International Journal of Security and Privacy in Pervasive Computing
Volume 14 • Issue 1

Non-Contact Fingerprint Template Protection Using DFT Combined Random Projection

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

ABSTRACT

In view of the different dangers to which users of contactless biometric systems are exposed, the authors have developed a contactless secure revocable model based on random projection and DFT (Discrete Fourier Transformation) to enhance contactless fingerprint authentication. Two matrices emerge, namely corresponding to the terminations and corresponding to the bifurcations. These matrices are then transformed in a first time thanks to the random projection. In a second time, they apply to them the Discrete Fourier Transformation called the DFT. This proposed non-contact revocable fingerprint model meets the requirements of revocability, diversity, security, and non-reversibility. The evaluation of the model through its results gives the most promising results compared to those existing. The equal error rate (EER) obtained is respectively equal to 0.19% for FVC2002 DB1, 1% for FVC2002 DB2, 4.29% for FVC2002 DB3, and 9.01% for FVC2004 DB2.

KEYWORDS

Cancelable, DFT, Non-Contact, Projection, Random, Security

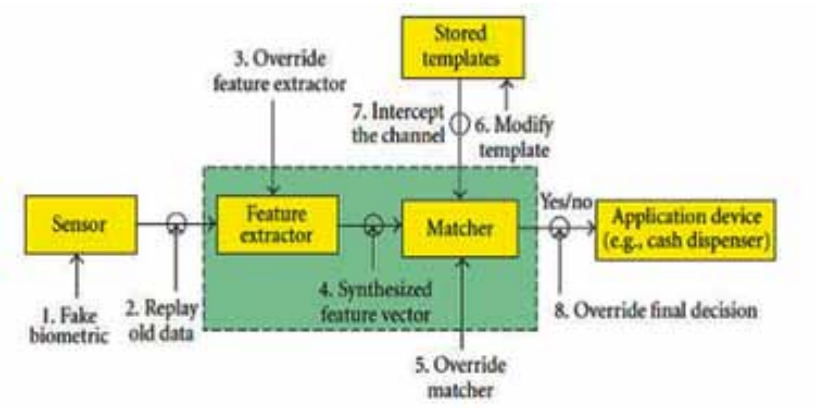
INTRODUCTION

Biometric authentication systems are increasingly being used extensively as part of the manifestation of identity and access control. It is based on the physiological characteristics that can be measured (signature, fingerprint, gait, strike, ...) of a human being. For a long time it has been used in sensitive systems passwords or tokens to allow users to authenticate. Generically, the biometric application is composed of: a) a sensor unit for recovering the non-contact image, b) generating a feature vector after the image acquisition from the contactless sensors in the module feature extraction, c) Storing extracted features in a database, d) Comparison module to check whether the stored characteristics match those of the user, e) a decision-making module for authorizing or not the access.

The most widely used biometric modality in many human authentication systems is the fingerprint as it offers both unnoticed and high performance. Compared to these modalities, the munities are the most appreciated representation. Unfortunately, many studies have shown that the original fingerprint could be based on sensitive information, which puts the fingerprint security debate back on the map. (Patel & Ratha, 2015) listed several levels of perpetrator attacks against a biometric authentication application that we illustrated in Figure 1. i) falsified biometric features such as a manufactured

DOI: 10.4018/IJSPPC.302007 *Corresponding Author

Figure 1. Weakness point in a biometric system



finger that can be presented to the image cipher unit, 2i) fraudulently captured mage submission to the system, 3i) a trojan horse program illegally presented to the device. extraction of characteristics to prefabricate features, 4i) false functions can be used to substitute for real functions, 5i) In order to bypass the system, illegal troop programs are used in the comparison module in order to produce a high score, 6i) can transform or revoke models stored in the database, 7i) in the communication channel between non-identical modules can intercept and transformed or the adaptation module overwritten. Several techniques work for the protection of data as presented by (Balasubramanian & Selv Kumar, 2014). Despite the fact that every day is a day of data protection, diversity and uniqueness performance is struggling to be achieved, preventing the user from authenticating to multiple applications with a single biometric model. The solution that achieves diversity and allows a user to register on multiple applications with the same model is revocable biometrics. (Jain &Nandakumar, 2008) proposed three main categorizations of approaches to protect biometric models, namely: cryptosystems, characteristic transformations and hybrid forms. All these methods each have their shortfall presented by (Rathgeb & Uhl,2011) and do not exactly meet the four main requirements of a perfect protection model. Our option in this article is the transformation of characteristics The fundamental idea of the functional transformation approaches is to transform the model by applying a modification function H of the original biometric model M and helped by a key C; The new model obtained H (M, C) is therefore stored in the storage module. We also use to generate the comparison model Q the function F. H(M, C) and H(Q, C) are then directly matched in the comparison module in order to decide whether the user is the correct one or not. Our proposed new approach is a non-invertible transformation for minute-based models (points of interest is the basis of this approach), which provide diversity, revocability, security and performance. Beyond all this, and in opposition to the other protection schemes of fingerprint models, our model is insensitive to the rigid transformations of fingerprint prints. Faced with the security threats that remain during the matching of fingerprints through the threats of confidentiality and protection, it urgently urges that suitable solutions be found to ensure security in biometric systems. The most virulent threats are brute force attacks and replay attacks used to stop the functioning of databases. Securing the client model, which is stored in a single shipment, remains a concern. We therefore want to refine the principles of revocability, security in the storage mode of the client model. The contactless model chosen in this article makes it possible to limit the possibilities of reproducing the fingerprint because our system does not leave any trace on the sensor at acquisition therefore this model limits the possibilities of reproduction. Our contribution is to build a non-reversible transformation that meets the requirements of revocability, diversity, security and performance. In the rest of this paper, section 2 presents our introduction, section 3 will present the acquisition of contactless fingerprint images and its processing, section 4 gives an introduction to

the basics of DFT and projection techniques random, section 5 describes the technique proposed to extract the revocable fingerprint model, an overview of the full analysis of the results will be given in section 6 and then we will conclude and give the perspectives in section 7

INTRODUCTION TO CONTACTLESS FINGERPRINT ACQUISITION

The need to identify human reliably has always been a major difficulty. The failure of the usual methods of identification (smart card, password ...) pushed men to seek other solutions. Biometric methods have therefore positioned themselves as a credible alternative. in general, two categories of fingerprint recognition algorithms have been identified throughout the literature. i) the first group of algorithms which are based on the relative position of the minutiae between them. This approach is indicated by the authors in [Jain & Hong, 1997;Djara & Vianou, 2009) and used by other authors in (Galy, 2005; Djara & Vianou, 2009). Directional filtering and binarization applied to the fingerprint image is successively performed as follows: the thinning (or skeletonization) of the grooves, then the arrangement on the image is evaluated with a view to lowering the characteristics of similarity between two templates by patterns. ii) the second category gathers the algorithms aiming to extract other particularities from these images like the local direction of the grooves as described by (Halici &Orguin,1996; Djara & Vianou) and (Capelli & Lumini, 1999; Djara & Vianou), the texture at the heart of the image to through the local frequency components. The author's proposal should be underlined by (Maio & Maltoni,1998; Djara & Vianou,2009). This solution makes it possible to locate the minutiae directly by using neural networks. In order to raise the robustness of systems based on fingerprints, the authors proposed to extract the minutiae on the entire finger by choosing to look at the case of the index. Using a segmentation technique, they proposed a new technique consisting in extracting the striations and the central line (1_c) from the striations by skeletonization. These authors identify and characterize the bifurcation and termination points on the l_c. in the next sub-section, we will characterize the minutiae by their parameter.

Spatial Characterization of the Minutiae by Their Parameter

The extraction of the fundamental characteristics of contactless fingerprint images has been explained in (Djara et al, 2009) by some researchers. Let us consider two sets of minutiae Ω_1 and Ω_2 , extracted from the age of contactless fingerprinting.

($\propto$) The set Ω_1 :

This grouping of minutiae is obtained by detecting and validating the final minutiae.

- (u_i, v_i) corresponds to the coordinates of the position of the termination in the fingerprint image;
- The angle of orientation φ_i is linked to the outgoing branch of the point.

$$\Omega_1 = \{\Psi_i = (u_i, v_i, \varphi_i);\ i \in [1 \ldots \in]\} \quad (1)$$

The number of terminations detected and validated is $\in$.

β The Set Ω_2 :

Bifurcations detected and validated are regrouping in this set. So for each bifurcation, two characteristics are extracted:

- The coordinates (u_j, v_j) of the bifurcation point
- The three angles $\varphi_{1j}, \varphi_{2j}, and \varphi_{3j}$ as shown in figure 3.

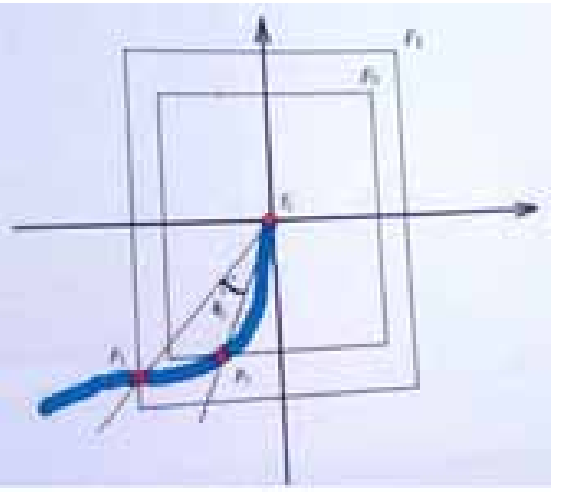
$$\Omega_2 = \{A_j = u_j, v_j, \varphi_{1j}, \varphi_{2j}, and \varphi_{3j}); j \in [1...\sigma] \quad (2)$$

σ is the number of bifurcations detected and validated.(Djara et al, 2009). In the next sub-section, we will deal with the bifurcation branches.

Bifurcation Branches Orientation

The relative angles of the three branches constitute the vicinity of a bifurcation point. These angles constitute the parameters for spatial characterization of the bifurcation. The authors in (Dara et al, 2009) have centered a window W of size m x m. We can observe three points Q_1, Q_2, Q_3 with respective coordinates: (u_1, v_1), (u_2, v_2), (u_3, v_3) branch intersection with W on the perimeter of the window. They used a 13x13 window.

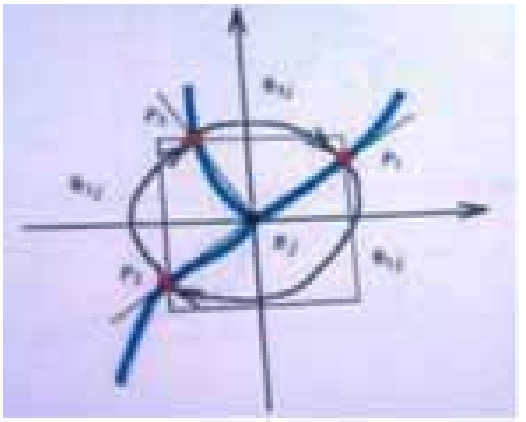
Figure 2. Determination of the termination angle (Djara et al, 2009)



This is dependent on the minimum length of a branch. They selected for a minimum branch length of 15 pixels after several experimental tests. To get around the difficulty of ending up with a window that does not exactly coincide with the branches during its larger size has this minimum length, it would then be necessary that the window size be corresponding to this minimum length. To determine the angles $\varphi_{1j}, \varphi_{2j}, \varphi_{3j}$ between the branches, you will have to apply the formulas (3), (4), (5) (see Figure 3).

$$\varphi_{1j} = Arccos\left(\frac{\overrightarrow{B_jP_1}.\overrightarrow{B_jP_2}}{B_jP_1 \times B_jP_2}\right) \quad (3)$$

Figure 3. Determination of the bifurcation angle [26]



$$\varphi_{2j} = Arccos\left(\frac{\overrightarrow{B_jP_2}.\overrightarrow{B_jP_3}}{B_jP_2 \times B_jP_3}\right) \tag{4}$$

$$\varphi_{3j} = Arccos\left(\frac{\overrightarrow{B_jP_3}.\overrightarrow{B_jP_1}}{B_jP_3 \times B_jP_1}\right) \tag{5}$$

B_j is the jth bifurcation point.

In short, the M bifurcation points are associated with a matrix made up of M rows and 5 columns (6). Each bifurcation point is symbolized by a rank in the matrix and the columns represent respectively the coordinates of the point and the angles which the branches make between them.

$$\boldsymbol{v}_{b1} = \begin{pmatrix} u_1 & v_1 & \varphi_{11}\varphi_{21}\varphi_{31} \\ u_2 & v_2 & \varphi_{12}\varphi_{22}\varphi_{32} \\ \cdots & \cdots & \cdots\cdots\cdots \\ u_M & v_M & \varphi_{1M}\varphi_{2M}\varphi_{3M} \end{pmatrix} \tag{6}$$

Next section, we will deal with angles terminal branches orientation.

Orientation Angles of Terminal Branches

It will be a question of considering two concentric windows (F_0,F_1)of the end point T_i. F_0 is the size n*n and F_1 is the size m*m with n < m. Along the circumference of the window F_0. