) between them is smaller than an angular tolerance θ_0.

$$ed\left(t_i,t'_q\right)=\sqrt{\left(x_i-x'_q\right)^2+\left(y_i-y'_q\right)^2}\le d_0\ \ and \tag{14}$$

$$od\left(t_i,t'_q\right)=min\left(\left|\theta_i-\theta'_q\right|,360-\left|\theta_i-\theta'_q\right|\right)\le\theta_0 \tag{15}$$

MINUTIAE MATCHING

The nature of the deformation between our images is a rigid transformation expressed by:

$$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{pmatrix} u_0 & u_1 & u_2 \\ v_0 & v_1 & v_2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} \tag{16}$$

with

$$\begin{aligned} u_0 &= \cos(\theta) \; u_1 = -\sin(\theta) \; u_2 = (1-\cos(\theta))x_0 + y_0 \sin(\theta) + t_x \cos(\theta) - t_y \sin(\theta) \\ v_0 &= \sin(\theta) \quad v_1 = \cos(\theta) \quad v_2 = (1-\cos(\theta))x_0 + y_0 \sin(\theta) + t_x \sin(\theta) + t_y \cos(\theta) \end{aligned} \tag{17}$$

where $M_0 \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$ is the center of rotation, θ the angle of rotation, $\begin{pmatrix} t_x \\ t_y \end{pmatrix}$ the coordinates of the translation vector and $M' \begin{pmatrix} x' \\ y' \end{pmatrix}$, the transform of $M \begin{pmatrix} x \\ y \end{pmatrix}$.

In the research phase of the best deformation, the correspondence between the sets of control points is obtained by calculating the descriptor vector of Zernike moments on a window of size $L \times L$ centered at each point, taking into account ridges bifurcations. Comparison of correlation coefficients between the descriptors vectors of Zernike moments helps define the corresponding points. The estimation of parameters of the existing deformation between the images is performed using RANSAC algorithm (Random SAmple Consensus) that suppresses wrong matches. The correspondence between these two sets of control points is obtained by following these steps:

- Subdivide each image into thumbnail size $L \times L$ centered on each point B_i.
- For each thumbnail centered on this point B_i, construct the descriptor vector of Zernike moments M_z as follows:

$$M_z = \left(\left| z_{11} \right|, \ldots, \left| z_{pq} \right|, \ldots, \left| z_{55} \right| \right) \tag{18}$$

where $\left|z_{pq}\right|$ is the module of Zernike moments. We have used as the highest order of moments 5 after several experimental trials. Although the higher order moments are the fine details of the image, they are more sensitive to noise than lower order moments. The Zernike moment of order p with repetition q for a continuous image function $f\left(x,y\right)$, that vanishes outside the unit disk is:

$$Z_{pq} = \frac{p+1}{\pi} \iint\limits_{x^2+y^2\leq 1} V_{pq}^{*}\left(\rho,\theta\right) f\left(x,y\right) dxdy \tag{19}$$

If F is the digital image of f, the above equation becomes:

$$Z_{pq} = \frac{p+1}{\pi} \sum_{x=1}^{N}\sum_{y=1}^{N} V_{pq}^{*}\left(\rho,\theta\right) F\left(x,y\right) \tag{20}$$

with

$$V_{pq}\left(\rho,\theta\right) = R_{pq}\left(\rho\right) e^{iq\theta} \tag{21}$$

where R_{pq} is the Zernike radial polynomials of order p with repetition q in $\left(\rho,\theta\right)$ polar coordinates given by:

$$R_{pq}\left(\rho\right) = \sum_{s=0}^{\frac{p-|q|}{2}} \frac{\left(-1\right)^{s}\left(p-s\right)!}{s!\left(\frac{p+|q|}{2}-s\right)!\left(\frac{p-|q|}{2}-s\right)!} \rho^{p-2s} \tag{22}$$

In the above equation p is a non-negative integer, ($p \geq 0$), and q positive and negative integers subject to the constraints:

$$\begin{cases} p-|q| \ \ is \ \ even \\ |q| \leq \ p \end{cases} \tag{23}$$

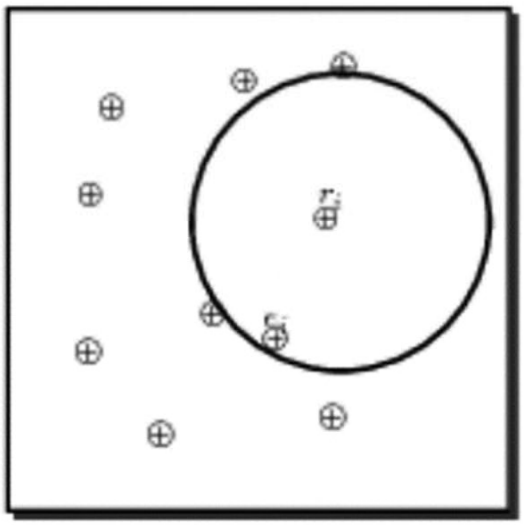
where V_{pq}^{*} denote complex conjugate of V_{pq}, $\rho = \sqrt{x^2+y^2} \ \leq 1$ and $\theta = tan^{-1}\left(\frac{y}{x}\right)$.

- For any point r_i of the reference image, we suppose that its corresponding e_i of input image is from a set of points located within a certain radius R_0 around r_i. The radius R_0 limits the search for corresponding and therefore, dramatically reduces the number of comparisons to achieve in order to find out the corresponding points.
- The matching process is performed by calculating the correlation coefficients between the two descriptor vectors. The corresponding points are those which give the maximum value of correlation coefficients.

The correlation coefficient between two vectors of the features $X\left(x_1,\ldots,x_n\right)$ and $Y\left(y_1,\ldots,y_n\right)$ is given by the following formula:

$$C=\frac{\sum_{i=1}^{n}\left(x_i-\bar{x}\right)\left(y_i-\bar{y}\right)}{\sqrt{\sum_{i=1}^{n}\left(x_i-\bar{x}\right)^2}\times\sqrt{\sum_{i=1}^{n}\left(y_i-\bar{y}\right)^2}} \tag{24}$$

Figure 10. Determining the corresponding e_i (of input image) of a point r_i (of the reference image)



where $\bar{x}$ and $\bar{y}$ are averages of the two vectors X and Y respectively. If C is 0, the two vectors are not correlated. The two vectors are better correlated when C is far from 0 (near -1 or 1).

Once the sets of points $I_t(.)$ and $I_{t+d}(.)$ are aligned by applying the model of deformation given by Equation 16, the algorithm "Rb-Re Similarity" starts. The formal algorithm is the following (see figure 11).

Figure 11. Rb-Re Similarity

Let n_0 be the maximum number of matching minutiae computed after performing all fingerprint rigid transformation.
Let n_1 be the maximum number of matching Rb computed after performing all fingerprint rigid transformation.
Let n_2 be the maximum number of matching Re computed after performing all fingerprint rigid transformation.
for $i \leftarrow 1, M$ **do**
  for $j \leftarrow 1, M'$ **do**
    if RbSimilarity(b_i, b'_j) **then**
      $n_1 \leftarrow n_1 + 1$.
      break.
    end if
  end for
end for
for $i \leftarrow 1, N$ **do**
  for $j \leftarrow 1, N'$ **do**
    if ReSimilarity(t_i, t'_j) **then**
      $n_2 \leftarrow n_2 + 1$.
      break.
    end if
  end for
end for
$n_0 \leftarrow n_1 + n_2$.
function RbSimilarity(a, b)
  if $ed(a,b) \le d_0$ && ($od(a,b)_1 \le \theta_0$ && ($od(a,b)_2 \le \alpha_0 \,\|\, od(a,b)_3 \le \beta_0$)) **then**
    return ***true***
  else
    return ***false***
  end if
end function
function ReSimilarity(a, b)
  if $ed(a,b) \le d_0$ && $od(a,b) \le \theta_0$ **then**
    return ***true***
  else
    return ***false***
  end if
end function

The purpose of a match algorithm is to evaluate the similarity of two fingerprints, and to judge whether they belong to the same finger or not. In our method, the similarity value is computed using the formula presented by Galy (2005):

$$MS = \frac{N}{\max\left(N_{I_t}, N_{I_{t+d}}\right)} \tag{25}$$

where N_{I_t} and $N_{I_{t+d}}$ are the template and query fingerprint minutiae sets respectively, and N is the amount of matching minutiae pairs.

We created a database (available in http://refod.net/images/Fingerprint/DB2.zip) containing 420 prints with 28 different sets of fingers, each with 15 acquisitions.

Let F_{ij} be the j^{th} fingerprint sample of the i^{th} finger and T_{ij} the corresponding template $(1 \le i \le n; 1 \le j \le m)$. The template T_{ij} are computed from the corresponding F_{ij} and stored on a disk by our platform

For matching, we perform the following operations:

1. **Genuine Matching (GM):** Each fingerprint template T_{ij} is matched against the fingerprint images F_{ik} $(k \neq j)$ and the corresponding Genuine Matching Score gms_{ijk} are stored.
2. **Impostor Matching (IM):** Each fingerprint template T_{k1} is matched against the fingerprint images from different fingers F_{ij} (i > k) and the corresponding Impostor Matching Score ims_{ik} are stored.

The number of matching is defined in each case:

Case 1: $NGRA = \left\|\left\{gms_{ijk}, i \in [1 \ldots n], 1 \le j \neq k \le m\right\}\right\| = n * m * (m-1)$. In our case NGRA = 5880. NGRA is the Number of Genuine Recognition Attempts.

Case 2:

$NIRA = \left\|\left\{ims_{ik}, i \in [1 \ldots n], 1 \le j \neq k \le m\right\}\right\| = m\left[(n-1) + (n-2) + \ldots + 1\right]$.

In our case NIRA = 5670. NIRA is the Number of Imposter Recognition Attempts.

The GM distribution and the IM distribution are computed and graphically reported to show how the algorithm differentiates the classes. The FMR (False

Match Rate) and FNMR(False Non-Match Rate) curves are computed from the above distributions for the threshold t ranking from 0 to 1.

The pairs (FMR(t), FNMR(t)) are plotted for the same value of t to obtained a ROC (Receiver Operating Characteristics) curve.

FMR(t) and FNMR(t) are defined by:

$$FMR(t) = \frac{card\left\{ims_{ik} \;/\; ims_{ik} \geq t\right\}}{NIRA} \tag{26}$$

$$FNMR(t) = \frac{card\left\{gms_{ik} \;/\; gms_{ijk} < t\right\}}{NGRA} \tag{27}$$

card denote the cardinality of a given set, FMR(t) denotes the percentage of $ims_{ik} \geq t$ and FNMR(t) denotes the percentage of $gms_{ijk} < t$.

EXPERIMENTAL RESULTS

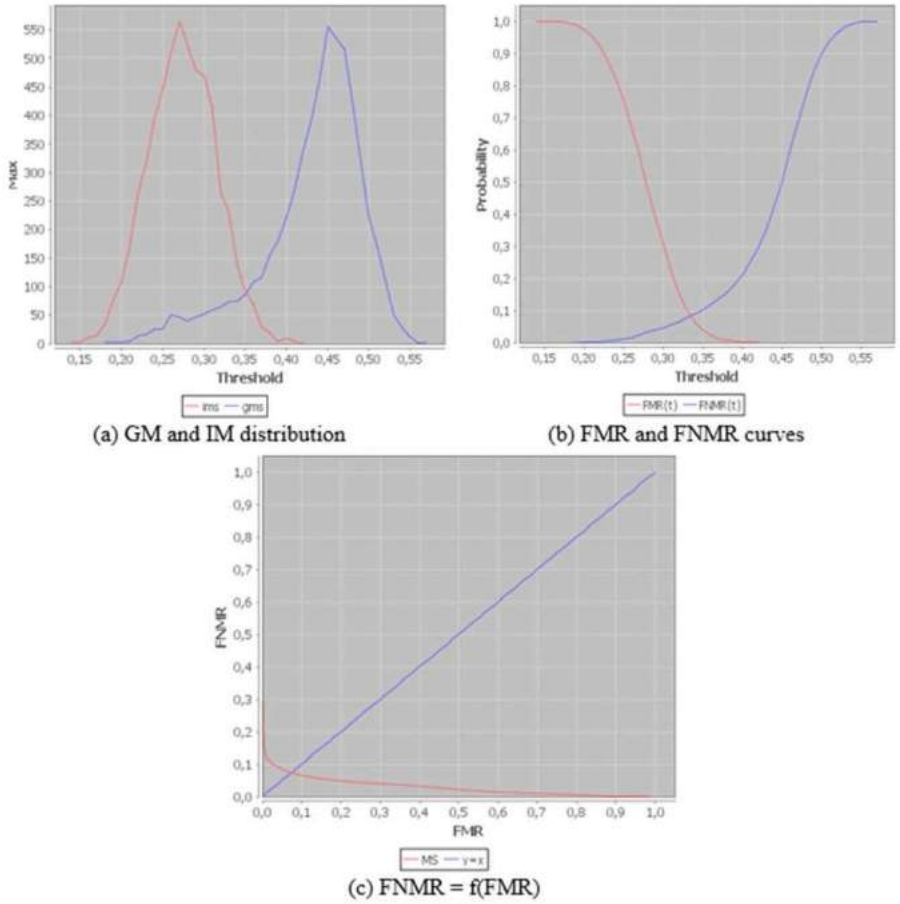
Figure 12, shows in (a) GM and IM distributions. In (b) and (c) FMR-FNMR curves and ROC are respectively represented. We evaluate the algorithm performance by using Equal Error Rate (EER) where FMR = FNMR. We notice from figure 12-(b) that FMR and FNMR values are respectively 7.64% and 6.46% at a threshold (**th**) value of 0.33.

From the database, we achieved an EER to the order of 7.05%. The matching time is approximately 0.6s. The performance of our algorithm is acceptable. The results can be improved ensuring that the database does not contain such poor quality fingerprint images.

FUTURE RESEARCH DIRECTIONS

In a future work, the performance of our algorithms can be improved by taking into account the 3D fingerprint identification presented in (Ajay & Kwong, 2015; Hong Kong Polytechnic, 2013; Wang et al., 2010). We can also enhance our sensor by using a camera with flash instead of having a separate light device. The same sensor equipped with flash can be used to acquire the image of the face in the perspective of a multimodal system. This would result in a substantial saving for

Figure 12. GM-IM, FMR-FNMR curves and ROC



(a) GM and IM distribution

(b) FMR and FNMR curves

(c) FNMR = f(FMR)

the operational system to be developed. The biometric verification system proposed in this paper is based on the only fingerprint modality; it is a monomodal system. However, monomodal biometric systems have three main limitations: a limitation in terms of performance (physical characteristics variation), a limitation in terms of universality of use (absence of certain biometrics) and a limitation in terms of fraud detection (identity theft) (AlMahafzah et al., 2012 ; Allano, 2009 ; Ross, 2007). These limitations can be reduced or even eliminated by the joint use of several biometric systems which then form a multimodal biometric system. The contactless fingerprint

can therefore be combined with the face in order to improve the performance, robustness and universality of the system to be developed. Since face recognition is by nature contactless, we will develop a fully contactless multimodal biometric system. Particular emphasis will be placed on the method of the scores fusion for the two modalities to be used.It will be the fusion of scores in a sequential approach adapted to the user. In all cases described above, the extracted features will be stored in a database for future comparisons. It will then raise the problem of protecting these stored templates against spoofing actions. One of the vulnerability levels of biometric verification systems is the ability to modify the template. To ensure the protection of the templates, the most used approach is the rigid transformation which performs a translation and a rotation (Moudjahdi et al., 2012) without modifying feature characteristics. This rigid transformation approach that uses the Hausdroff distance (Ali and Prakash, 2015) poses the problem of the security of the person to be authenticated. Indeed, in this approach, the parameters of transformation are provided by man. As a result, there is a risk that these parameters will be forgotten in the case of a memory disorder such as Alzheimer's. On the other hand, the individual who wants to authenticate can be attacked in order to remove the template protection settings. To eliminate these risks, we propose an innovative technique which consists in having the parameters of protection of the template provided by the computer. The implementation of this technique consists in first determining the coordinates of the center of mass of the registered biometric image. In a second step, the area of interest of size $N \times M$ having the characteristic points of the image is defined. The third and fourth steps will be respectively the computation of the Zernike Moment and the various associated modules. In the fifth and last step, a random choice will be made among the modules calculated to obtain the distance do.

