International Journal of Information Security and Privacy
Volume 16 • Issue 1

Cylindrical Curve for Contactless Fingerprint Template Securisation

Boris Jerson Zannou, University of Abomey-Calavi, Benin*
Tahirou Djara, University of Abomey-Calavi, Benin
Antoine Vianou, University of Abomey-Calavi, Benin

ABSTRACT

A large quantity of biometric models has rapidly proliferated in biometric applications. Due to the fact that biometric systems expose users to enormous risks that endanger , the authors improved an existing technics technique and adapted it to the contactless system. The proposed model, in this article, propose a very secure fingerprint model protection technique in which a cylindrical curve is generated as a user secure model for a contactless fingerprint. During the construction of our model, the authors use three invariants intra-personals characteristics, namely the set of distances between the detailed points and the center of mass, the orientation information of the detailed points and the number of endings between the minutiae points and the singular point. The results of the experimental analysis performed on the FVC databases (2000, 2002 and 2004) and the authors' own database show a highly encouraging performance and present the viability of the proposed technique.

KEYWORDS

Biometry, diversity, fingerprint, revocability, security, thoroughness

1. INTRODUCTION

Biometrics identifies human characteristics and traits. The fingerprint remains the most used characteristic during human authentication because it works well and is unique. The minutiae are the most adopted representation. Although minutiae are the most adopted representation, it is exposed to several dangers that several researches have proven. The architecture of the figure 2 gives several types of attacks. The literature reviews vulnerabilities and attacks against a biometric system are described in several ways and based on the opinion of several authors in (Ratha et al, 2001; Ratha et al, 2003;Cukik et al, 2005; Adler et al, 2005; Jain et al, 2006; Roberts et al, 2008; Jain et al, 2008) . Eight levels of attacks have been identified, namely:

- Presentation attacks: fingerprints are presented at the entrances after having reproduced them;
- Hacking and use of fingerprint data after bypassing the sensor;
- Usurped features are substituted for the original;
- Tampering with the correspondence module to use false functionality;
- Data replay attacks;
- Replacement of the characteristics module by a trojan horse;
- Spying on the channel between the feature extraction module and the classifier by an opponent in order to record the original model and replay it.

DOI: 10.4018/IJISP.303664 *Corresponding Author

Figure 1. Secured contactless cylindrical fingerprint template generation

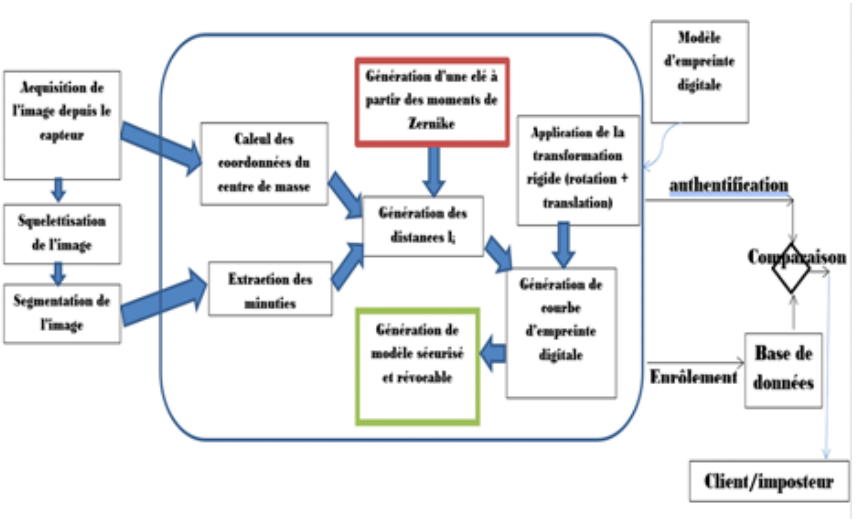
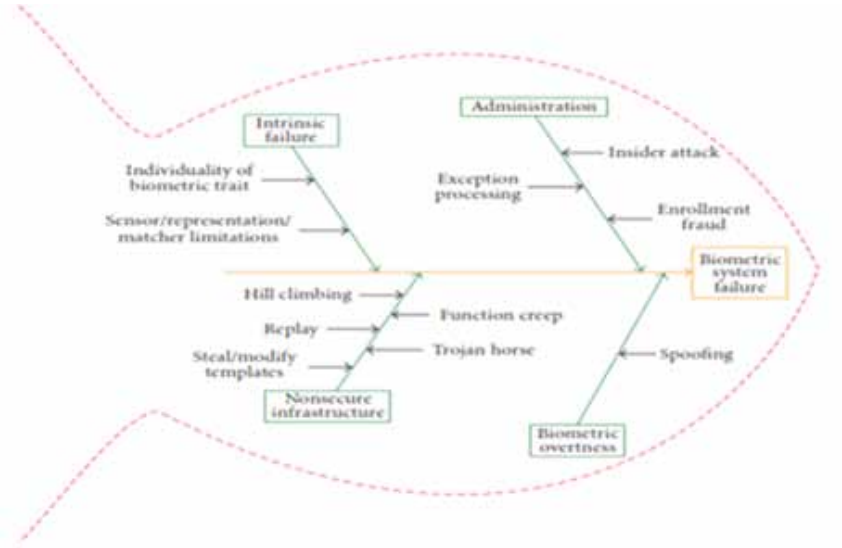


Figure 2. Fish bone model to categorize vulnerabilities of fingerprints template

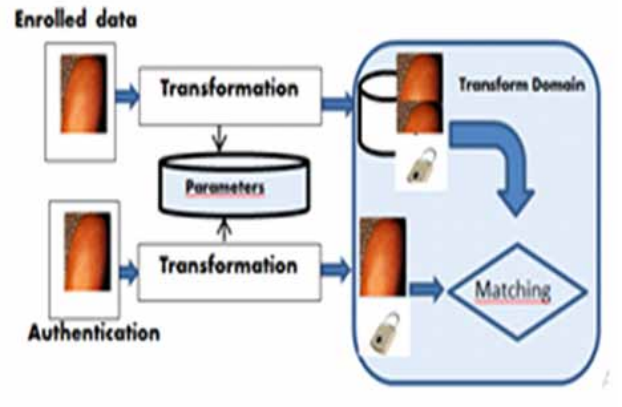


Each attack is dependent on a set of resources and constraints which makes it possible to classify it according to its acuity or its severity. The attack on the fingerprint templates stored in the comparison module, should be considered a major threat to authentication systems and one of the most formidable attacks against fingerprint-based authentication systems digital.

Due to the threats identified above, solutions to protect biometric models have emerged. The literature subdivides them into two categories: the transformation of characteristics (revocable biometrics) and biometric cryptosystems (biometric encryption). The cryptosystem makes it possible to protect the characteristics directly using the biometric function. Furthermore, revocable biometrics (Ratha et al, 2008) is specifically indicated for the protection of biometric models. it takes into account irreversible transformations that can modify the templates so that the security and confidentiality of the models can

be operated. When a revocable model is compromised, another revocable model can be regenerated from the same characteristics of the fingerprint. Biometric schemes vary according to the different modalities. Furthermore, the generical functioning of a revocable global biometric system is close to the conventional system where the global architecture includes a sensor, a characteristics extractor and a comparison module in which the comparison is made and a decision is made in the transformation field rather than in the field of characteristics, Passwords or specific items such as random numbers. We will use as transformation function a function going in the many to one direction (non-invertible transformation) or a mixing mechanism (salting) to modify biometric models (Jain et al, 2008). A schematic diagram representing a generally revocable biometric system is schematized as follows:

Figure 3. General cancelable biometric systems diagram block



However it is very difficult to size a protection model taking into account the following creeks (Nandakumar et al, 2008):

- **Non-invertibility or irreversibility**: Make it impossible to reconstruct the original image from an instance or several instances of protected models, taking into account or not the auxiliary data. This property makes it possible to avoid confidentiality attacks such as inversion attacks and attacks via the multiplicity of records (ARM);
- **Revocability or renewability**: If the old model is compromised, a new model instance can be generated by revoking the old one;
- **Non-linkability**: To raise the difficulties of to be able to differentiate two or more instances of the protected models derived from the same biometric trait. This property prevents cross-correspondence between different applications, thus protecting user privacy;
- **Preservation of performance**: The accuracy performance of protected models must be preserved in comparison with counterparts before transformation.

The protection of biometric models has emerged in order to lessen the impact of the unauthorized use of biometric data. Thus in (Cappelli et al, 2007), Cappelli et al have proved the possibility of reconstruction of the fingerprint image based on the original model or by recovering the characteristics. Thus, public works and civil engineering hold the attention of researchers in recent years as an emerging concept of securing biometric data and a bulwark against circumvention of security and confidentiality when the database of biometric models is violated. Challenges in deployment remain to

the BTP(Biometric Protection Template) schemes in real biometric authentication systems. Although BTP often introduces increased computational complexity into the model generation process and requires high execution time inside the mechanism generation models and therefore need a longer execution time to enroll and authenticate fingerprints. Due to the confidentiality of users of a biometric system, the crypto-system is a gain since it requires no storage. This article proposes a hybrid building and public works scheme combining both revocable biometrics (and specifically revocable fingerprint) and biometric cryptosystems to provide a security, confidentiality and performance oriented solution for attacks on biometric model databases.

2. LITTERATURE REVIEW

Generally classified as revocable biometrics (Ratha et al, 2001) and crypto-biometric systems (Cavoukian et al, 1996), the protection of biometric templates is booming due to the increase and improvement of impostor techniques. By applying a distortion and a renewed transformation to the characteristics of original biometric data, revocable biometrics makes it possible to output a template that is computer-impossible to retrieve. A digital key is issued that is linked to the user's biometric data. The first sophisticated fingerprint-based key linking technique was first exhibited by Soutar et al. and extended by mytec1 (Soutar et al, 1996) and then this version evolved to become Mytec2 (C Soutar et al, 1998), (C Soutar et al, 1998), (A Juel et al, 2007). Their solutions are based on the correlation that proved to be insoluble in the sense of accuracy and security. Juels and Wattenberg (A. Juels et al, 1999) The authors in Wang et al,2012), on the other hand, were concerned about protecting the original fingerprint data. They suggested a framework in which a point of dense mapping several to one is used. Others in (Halevi et al, 2013) suggest a device to identify a customer according to his position using radio frequency identification (RFID) systems. Some authors in (Sandhya et al, 2015) have suggested the approach of the revocable fingerprint model based on the closest neighborhood k architecture. An approach based on the first central points identified in order to detect the area of interest (ROI) has been proposed by some authors in (Derman et al, 2010). The characteristic elements within the ROI are only used in this approach. Some other authors have developed fundamental techniques by building fixed-length structures from minutiae points. Some customer specimens are needed in this method for the implementation of the system. Authors in (S Wang et al, 2016) have suggested a technique without alignment in order to produce revocable models. It is a non-reversible method which is used to ensure the safety of the bit-prick frequency specimens used. A scheme originally based on the Delaunay triangles for the production of revocable client patterns was suggested in (S Wang et al, 2016). A biometric identification scheme is suggested. This scheme is based on the geometric statistical descriptor. Also to protect the fingerprint characteristics of a client, the authors in (Sandhva et al, 2017) suggested a framework based on the merging of structures. A hybrid fingerprint mating that consists of a single step of local minutiae mating followed by a consolidation step has been experimented by researchers in (H. Tran et al, 2017). In (Wang et al, 2017) researchers used powerful non- inverting transmutation on the binary presentation of a fingerprint to generate a revocable client model. Some in (X. SI et al, 2017) have introduced a scheme based on dense storage of fingerprints to reduce intra-subject variation. Others in (S. Wang et al, 2017)) have proposed a foolproof hardware implementation allowing the enhancement of the fingerprint image with the anisotropic Gaussian. Some authors have proposed a new scheme to produce revocable client models based on local minutia structures using zoned minutia pairs. A protection scheme called Fingerprint Shell has been introduced by authors in (Moujahdi et al, 2014). This scheme is based on the construction of spiral curves from fingerprints. Using the spiral curves proposed in (Moujahdi et al, 2014), some other authors have developed an extension of (Ali S. et al, 2015) for better results in (Ali S. et al, 2017), (S. Ali et al, 2018). Others in (Zannou et al, 2019) have applied this method to a contactless system and increased security by using zernike moments as used by (Djara et al, 2009).

This contactless system prevents some security problems in the office and protects against the risk of epidemics in contact applications. The secure version of was proposed in (Zannou et al, 2019).

The next sect section will presents the extraction, the characterization technics and then we will presents our technics itself.

3. SECURE CONTACTLESS CYLINDRICAL FINGERPRINT TEMPLATE GENERATION

This section describes what our contactless fingerprint template stand for.

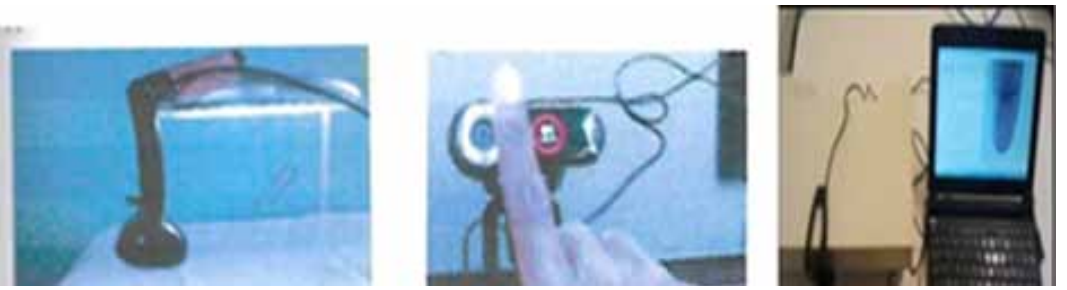
3.1. Extraction of the Characteristics of The Acquired Image

This step involves the extraction of the minutiae points present in the fingerprint image for the calculation of the secure model and the calculation of the center of mass of the fingerprint image.

3.1.1. Image Acquisition

The user is invited to place the opposite side of his finger on a shelf marked by a rectangular area to limit movement. The user's palm is facing the webcam. We then proceed to capture the fingerprint. Our images are in JPG format with a size of 640 × 480 pixels reduced to 480×480 for our experiments. The acquired images come from several individuals. Several experimental tests were carried out to define the distance of the webcam from the tablet, which is 7 cm. The contactless fingerprint acquisition system we used consists of a medium- resolution digital photo capture webcam (Logitech c120), a capture interface to visualize the sharpness of the images before capture, and hardware lighting.

Figure 4. Non-contact acquisition system (Djara et al,2009) during preprocessing, we opted for the grayscale thresholding developed in (DMerad et al, 2004).



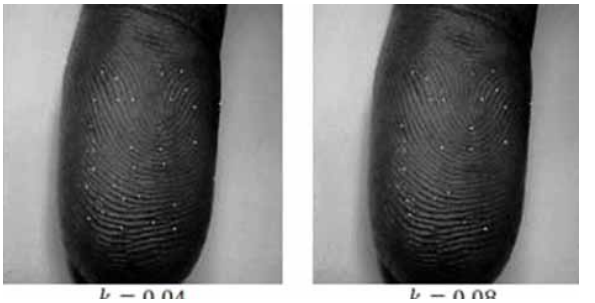
3.2. Spatial Characterization of Fingerprints

(Wang et al, 2016) have used as biometric signature the position of the minutia in the image (coordinates (x, y)), the type of minutia in question (termination or bifurcation) and their direction determined as shown in Figure 5

In all cases, the direction is measured in relation to the horizontal. Here we propose a modification for taking angles. Indeed, we retain as a parameter of spatial characterization:

- The type of minutiae: termination or bifurcation,
- The position of the detail in the image: coordinates (u, v),
- Their direction determined (Djara et al, 2010)

Figure 5. Example of detection of points of interest (Djara et,2009)



The angles used here are independent of the orientation of the impression. For minutiae of the bifurcation type, these are the relative angles between the branches, whereas for the terminations it is the angle which lays between two vectors having as origin the termination point and as ends two points belonging to the termination branch.

The spatial feature extraction algorithm we have developed consists of three steps which are: detection and elimination of false timings and determination of the orientation of the branches.

We first present the method we used to detect the minutiae. In a second step, we present the method for eliminating false minutiae and the technique for determining the orientation of branches that we have developed.

3.2.1. Parameters for Spatial Characterization of Minutiae

Let E_1 and E_2 be two sets of minutiae.

a) **The E_1 set**:are extracted:

· The position of the This set groups together the detected and validated termination type timers. For each termination, two characteristics termination in the image: coordinates (x_i, y_i), the orientation θ_i linked to the outgoing branch of the point as shown in Figure 6

Figure 6. Characteristics extracted from a minutiae: (a) Nicolas GALY (b) Christel-Loic TISSE(Djara et al, 2010)

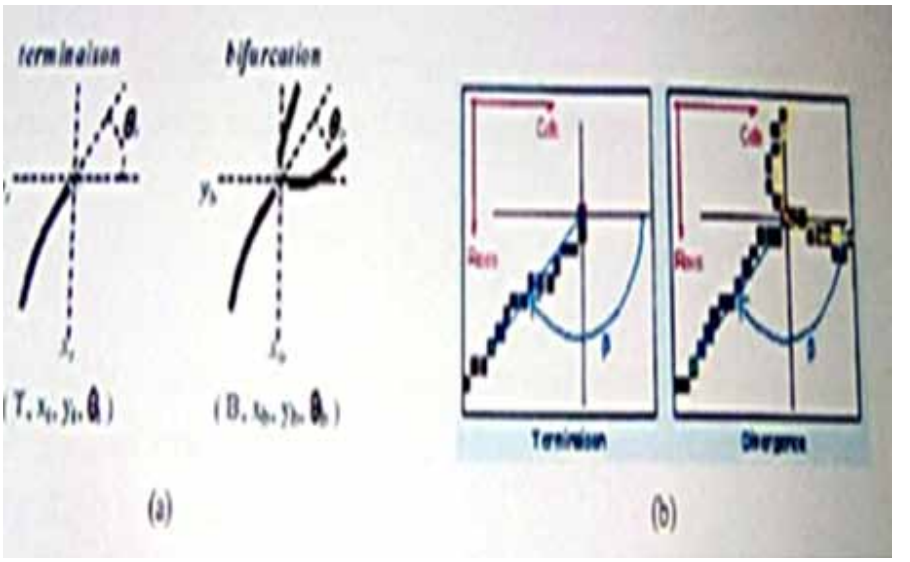
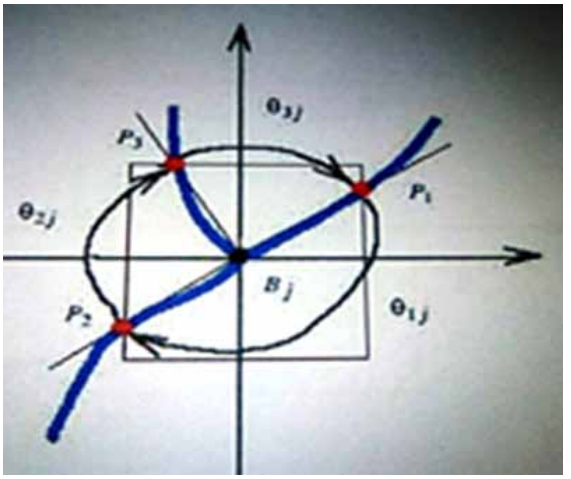


Figure 7. Determination of termination angle



$$E_1 = \{T_i = (u_i, v_i, \theta_i);\ i \in [1...N]\} \tag{3.1}$$

N is the number of terminations detected and validated (Djara et al, 2010).

b) The E_2 set:

It groups together all the bifurcations detected and validated. Thus, for each bifurcation, two characteristics are extracted:

The coordinates (u_j, v_j) of the bifurcation point. The three corners θ_{1j}, θ_{2j} and θ_{3j} as shown in Figure 5.

$$E_2 = \{B_j = (u_j, v_j, \theta_{1j}, \theta_{2j}, \theta_{3j});\ j \in [1...M]\} \tag{3.2}$$

M is the number of bifurcations detected and validated (Djara et al, 2010)

3.2.2. Bifurcation Branch Orientation

The vicinity of a bifurcation point consists of three branches whose relative angles are parameters for the spatial characterization of the bifurcation. A window F of size n x n is centered on each bifurcation point. On the perimeter of the window, there are three points P1, P_2 and P_3 with respective coordinates: (u_1, v_1), (u_2, v_2), and (u_3, v_3) intersection of the branches with F.

We used a 13 x 13 size window. This size is related to the minimum length of a branch. After several experimental tests, we have chosen 15 pixels as the minimum length of a branch. So the size of the window must be at most equal to this minimum length to avoid ending up with a window that does not really cut the branches when its size would be greater than this minimum length.

The determination of the angles ρ_{1j}, ρ_{2j} and ρ_{3j} between the three branches is done by applying the formulas (3.10), (3.11), (3.12)

$$\rho_{1j} = Arccos\left(\frac{\overrightarrow{B_jP_1}.\overrightarrow{B_jP_2}}{B_jP_1 \times B_jP_2}\right) \tag{3.3}$$

Figure 8. Bifurcation Angle determination

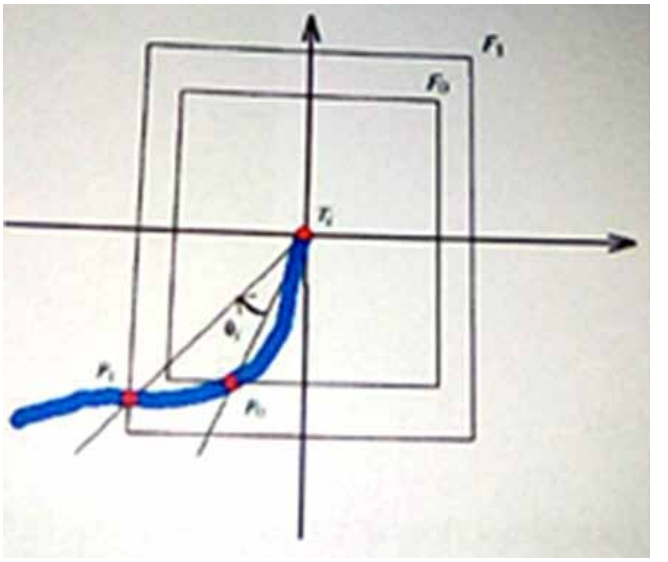
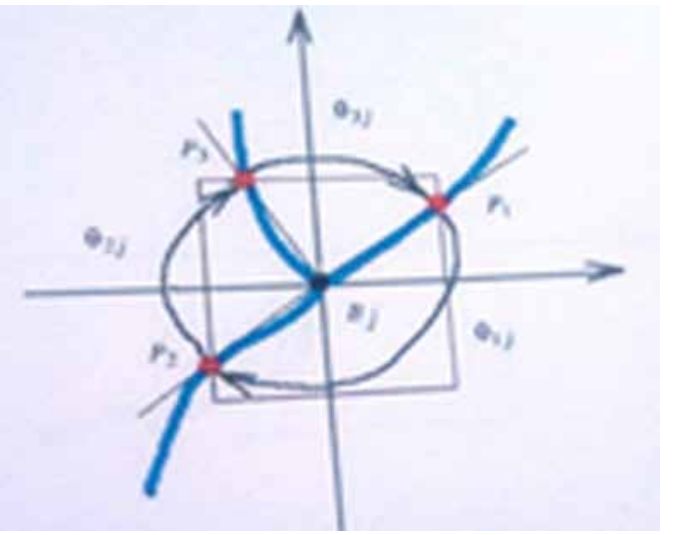


Figure 9. Determining bifurcation angles



$$\rho_{2j} = Arccos\left(\frac{\overrightarrow{B_jP_2}.\overrightarrow{B_jP_3}}{B_jP_2 \times B_jP_3}\right) \tag{3.4}$$

$$\rho_{3j} = Arccos\left(\frac{\overrightarrow{B_jP_3}.\overrightarrow{B_jP_1}}{B_jP_3 \times B_jP_1}\right) \tag{3.5}$$

B_j being the junction point.

In summary, to the M bifurcation points is associated a matrix composed of M rows and 5 columns (3.13). Each bifurcation point is represented by a row in the matrix and the columns represent respectively the coordinates of the point and the angles between the branches.

$$\begin{pmatrix} u_1 & v_1 & \rho_{11} & \rho_{21} & \rho_{31} \\ u_2 & v_2 & \rho_{12} & \rho_{22} & \rho_{32} \\ \dots & \dots & \dots & \dots & \dots \\ u_M & v_M & \rho_{1M} & \rho_{2M} & \rho_{3M} \end{pmatrix} \tag{3.6}$$

3.2.3. Orientation of the Branches of Terminations

One considers two concentric windows (F_0, F_1) of center the point of termination T_I. F_0 is serious N X N and F_1 of size m $\times$ m with N < m. On the perimeter of the window F_0 we have a point P_0 intersection of the branch with F_0. Also on the perimeter of the window F_1 we have a point P_1 intersection of the branch with F_1. The angle of termination the 2nd considered is the angle between $\overrightarrow{T_iP_0}$ et $\overrightarrow{T_iP_1}$ as indicated on figure 5.

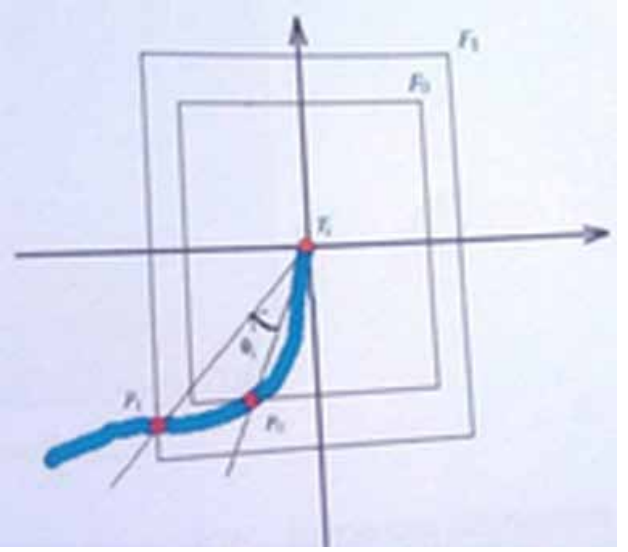
We used F_0 with N = 5 and F_1 with m = 13.

The determination of this angle is done by applying the formula (3.7)

$$\rho_i = Arccos\left(\frac{\overrightarrow{T_iP_0}.\overrightarrow{T_iP_1}}{T_iP_0 \times T_iP_1}\right) \tag{3.7}$$

T_i being the iieme point of termination.

Figure 10. Determination of the angle of termination



In short, with N points of termination a matrix made up of N lines and 3 columns (3.15) is associated. Each line of the matrix represents a termination and the columns respectively represent the coordinates of the point and the angle of the branch (Djara et al, 2010).

$$\begin{pmatrix} u_1 & v_1 & \rho_1 \\ u_2 & v_2 & \rho_2 \\ \dots & \dots & \dots \\ u_N & v_N & \rho_N \end{pmatrix} \tag{3.8}$$

3.2.4. Presentation of the Technique of Construction of the Cylindrical Curve

An authentication fingerprint system requires a technique that is invariant by rotation and translation. In addition, it must also be efficient in terms of managing intra-personal variation. Moujahdi et al. proposed such a technique called Fingerprint Shell (Moudjadi et al, 2014) which transforms the minutiae based fingerprint model into a spiral curve using the user's d_0 key. This technique first calculates the distance between each minutiae point and the COM and then ranks them in ascending order for the generation of the spiral curve. Let hn be the values of the distances in ascending order. A curve that has a spiral shape is constructed from h_1, h_2, … , h_n, the user key and it ordered the distance values as shown in Figure 7.

In the spiral curve, the distances h_1+h_0, $h_2 + h_0$, - - , $h_n + h_0$ form contiguous right-angled triangles, with these distances as the hypotenuse of the triangles respectively. In (Ali et al, 2015), the authors proposed the use of a key pair instead of a single key to improve the security of the Shell Fingerprint. These techniques (Fingerprint Shell and the one presented in (Ali et al, 2015)) are highly dependent on the distances between minutiae points and the singular point, and in these techniques, if an opponent gets the information from the spiral curve (the coordinates (u_1, v_1), (u_2, v_2) - - (u_n, v_n)) by attacking the database where the user's model is stored then from this information, the distances between the minutiae points and the singular point (h) can be easily obtained as shown in algorithm 1.

ü These distances between the minutiae points and the singular point never change since they are constantly associated with the user's fingerprint. Since the spiral curve is generated from these distances, if the spiral curve is then compromised, the total security of the biometric system depends solely on h_0 the user's key. In this case, the biometric system will look like a password-based system, where the user's key will behave like a password for the user. This represents a serious disadvantage and security threat to the techniques proposed in (Moujahdi et al, 2014) and (Ali et al, 2015). Also in (Zannou et al, 2019), authors have proposed a similar technique that relies heavily on the center of mass of the image given that the singular point may be multiple or even non-existent. The better the keys are generated from zernike moments. The resulting spiral curves are compared using Hausdorff distances, so there is a need to secure the distances between the minutiae points and the center of mass in the sequence.

The weaknesses and alternatives for improving the techniques proposed in (Zannou et al, 2019; Ali et al 2015; Moujahdi et al, 2014) are summarized below:

- These techniques use non-revocable distances calculated between the minutiae points and the singular point if the user's model is compromised then the information relating to these distances is also compromised;

Figure 11. Secured distance generation : a) Example of fingerprint where circle are the location minutiae points whereas the point marked with a box shows the singular point and arrows show the orientation of minutiae points. B) calculation of the distance l_i of the i^{th} minutia point

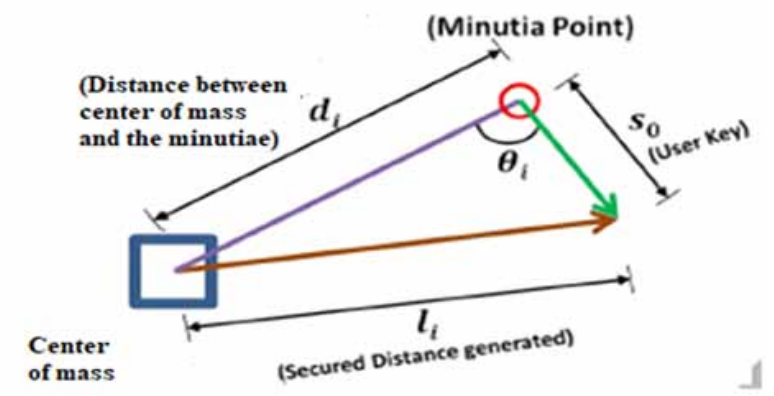


Figure 12. (a) Computation of Fingerprint Shell using key h_0 and distances h_n

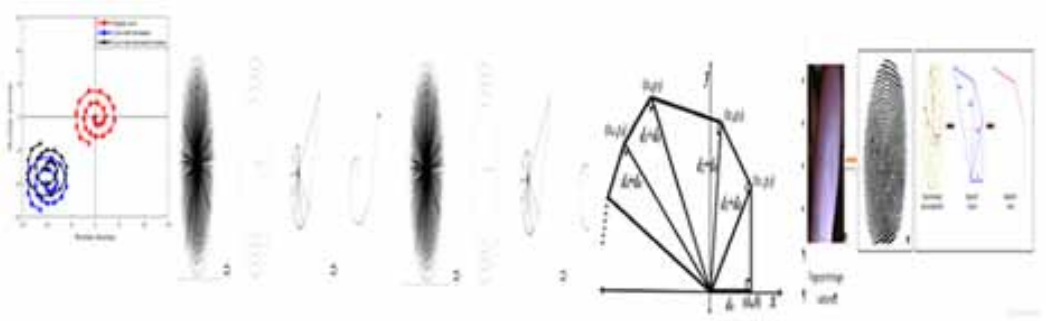


Figure 13. (b) Algorithme 1

Algorithm 1: 2D Spiral Curve

```
   Input  : d0, com : coordinates of center of masse, listDn : sorted list of d_n
   Output : Spiral Curve S
1  begin
2      r ← d0;
3      x ← 0.0;
4      y ← 0.0;
5      tta ← 0.0;
6      p ← new List();
7      for i ← 0 to listDn.length do
8          if i = 0 OR i = 1 then
9              r ← d0;
10             tta ← .0;
11         end
12         else
13             dy ←euclidianNorm(listDn[i] + d0, listDn[i − 1] + d0);
14             dx ← listDn[i − 1] + self.d0;
15             tta ← tta + atan(dy/dx);
16             r = listDn[i] + d0;
17         end
18         x ← r * cos(tta);
19         y ← r * sin(tta);
20         p.append((x, y))
21     end
22     S ← plot(p);
23 end
```

- These techniques use singular dots which can be multiple on a fingerprint image or non-existent when the fingerprint is damaged ;
- The key can be misplaced or forgotten, especially when the individual has Alzheimer's;
- Contact systems expose users to epidemics;
- Images from contact systems are subject to distortion;
- Non-contact systems prevent many of the attacks associated with contact systems.

Since we know that the orientation of a calculated minutiae point with respect to the line joining center of mass (COM) and minutiae point is an invariant characteristic, which can be used for a strong and secure user model generation. The termination number between the minutiae points and the center of mass (COM) can also be used in these techniques for secure biometric template generation with high resistance against rotational and translational effects. The proposed technique generates the highly secure user template and overcomes the drawbacks of (Moujahdi et al, 2014; Ali et al, 2015; Zannou et al, 2019) in the following way:

- The orientation of the minutiae points relative to the line joining the minutiae points and the center of mass (COM) is used to calculate revocable distances. To generate the revocable distances, the orientation information obtained from a minutiae point is merged with the distances between the minutiae points and the center of mass (COM).
- The revocable distances are used to generate the secure user model. In this case, if a template is compromised then the user will have the freedom to use another set of distances (since the distances are revocable) to generate a new biometric template.
- The number of terminations between minutiae points and center of mass (COM) is also used to secure the secure biometric template generation. Using the number of terminations, the proposed technique generates a secure revocable contactless cylindrical curve based on the user's template.

The generated cylindrical contactless cylindrical model proves to be more secure and strong unlike the user model in dimension 2 generated in (Ali et al, 2015 and Moujahdi et al, 2014)

4. TECHNIQUE SUGGESTED

- The main motivation of the proposed technique for the calculation of the fingerprint-based biometric model is to generate a secure cylindrical curve by spherical and mathematical transformations using the details extracted from the minutiae points belonging to the user's fingerprint. This cylindrical curve is used as a secure model for user enrollment and recognition. The cylindrical curve is constructed in such a way that even if the opponent obtains the data from the cylindrical curve, he will be difficult to obtain any type of information related to the characteristics of the user's fingerprint.
- The model is generated from the fingerprint print using a set of keys $\{ w_0, p_0, b_0 \}$. Figure1 shows the diagram of the proposed technique. During enrollment, the generated template of $\{ w_0, p_0, b_0 \}$of the user is stored in the database that is later used for authentication the user. Algorithm 2 shows the calculation of the proposed secure biometric template from the fingerprint print. In the proposed technique, we call the u-axis, the rib axis the v-axis and the c-axis in 3-dimensional space. Details of the steps in the calculation of the proposed secure non-contact revocable cylindrical curve are given below.

Figure 14. Computation of secured contactless cylindric

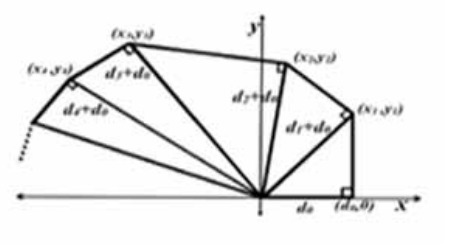


Figure 15. Computation of fingerprint shell using d_0 and d_i fingerprint template

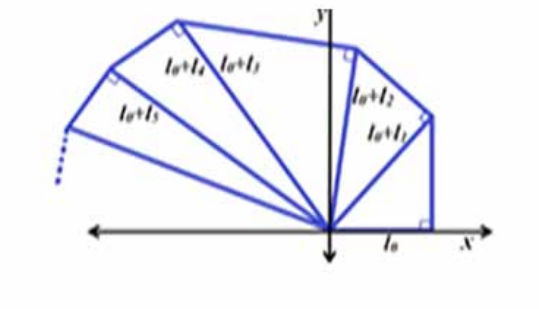


Figure 16. Images from our système

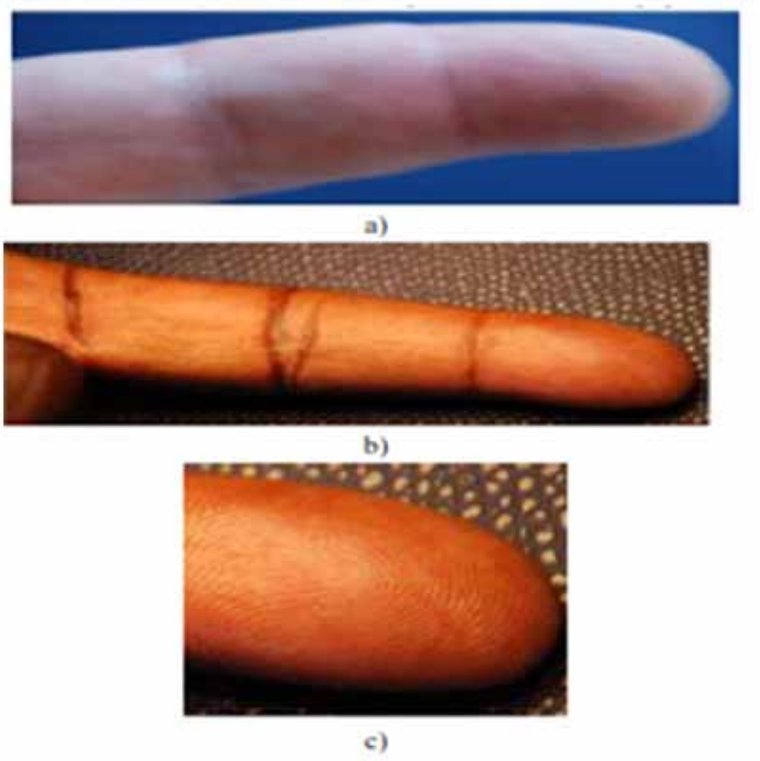


Figure 17. Key d_0 computation by using total part of s_0,l_0 and t_0

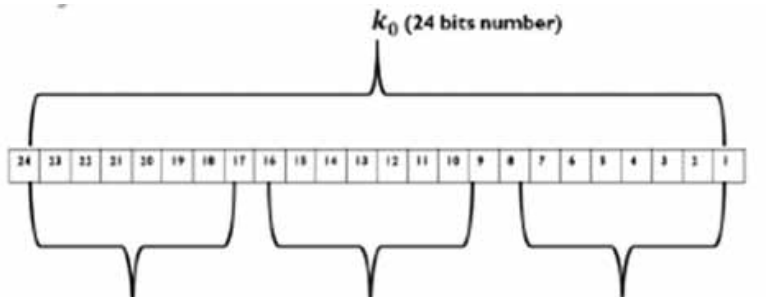
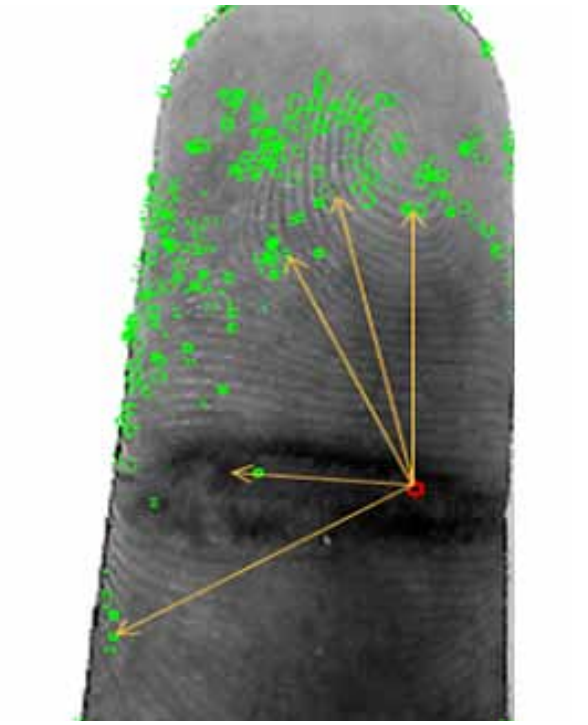


Figure 18. Ridge ending in ellipse and bifurcation in square on a fingerprint feature



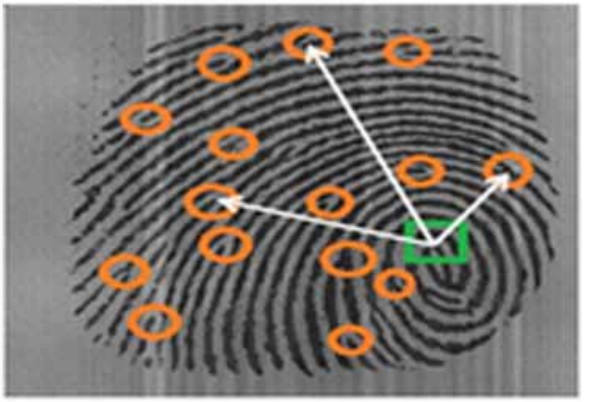
4.1. Coordinates of the Centre of Mass

• The coordinates of the COM, ($\bar{u}, \bar{v}$), is the intersection of the lines .This technics has been developed in (Djara et al, 2009).

4.1.1. Key Generation (w_0, p_0, b_0)

The calculation of the center of mass (COM) and the modified hausdorff distance was done in the article (Zannou et al, 2019)

Figure 19: Distances (white arrows) between extracted minutiae points(orange circle) and center of mass(green rectangle) are calculated



4.1.2. The User's w_0 Key

The user's w_0 key is calculated using the zernike moment (Djara et al, 2010). Because of the risk of forgetting (Alzheimer's patient), it is stored in the database and restored if necessary. w_0 thus ensures the revocability of the system in the sense that when the user changes this key (in case of compromise) the generated cylindrical curve differs totally from the previous one.

4.1.3. Calculation of Safe Distances l_i

Let n minutiae points present in the fingerprint image. Let h_0, h_1, - - -, h_n be the distances separating respectively the center of mass at each ith minutiae and θ_i the orientation relative to each minutiae with respect to the COM. Now let g_0, g_1, …, g_n be the number of terminations of these termination points relative to the COM. A user key w_0 is used to generate the safe distances p_i (i = 1, ... , n) for each user. Calculating the safe distance p_i(i=1...n) for each minutiae point requires the involvement of the COM locations and minutiae and the details of the ρ_i(i=0).n orientation of each COM-related minutiae point. Figure 11b depicts the relationship between h_i, w_0, and p_i for each i^{th} minutiae point. Applying the triangular law of vector addition, the numerical value of li is given as follows:

$$p_i = \sqrt{h_i^2 + w_0^2 + 2(h_i * w_0 * \cos(\rho_i))} \quad (4.1)$$

We call li a safe distance since it is calculated from the distance between the minutia point and the center of mass (COM), the orientation information of a minutia point relative to the center of mass (COM) and the user key w_0. The orientation information of minutiae points relative to the center of mass (COM) is not stored in the database, w_0 if the distances (p_i) are compromised, we can revoke them and replace them with another set of distances by changing the user key w_0, thus obtaining a secure distance p_i. The minutiae points are arranged relative to the safe distances (p_i, i = 1...n) in ascending order. The distances (p_i) are ordered in ascending order for later calculation. Let p_1, p_2, …, p_n be the distances in ascending order.

4.1.4. Construction of the Cylindrical Curve

Using a user key w0 and the ordered distances li, several contiguous right-angled triangles are constructed, the distances (p_0, … , p_n) are the hypotenuses of these triangles as shown in Figure

8 where w_0 and hi are the sides of the right angle. This generates a secure revocable non-contact cylindrical curve. Figure 6a shows an example of a spiral curve for a fingerprint where the abscissa and ordinate values are calculated as mentioned in Algorithm 2.

4.1.5. Calculation of g_i

The calculation of gi is as follows:

$$g_i=p_i+p_0. \tag{4.2}$$

Transformation of cylindrical coordinates to cartesian coordinates

4.1.6. Calculation of σ_i

$$\sigma_i = \begin{cases} tan-1\left(\frac{v_0}{u_0}\right) & sii=0 \\ \omega_{i-1} + \tan^{-1}\left(\frac{r_{i-1}}{r_i}\right) & sii\neq 0 \end{cases} \tag{4.3}$$

5. CALCULATION OF COORDINATES U_I, V_I AND C_I

ui and vi are obtained by changing variables from cylindrical to spherical coordinates. Let us assume that $c_i = \rho_i * b_0$

The ui and vi coordinates are deduced as follows:

$$\begin{cases} u_i = gi * \cos\left(\rho_i\right) \\ v_i = g_i * \sin\left(\rho_i\right) \\ c_i = \rho_i * t_0 \end{cases} \tag{4.4}$$

5.1. Secure and Revocable Cylindrical Fingerprint Curve Construction

The cylindrical curve is calculated from the spiral curve in dimension 2 obtained in the previous step using the information of the number of terminations and a user key b_0. For the ith point of the spiral curve, the rib is obtained using the user's key b_0 and the number of terminations g_i of the minutiae point i calculated by determining the terminations between the minutiae point and the center of mass (COM). The following equation define calculates the rib for the ith point in the spiral curve in dimension 2. This generates the safe and revocable cylindrical curve as shown in Figure 16b:

5.2. Transformation of the Spiral Curve

The curve in dimension 3 generated in the previous step is transformed using $\{ w_0, p_0, b_0 \}$, b_0 is a 24-bit integer generated from w_0, p_0, and b_0. The first 8 bits (from the least significant bit) of a_0 are the integral value of w_0, the next 8 bits are the integral value of p_0, and the last 8 bits are the integral value of b_0 as shown in Figure 10. In this way we carry out a transformation of the rotations of the

spiral curve in dimension 3 of angles w_0 and p_0 radians with respect to the ordinate axis and the rib axis, and a translation of the spiral curve in dimension 3 of a_0 units. The general notion of the translation of the spiral curve in dimension 3 is depicted in Figure 16a, while Figure 16b shows an example of the transformed safe revocable non-contact cylindrical curve for the initial safe revocable non-contact cylindrical curve shown in Figure 16a. The transformed safe revocable non-contact cylindrical curve obtained in this way is shown to be highly secure and is stored in the database which can be used later to authenticate the user.

Cylindrical curves are generated and stored in the database. During authentication, the user's model is generated considering the COM is used for comparison with all models stored in the database for a particular user. The best matching score obtained in the comparison is considered for the ðnale authentication.

Figure 20. Cylindrical template computation for fingerprint image using different set of keys

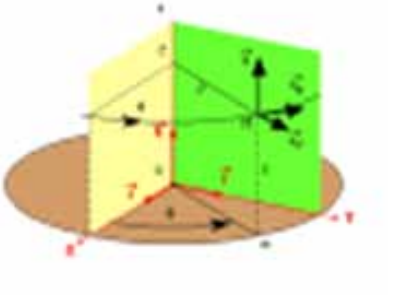
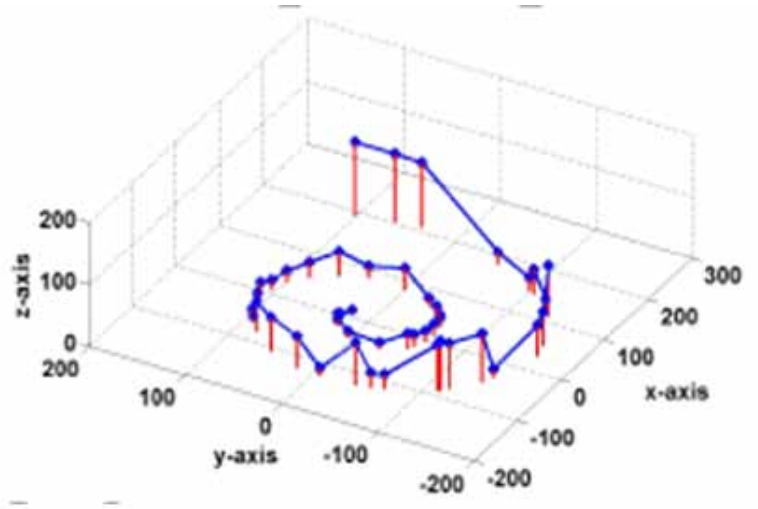


Figure 21. Cylindrical transformation



6. MATCHING

Authentication will be done using the secure revocable non-contact cylindrical curve generated from the scanned image. The generated curve is compared with the secure non-contact cylindrical curves

stored in the database for a particular customer and the coupling result is determined. When the matching score matches the matching threshold criteria then the customer is identified as the original user. In order to match two cylindrical curves we refer to Hausdorff's notion of distance (Taha et al, 20015 and Chen Y et al, 2017).

7. MAINTENANCE OF THE USER KEY

Each user of our developed technique has its own set of keys $\{ w_0, p_0, b_0 \}$. These keys can be maintained in two ways. At first, we can store it in the database so that it is accessible only to the authentication device that will be able to use it in the generation of the secure model. Second, the key set will only be disclosed to the specified client and he/she communicates it to the device during authentication. This method warns us of the decryption attack.

8. EXPERIMENTAL ANALYSIS

The evaluation of the proposed technique on the fingerprint databases FVC2000 DB1, FVC2000 DB2, FVC2002 DB1, FVC2002 DB2, FVC2002 DB3, FVC2002 DB4, FVC2004 DB1, FVC2004 DB2 and on the one we designed based on the FVC(Fingerprint Veriðcation Competition protocol) i.e. the fingerprint verification protocol (Maio D. et al,2002) as well as 1-versus-1 protocol (Ferrara et al, 2012).

8.1. Experimental Device

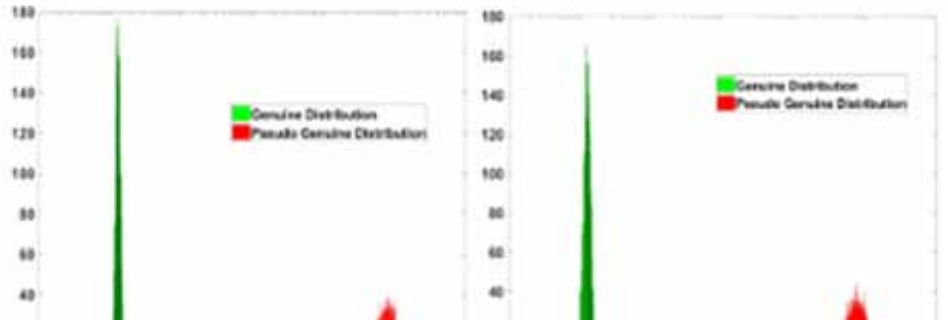
We conducted the experiments on an Intel® computer core™ i5-2500 CPU@3.1GHz processor with 4GB RAM. Our own fingerprint feature extraction application. Our application calculates and displays center of mass coordinates. Our application also allows us to process our images without contact through its different steps: image binarization, image skeletonization, minutiae detection and then minutiae extraction. After extracting the features, we store them in a feature matrix.

Table 1 provides details on the databases used to conduct the experiment. Table 2 provides detailed information about the number of images used to experiment with each technique. To evaluate the prowess of our method, we tested the False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), FMR1000 and ZeroFMR (Ali et al, 2015 and Moujahdi et al, 2014).With reference to the FVC protocol (Fingerprint Veriðcation Competition protocol) (Ferrara et al, 2012), the FAR calculation, each client's fingerprint reference model and resemblance scores are acquired to determine the distribution of the malware score. In order to later evaluate the FRR, each model of an individual's fingerprint image is compared with the remaining fingerprint image samples for the same individual and the resulting similarity scores are acquired to assess the distribution of the malicious person score. The FRR is later calculated by comparing each fingerprint template to the other fingerprint image templates from the same individual and similarity test results are obtained to determine the distribution of the original score. The relationship between the first original template and the second template from the same individual is determined in the 1-vs-1 protocol (Ferrara et al, 2012) for the purpose of calculating the FRR while for the purpose of evaluating the FAR, the comparison of the first template of the image of each individual is performed with the very first template of the fingerprint image of the other individuals. The value of the FRR(ZeroFMR1000) when estimating the FAR value is 0.001% while ZeroFMR remains the smallest value of the FRR when the FAR value is 0.0%. The Kolmogorov-Smirnov test (R. Wilcox, 2005) was used to evaluate the separability of the customer and malicious score distributions. In this evaluation, the set of values obtained is between 0 and 1 where a score very close to 1 describes a good separation of the results.

Table 1. Detail related to on the data bases used for the experiment

	Total subjects	Sample per subject	Total No of fingerprint samples
FVC2000 DB1	100	8	800
FVC2000 DB2	100	8	800
FVC2002 DB1	100	8	800
FVC2002 DB2	100	8	800
FVC2002 DB3	100	8	800
FVC2002 DB4	100	8	800
FVC2004 DB1	100	8	800
FVC2004 DB2	100	8	800
Our own base	1375	6	8250

Figure 22. Receiver Operating Caracteristics(ROC) curve obtained from many databases when our technique is using



8.2. Results and Discussion

The estimation of the results of the suggested technique in terms of revocability, diversity, safety and recognition rate is detailed in the following table:

9. REVOCABILITY

Assessment of revocability: When a biometric conformation of a customer of the system is vilified by a thief, the exposed conformation could be changed with another conformation built from the same biometric information of the customer; therefore the method of protection of the biometric conformation is qualified as revocable. In the suggested method, when a malevolent attacker attacks the database and generates the cylindrical curve of a system user, the client has the ability to change the set of client keys and generate a new cylindrical curve. Figures 16a and 16b show sample specimens generated for the same person based on different key sets. The resulting specimens differ from each other and do not resemble each other in any way. Therefore, when a cylindrical curve is corrupted, the user can modify the set of keys and produce a new curve that is totally different from the previous one based on the original identical biometric data. The robustness of the proposed template in terms of revocability is justified.

Table 2. Details of number of technical images of databases used for evaluation by various

	FVC2000 DB1	FVC2000 DB2	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2002 DB4	FVC2004 DB1	FVC2004 DB2	Our own base of data
Boult et al.[32]	800	800	800	800	-	-	800	800	-
Ahn et al.	-	-	800	800	800	800	-	-	-
KUMAR et al.[10]	-	-	-	-	-	-	-	-	-
Ferrara et al.[18]	-	-	800	800	800	800	800	-	-
Cappelli et al.[26]	_	_	800	800	800	800	-	-	-
Moudjadi et al.[9]	-	-	799	707	-	-	-	-	-
Tran et al.. [33]	-	-	-	800	-	-	-	-	
Khan et al.[33]	-	-	-	-	-	-	-	-	-
Derman and keskinoz[12]	-	-	-	-	-	-	-	-	-
Ali and prakash. [28]	-	-	-	-	-	-	-	-	8250
If et al.[36]	-	-	-	-	-	-	800	-	-
Sandya et al.[22]	-	-	800	800	800	-	-	-	-
Liu and zhao	-	-	800	800	-	-	-	-	-
Ali and Prakash	785	792	799	797	757	793	778	750	5292
Solution suggested									

Note: "-" in a cell indicates that the heights of this technique did not defer the number of images or the comparisons implied in the experimentation.

Type -I attack: The old template of a user that has been deleted is reused by the malicious person to damage the authentication device that contains a revived client specimen generated from the original fingerprint image of the same finger and using a different set of keys.

Type-II Attack: The old model of a revoked user is reused by a malicious person to verify the authentication device containing a revived specimen of the user generated from a fingerprint image of the same finger using different keys.

The results presented in Table 5 acquired for the revoked specimen attack for the suggested method on the FVC 2002 DB1 and DB2 databases. Based on the previous findings, we can clearly see that the proposed method against the revoked specimen attack. This is proof that revoked and renewed specimens do not look alike and cannot be traced.

9.2. Diversity

Assessing diversity: The diversity of a biometric specimen is achieved when it is guaranteed that the new specimen does not have a match with the old specimen. In order to evaluate the diversity, we test

Table 3. Evaluation of our model having for reference other models from performance indicators the protocol used is the FVC protocol(values are in percentages)

Various techniques	FVC2000 DB1			FVC2000 DB2			FVC2002 DB1			FVC 2002 DB2			Our own databse
Boult et al. [32]	EER	FMR 1000	zero FMR	EER	FMR 1000	zero FMR	EER	FMR 1000	zero FMR	EER	FMR 1000	zero FMR	EER
Ahn et al.	2.9	-	-	2.5	-	-	2.1	-	-	1.2	-	-	11.80
KUMAR and al.[10]	--	--	-	-	-	-	7.18	-	-	3.6	-	-	-
Ferrara et al.[18]	-	-	-	-	-	-	1.88	3.14	5.07	0.99	1.43	1.4	4.4
Cappelli et al. [26]	-	-	-	-	-	-	1.00	1.64	3.18	0.49	0.68	0.89	3.14
Moudjadi and al.[9]	-	-	-	-	-	-	2.03	4.18	6.36	1.01	1.39	2.21	-
Tran et al. [33]	-	-	-	-	-	-	-	-	-	0.49	0.07	-	-
Khan et al.[33]	-	-	-	-	-	-	-	-	-	-	-	-	-
Derman and keskinoz[12]	-	-	-	-	-	-	6	-	-	6	-	-	14
Ali and prakash. [28]	-	--	-	-	-	-	-	-	-	-	-	-	-
If et al. [36]	-	-	-	-	-	-	-	-	-	-	-	-	-
Technical Proposed													

Note: "-" in a cell indicates that the authors of this technique did not defer this particular value for the data base.

Table 4. Performance evaluation using 1-vs1 protocol (been worth in percentage)

Various Techniques	FVC2002												Our own database
	DB1			DB2			DB3			DB4			
	EER	FMR 1000	zero FMR	EER	FMR 1000	zero FMR	EER	FMR 1000	zero FMR	EER	FMR 1000	zero FMR	EER
Sandhya and al.[21]	0	-	-	0	-	-	3.65	-	-	-	-	-	-
Sandhya and al.[22]	0	-	-	0	-	-	1.65	-	-	-	-	-	-
Sandhya and al.[23]	0	-	-	0	-	-	1.65	-	-	-	-	-	-
Liu and Zhao[1]	-	0	0	-	0	0	-	-	-	-	-	-	-
Cappelli et al.[26]	0	0	0	0	0	0	2	3	5	3.48	5	5	-
Ferrara et al.[18]	0	0	0	0.02	0	1	3.43	4	5	3.37	9	11	-
Proposed techniques	0	0	0	0	0	0	0	0	0	0	0	0	0

Note: "-" in a cell indicates that the authors of this technique did not defer this particular value for the data base.

Table 5. Successful attack using revoked template (been worth are in percentage)

Database	Attack of type I	Attack of type II
FVC2002 DB1	0.0	0.0
FVC2002DB2	0.0	0.0

Table 6. Comparison of the average time taken by the algorithm (value in milliseconds)

	Template generation	Template matching
Fingerprint Shell[9]	52	0.9
Technical Proposed	73	1.4

the suggested method with several sets of keys (over 1000) and compare the generated specimens. Thus the robustness of the suggested method against cross-matching attack is evaluated.

Robustness against cross-matching: When a user of the system is using the biometric template of the same biometric information in several applications. Thus, if the malicious person uses a customer's specimen in one application, it will be impossible for him to use the same template in another application simultaneously. This would mean that the customer's specimens produced for a user for different systems are varied. We have considered two sets of user keys for each database; this would mean that we produce two different devices from two sets of keys. In device1, We identify the values p_0, w_0, t_0 randomly in the interval $p_0 \epsilon [0,10]$, $w_0 \epsilon [0.10]$ and $b_0 \epsilon [0.10]$, w_0 for device 2, the estimates of p_0, w_0 and b_0 are randomly selected in the range $l_0 \epsilon [15,20]$, $w_0 \epsilon [15,20]$ and $b_0 \epsilon [15,20]$. Each identical client fingerprint specimen in system 1 is confronted with fingerprint specimens of the same person in device 2 to evaluate the pseudo-original result. Figure 19 shows the distribution of the pseudo-authentic score for devices 1 and 2. The graph highlights the fact that the original similarity results for device 1 and the original pseudo-scores for device 2 are well separated. Figures 16a and 16b show that for different sets of keys, we have a clear difference in the specimens (cylindrical curves) generated from the biometric data p_0, b_0 and w_0 which proves the robustness of the suggested method against cross-matching attack. The diversity of the suggested method has been evaluated using many (more than 1000) different sets of customer keys and identical results as shown in figure 19 are obtained. All this proves that the suggested method has a very good revocability and diversity.

9.2. Security

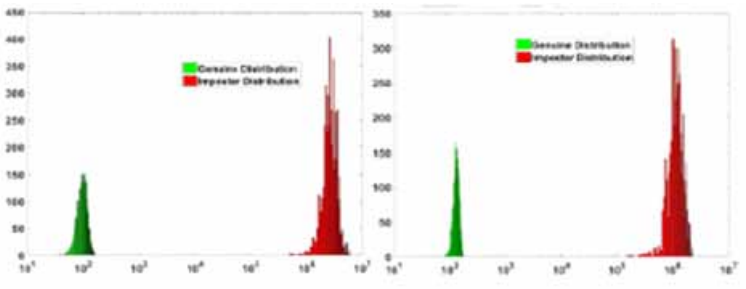
We analyze the security provided by the suggested method and compare it to the Shell fingerprint (Moujahdi et al, 2014). When the cylindrical curve is attacked in (Moujahdi et al, 2014), the distances between the minutiae points and the COM are easily computed as presented in algorithm 1. On the other hand, in our suggested method, when the client specimen is compromised, then the information about the revocable distances li can be extracted by the opponent. The distances between the minutiae points and the center of mass, and the orientation of the minutiae points with respect to the center of mass which are the revocable distances (p_1, p_2,...p_n) can be changed by changing the client key w_0. We can notice that the distances between the minutiae points and the COM are not stored in addition the orientation of the minutiae points relative to the center of mass either. The original distances (hi) and the orientation of the minutiae points h_0, h_1, ..., h_n relative to the center of mass cannot be discovered by a malicious person even if he decodes the cylindrical curve completely. Our cylindrical curve for our generated model is obtained from the distances li and a set of client keys, all these distances can be easily transformed by modifying the set of client keys. Thus, for the ith point of detail, the distance di to the center of mass and li the secure distance related to hi, extracted

from the client key s_0. Starting from figure 21b we clearly see that pi ϵ [h_i-w_0, h_i+w_0] and thus hi ϵ [p_i-w_0, pi+w_0], therefore each p_i for i varies from 1 to n. The values exist in a set of $2w_0$. Thus the distances between minutiae points and the center of mass cannot be obtained from the safe distances in our suggested method. Therefore, it follows that the proposed method provides a very high level of security and does not expose the information related to the thief's fingerprint even if the secure biometric specimen released in our proposed method is risky. Finally, the cylindrical curve can easily be modified by changing the client's keys.

Figure 23 presents the ROC curve of the unprotected system as well as the ROC curves of the three protection regimes considered in this study. First, we discuss the zero-effort attack scenario (Figure 23(a)), where the transformation parameters are known by the adversary, who tries to bypass the system using their own biometric models. A small performance degradation can be observed in the case of the spiral curve while the classiðcation performance is increased in the case of the cylindrical curve. In practice, both approaches need additional information (key, password, fingerprint etc.) during authentication. In the case of the cylindrical curve, even if the adversary has additional information, additional processing is required aðn order to exploit the stolen parameters correctly/ efðctively since the unique knowledge of the keys does not give access to the system.

In the scenario where the adversary does not possess the transformation parameters (ðgure 23(b)), there is a signiðcative increase in performance for the three protected systems compared to the unprotected system. The reduction in FARs, due to the use of a speciðc key for each user, makes this result very obvious. We can also notice a small degradation in the performance of the cylinder curve. This can be explained by the different ways in which the additional information is used.

Figure 23. Pseudo-Genuine/Genuine results repartition accordind to our technique(a) for FVC2002 DB1 database (b) for FVC2002 DB2 database



We can also notice a small degradation of the performance of the cylindrical curve approach compared to the Biohashing and BioPhasor approaches. This can be explained by the different ways in which additional information is used.

9.3. Performance

We evaluate the ERR of our method by comparing the results with the fingerprint shell [39] with other timely methods that still exist in order to evaluate the performance of our suggested method in terms of client recognition. The comparison of our score with that of other existing methods based on the FVC protocol while Table 4 gives us the results or 1-vs-1 methods are solicited. The experiment was conducted randomly for keys belonging to the intervals p_0 ϵ [0,50], w_0 ϵ [0,50] and b_0 ϵ [0, 50]

Figure 24. Imposter/Genuine repartition results distribution for our technique (a) FVC2002 DB1 database (b) forFVC2002 DB2 database

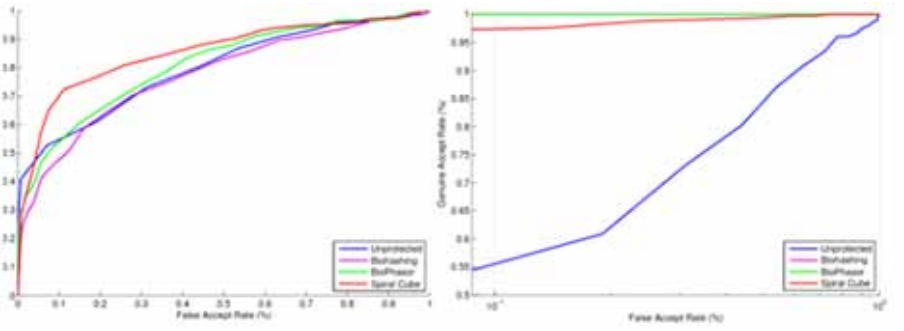
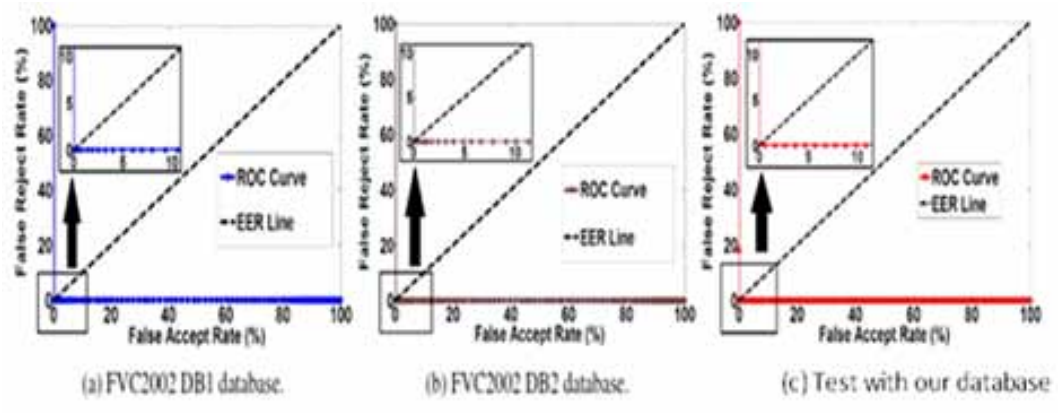


Figure 25. Curves ROC by using the data base YALE



for a perfect EER of 0.00%. The K-S (Kolmogorov-Smirnov) test for differents experiments directed by selecting the values of keys in the mentioned range equal to 1, which proves the ideal separation of the original and fraudulent results. Figure 10 shows the histogram of the distribution of original results or fraudsters for the fingerprint databases FVC2002 DB1 and FVC2002 DB2.

10. CONCLUSION

Biometrics offers a number of advantages over traditional authentication systems. However, there are still some problems in terms of security, confidentiality and privacy. There are many ways to manage this by securing a user's biometric templates. Among these solutions we can cite Fingerprint Shell which was previously suggested by (Moujahdi et al, 2014), Enhanced Fingerprint Shell (Ali et al, 2015), and contactless enhanced Fingerprint Shell (Zannou and al, 2019). In this article, we proposed a technique to build a highly secure template of a user using the data extracted from the contactless fingerprint through template generation corresponding to the minutiae points of a fingerprint. The proposed technique is robust and can handle the variations due to the translation and rotation of a finger on the fingerprint sensor at the time of fingerprint capture. The evaluation of the proposed technique has been performed on FVC2002 DB1, DB2, and DB3 fingerprint databases and on our own database. The EER(0.00%)

values obtained for the proposed technique show its good recognition capability for different scenarios with different keys. The performance was also judged to be much better compared to other existing approaches. The overall experimental results and their analysis show the effectiveness of the proposed technique in terms of revocability, diversity, safety and performance. Future work will focus on the texture aspects that are also of great interest in strengthening contactless authentication.

FUNDING AGENCY

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCE

Adler, A. (2005). Vulnerabilities in Biometric Encryption Systems. In Audio- and-Video-Based Biometric Person Authentication, 3546, pp 1100–1109. Springer Berlin Heidelberg.

Ahn, D., Kong, S. G., Chung, Y. S., & Moon, K. Y. (2008). Matching with secure ðngerprint templates using non-invertible transform. In *Proc*, 2, pp. 29–33). Of CISP.

Ali, S. S., & Prakash, S. (2018). *3-Dimensional Secured Fingerprint Shell*. Patt.Recogn. Letters.

Ali, S. S., & Prakash, S. (2015). Enhanced Fingerprint Shell. In *Proc. of SPIN 2015*, pp 801–805.

Ali, S. S., & Prakash, S. (2017). Fingerprint Shell Construction with Prominent Minutiae Points. In *Proc. of COMPUTE 2017*, pp 91–98. ACM.

Andakumar, K., & Jain, A. K. (2015). Biometric Template Protection Schemes: Bridging the Performance Gap Between Theory and Practice. *IEEE Signal Processing Magazine*, *32*(5), 88–100. doi:10.1109/MSP.2015.2427849

Boult, T. E., Scheirer, W. J., & Woodworth, R. (2007). Revocable ðngerprint biotokens: Accuracy and security analysis. In *Proc. of CVPR 2007*, pages 1–8.

Cappelli, R., Ferrara, M., & Maltoni, D. (2010). Minutia Cylinder-Code: A New Representation and Matching Technique for fingerprint Recognition. *IEEE Trans. on PAMI*, *32*(12), 2128–2141.

Cappelli, R., Ferrara, M., & Maltoni, D. (2010). Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition. *IEEE Trans. on PAMI*, *32*(12), 2128–2141.

Cappelli, R., Maio, D., Lumini, A., & Maltoni, D. (2007). Fingerprint image reconstruction from standard templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *29*(9), 1489–1503. doi:10.1109/TPAMI.2007.1087

Cavoukian, A., & Stoianov, A. (2009). Biometric encryption. In *Encyclopedia of Cryptography and Security*. Springer.

sChen, , YHe, , Y.W., & Hou, N. (2017). A local start search algorithm to compute exact Hausdorff Distance for arbitrary point sets. *Pattern Recognition*, *67*, 139–148.

Christel-Loic, T., Lionel, M., Lionel, T., & Michel, R. (2001). Système automatique de reconnaissance d'empreinte digitales, sécurisation de l'authentificationsur cartes à puce . http://hdl.handle.net/2042/3242/13225.

Cukic, B., & Bartlow, N. (2005). Biometric System Threats and Countermeasures : A Risk Based Approach. In *Biometric Consortium Conference*, 2005.

D. Merad, D. (2004). *Reconnaissance 2D/3D et 2D/3D d'objets à partir de leurs squelettes.* [PhD thesis] Université d'Evry-val d'Esonne.

Derman, E., & Keskinoz, M. (2016). Normalized cross-correlation based global distortion correction in ðngerprint image matching. In *Proc. of IWSSIP 2016*, pages 1–4.

Djara, T. and Vianou, A. (2009) Fingerprint Registration Using Zernike Moments : An Approach for a Supervised Contactless Biometric System. *9*, pp. 254–271.

Dorizzi, B., Cappelli, R., Ferrara, M., Maio, D., Maltoni, D., & Houmani, N. S. (2009). GarciaSalicetti, and A. Mayoue, "Fingerprint and on-line signature veriðcation competitions at icb 2009. In *Proceedings of the International Conference on Biometrics (ICB)*, Alghero, Italy, pp. 725–732.

Ferrara, M., Maltoni, D., & Cappelli, R. (2012). Noninvertible Minutia CylinderCode Representation. *IEEE Trans. on IFS*, *7*(6), 1727–1737.

Ferrara, M., Maltoni, D., & Cappelli, R. (2012). Noninvertible Minutia Cylinder-Code Representation. *IEEE Trans. On IFS*, *7*, 1727–1737.

Ferrara, M., Maltoni, D., & Cappelli, R. (2014). A two-factor protection scheme for MCC ðngerprint templates. In *Proc. of BIOSIG 2014*, pages 1–8.

Halevi, T., Li, H., Ma, D., Saxena, N., Voris, J., & Xiang, T. (2013). Contextaware defenses to rðd unauthorized reading and relay attacks. *IEEE Transactions on Emerging Topics in Computing*, *1*(2), 307–318.

Harris, C., & Stehens, M. (1988). A combined corner and edge detector. In *proceeding of the 4th Alvey Vision Conference*, pp 147-151.

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

Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric Template Security. *EURASIP Journal on Advances in Signal Processing*, *1*, 1–17.

Jain, A.K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. EURASIP J. Adv. Signal Process, p. 113:1–113:17.

Jain, A. K., Ross, A., & Pankanti, A. (2006). Biometrics : A tool for information security. Information Forensics and Security. *IEEE Transactions on*, *1*(2), 125–143.

Juels, A., & Sudan, M. (2002). A fuzzy vault scheme. In *Proc. of IEEE International Symposium on Information Theory*, page 408.

Juels, A., & Wattenberg, M. (1999). A fuzzy commitment scheme. In *Proc* (pp. 28–36). Of CCS.

Kumar, N., & Verba, P. (2012). Fingerprint image enhancement and minutiae matching. International *Journal of Engineering Sciences & Emerging Technologies,* pp 37-42.

Liu, E., & Zhao, Q. (2017). Encrypted domain matching of ðngerprint minutia cylinder-code (MCC) with l minimization. *Neurocomputing*, *259*, 3–13.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2002). FVC2000: FIngerprint veriðcation competition. *IEEE Trans. on PAMI*, *24*, 402–412.

Moravec, H. (1981). Rover obstacle avoidance. In *Proceeding of the 7th International Joint Conference on Artificial Intelligence*, page 785-790.

Moujahdi, C., Bebis, G., Ghouzali, S., & Rziza, M. (2014). Fingerprint shell: Secure representation of ðngerprint template. *Pattern Recognition Letters*, *45*, 189–196.

Nagar, A., Nandakumar, K., & Jain, A. K. (2010). A hybrid biometric cryptosystem for securing ðngerprint minutiae templates. *Pattern Recognition Letters*, *31*(8), 733–741.

Nagar, A., Nandakumar, K., & Jain, A. K. (2008). Securing ðngerprint template: Fuzzy vault with minutiae descriptors. In *Proc. of ICPR 2008*, pages 1–4.

Nicolas, G. (2005). Etude d'un système complet de reconnaissance d'empreintes digitales pour un microsystème à balayage. [PhD thesis] Institut National Polytechnique de Grenoble-INPG.

Ratha, N. K., Chikkerur, S., Connell, J. H., & Bolle, R. M. (n.d.). Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 29*(4), 561–572. 10.1109/TPAMI.2007.1004

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, *40*(3), 614–634. doi:10.1147/sj.403.0614

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, *40*(3), 614–634. doi:10.1147/sj.403.0614

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2007). Biometrics break-ins and band-aids. *Pattern Recognition Letters, 24(*13), pp 2105 – 2113, 2003.

Roberts, C. (2007). Biometric attack vectors and defenses. *Computers & Security*, *26*(1), 14–25.

34. Sandhya, M., & Prasad, M. V. N. K. (2017). Securing ðngerprint templates using fused structures. *IET Biometrics*, *6*(3), 173–182.

Sandhya, M., & Prasad, M. V. N. K. (2015). k-Nearest Neighborhood Structure (k-NNS) based alignment-free method for ðngerprint template protection. In *Proc. of ICB 2015*, pages 386–393.

Sandhya, M., Prasad, M. V. N. K., & Chillarige, R. R. (2016). Generating cancellable ðngerprint templates based on Delaunay triangle feature set construction. *IET Biometrics*, *5*(2), 131–139.

Sarvaiya, J., Patnaik, S., & Golklani, H. (2010). Image registration using nsct and Invariant moment. *International Journal of image Processing(IJIP),4*(2), pp.119-130.

Si, X., Feng, J., Yuan, B., & Zhou, J. (2017). Dense registration of ðngerprints. *Patt. Recogn.*, *63*, 87–101.

Soutar, C., Roberge, D., Stoianov, A., Gilroy, R., & Kumar, B. V (1998). Biometric encryption: enrollment and veriðcation procedures. In Aerospace/Defense Sensing and Controls, pages 24–35. International Society for Optics and Photonics, 1998.

Soutar, C., Roberge, D., Stoianov, A., Gilroy, R., & Kumar, B. V. (1999). *Biometric encryption*. ICSA Guide to Cryptography.

Soutar, C., Roberge, D., Stoianov, A., Gilroy, R., & Kumar, B. V. (1998). Biometric encryption using image processing. In Photonics West'98 Electronic Imaging, pp. 178–188. International Society for Optics and Photonics.

Taha, A. A., & Hanbury, A. (2015). An Efficient Algorithm for Calculating the Exact Hausdorff Distance. *IEEE Trans. on PAMI*, *37*, 2153–2163.

Tahirou D., Marc-Kokou A., & Nait, A. (2010). Caracterisation Spatiale des empreintes digitales de l'index en analyse Biométriques. Actes du CARI. Yamoussoukro, pp 501-508.

Teoh, A. B. J., & Kim, J. (2007). Secure biometric template protection in fuzzy commitment scheme. *IEICE Electronics Express*, *4*(23), 724–730.

Tomko, G. J., Soutar, C., & Schmidt, G. J. (1996). Fingerprint controlled public key cryptographic system. US Patent 5,541,994.

Tong, V. V. T., Sibert, H., Jeremy, L., & Girault, M. (2007). Biometric fuzzy extractors made practical: a proposal based on ðngercodes. In Proc. Of ICB 2007, pp 604–613. Springer.

Tran, M. H., Duong, T. N., Nguyen, D. M., & Dang, Q. H. (2017). A local feature vector for an adaptive hybrid ðngerprint matcher. In *Proc* (pp. 249–253). Of ICIC.

Wang, S., Deng, G., & Hu, J. (2017). A partial Hadamard transform approach to the design of cancelable ðngerprint templates containing binary biometric representations. *Patt. Recogn.*, *61*, 447–458.

Wang, S., & Hu, J. (2012). Alignment-free cancelable ðngerprint template design: A densely inðnite-to-one mapping (DITOM) approach. *Patt. Recogn.*, *45*(12), 4129–4137.

Wang, S., & Hu, J. (2016). A blind system identiðcation approach to cancelable ðngerprint templates. *Patt. Recogn.*, *54*, 14–22.

Wang, S., & Hu, J. (2016). A blind system identiðcation approach to cancelable ðngerprint templates. *Patt. Recogn.*, *54*, 14–22.

Wang, S., Yang, W., & Hu, J. (2017). Design of Alignment-Free Cancelable Fingerprint Templates with Zoned Minutia Pairs. *Patt. Recogn.*, *66*, 295–301.

Zannou, S. B., Djara, A., Vianou, A. (2019). Secured revocable contactless fingerprint template based on center of mass", 2019 3rd International conference on Bio-engineering for Smart Technologies(BioSMART), 2019