CONCLUSION

In this paper, we investigated a fingerprint matching algorithm with only minutiae information as an approach for a supervised contactless biometric system. In this new context, our experiments show that fingerprint images can be well matched using the minutiae matching method. The performance of the algorithm is evaluated through a created database using the CBFS. As shown, we have led 5880 comparisons intra-class (Number of Genuine Recognition Attempts) and 5670 comparisons inter-class (Number of Imposter Recognition Attempts). The illustration of the results available in the contact context shows that the performance of our algorithms is acceptable. The results are encouraging with an Equal Error Rate around 7.05%.

Compared to the contact-based fingerprint verification method, the contactless method offers greater ease of use for users. The sensor used for acquiring the contactless image is very affordable. We will implement our algorithm for secure digital borrows contactless and define other original algorithm digitals fingerprint security without contact using the sphere of Pointcarré.

REFERENCES

Ali, S. S., & Prakash, S. (2015). Enhanced fingerprint Shell. *Signal Processing and Integrated Networks (SPIN), 2015 2nd International Conference on*. doi:10.1109/SPIN.2015.7095438

Allano, L. (2009). *La Biométrie multimodale: stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles* (Thèse de doctorat). Institut National des Télécommunications Paris.

AlMahafzah, H., & AlRwashdeh, M. Z. (2012). A survey of multibiometric systems. *International Journal of Computers and Applications*, *43*(15).

Arcelli, C., & Di Baja, G. S. (1985). A width-independent fast thinning algorithm. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *4*(7), 463–474. doi:10.1109/TPAMI.1985.4767685 PMID:21869284

Bhowmik, U. K., Ashrafi, A., & Adhami, R. R. (2009). A Fingerprint Verification Algorithm Using the Smallest Minimum Sum of Closest Euclidean Distance. In *Electrical, Communications, and Computers, 2009.CONIELECOMP 2009. International Conference on* (pp. 90-95). IEEE. doi:10.1109/CONIELECOMP.2009.57

Djara, T., Assogba, M. K., & Nait-Ali, A. (2010). Caractérisation spatiale des empreintes de l'index en analyse biométrique. *Actes du CARI 2010*, 501-508.

Galbally, J., Fierrez, J., Ortega-Garcia, J., & Cappelli, R. (2014). Fingerprint Anti-spoofing in Biometric Systems. In S. Marcel, M. Nixon, & S. Li (Eds.), *Handbook of Biometric Anti-Spoofing. Advances in Computer Vision and Pattern Recognition*. London: Springer. doi:10.1007/978-1-4471-6524-8_3

Galy, N. (2005). *Etude d'un système complet de reconnaissance d'empreintes digitales pour un capteur microsystème à balayage* (Thesis). Institut National Polytechnique de Grenoble - INPG.

He, Y., Tian, J., Luo, X., & Zhang, T. (2002). Image enhancement and minutiae matching in fingerprint verification. *Pattern Recognition Letters*, 1349–1360.

Hiew, B., Teoh, A., & Pang, Y. (2007). Touch-less fingerprint recognition system. *ICB, LNCS*, *3832*, 24–29.

Ito, K., & Morita, A. (2009). A fingerprint recognition algorithm using phase-based image matching for low quality fingerprints. IEEE.

Jain, A., Lin Hong, , & Bolle, R. (1997). On-line fingerprint verification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *19*(4), 302–314. doi:10.1109/34.587996

Jain, A., Prabhakar, S., Hong, L., & Pankanti, S. (2000). Filterbank-based fingerprint matching. *IEEE Transactions on Image Processing*, *9*(5), 846–859. doi:10.1109/83.841531 PMID:18255456

Khalila, M. S., Mohamada, D., Khanb, M. K., & Al-Nuzailia, Q. (2010). Fingerprint verification using statistical descriptors. *Digital Signal Processing*, *20*(4), 1264–1273. doi:10.1016/j.dsp.2009.12.002

Kumar, A., & Kwong, C. (2015, March). Towards contactless, low-cost, and accurate 3D fingerprint identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *37*(3), 681–696. doi:10.1109/TPAMI.2014.2339818 PMID:26353269

Kumar, R., Chandra, P., & Hanmandlu, M. (2012). Statistical descriptors for fingerprint matching. *International Journal of Computers and Applications*, *59*(16), 24–27. doi:10.5120/9633-4361

Labati, R. D., Genovese, A., & Piuri, V. (2013). Fabio Scotti Contactless fingerprint recognition: A neural approach for perspective and rotation effects reduction. *Computational Intelligence in Biometrics and Identity Management (CIBIM), 2013 IEEE Workshop on*.

Liu, X., Pedersen, M., Charrier, C., Cheikh, F. A., & Bours, P. (2016). *An improved 3-step contactless fingerprint image enhancement approach for minutia detecting*. IEEE.

Maltoni, D., Maio, D., Jai, A. K., & Prabhakar, A. (2003). *Handbook of fingerprint recognition* (2nd ed.). Springer.

Marasco, E., & Ross, A. (2015). A Survey on anti-spoofing schemes for fingerprint recognition systems. *ACM Computing Surveys*, *47*(2).

Matsumoto, T., Matsumoto, H., Yamada, K., & Ho-shino, S. (2002). Impact of artificial “gummy” fingers on fingerprint systems. SPIE, 4677.

Medina-pérez, M. A., & Gracia-Barroto, M. (2012). al, Improving fingerprint verification using minutiae triplets. *Pattern Recognition*, 3418–3437.

Mehtre, B. M. (1993). Fingerprint image analysis for automatic identification. *Machine Vision and Applications*, *6*(2), 124–139. doi:10.1007/BF01211936

Mil'shtein, S., Palma, J., Liessner, C., Baier, M., Pillai, A., & Shendye, A. (2008). *Line scanner for biometric applications*. Traitement du Signal.

Milshtein, S., Pillai, A., Kunnil, V. O., Baier, M., & Bustos, P. (2011). Applications of Contactless Fingerprinting, Recent Application in Biometric. In Tech.

Mojtaba, M. W. B. (2010, January). Liveness and Spoofing in Fingerprint Identification Issues and Challenges. Academic Press.

Moujahdi, C., Ghouzali, S., Mikram, M., Rziza, M., & Bebis, G. (2012). Spiral cube for biometric template protection. In *Imageand Signal Processing* (Vol. 7340, pp. 235–244). Springer. doi:10.1007/978-3-642-31254-0_27

Pankanti, S., Prabhakar, S., & Jain, A. (2002). On the individuality of fingerprints. *IEEE Trans. Pattern Anal.*, *24*(8), 1010–1025. doi:10.1109/TPAMI.2002.1023799

Parziale, G., Santana, E.-D., & Hauke, R. (2006). The surround imager: A multi-camera touchless device to acquire 3d rolled-equivalent fingerprints. *ICB, LNCS*, *3832*, 244–250.

Pillai, A., & Mil'shtein, S. (2012). Can Contactless fingerprint be compared to existing database? *Homeland Security (HST), 2012 IEEE Conference on Technologies for*.

Qader, H. A. (2006). *Fingerprint recognition using zernike moments*. Internationnal Arab Journal of Information Technology.

Ross, A. (2007). An introduction to multibiometrics. *Proc. of the 15th European Signal Processing Conference (EUSIPCO)*.

Sha, L. F., Zhao, F., & Tang, X. O. (2003). Improved fingercode for filterbank-based fingerprint matching. *International Conference on Image Processing, 2*, 895-898.

The Hong Kong Polytechnic University 3D Fingerprint Images Database. (2013). Retrieved from http://www.comp.polyu.edu.hk/~csajaykr/3Dfingerprint.htm

Tico & Kuosmanen. (2003). Fingerprint matching using an orientation-based minutia descriptor. *IEEE Trans. PAMI., 25*(8), 1009-1014.

Virk & Maini. (2012). Fingerprint image enhancement and minutiae matching in fingerprint verification. *Journal of Computing Technologies*.

Wang, Y., Lau, D. L., & Hassebrook, L. G. (2010). Fit-sphere unwrapping and performance analysis of 3D fingerprints. *Applied Optics*, *49*(4), 592–600. doi:10.1364/AO.49.000592 PMID:20119006

Yin, X., Hu, J., & Xu, J. (2016). Contactless fingerprint enhancement via intrinsic image decomposition and guided image filtering. *Industrial Electronics and Applications (ICIEA), 2016 IEEE 11th Conference on*.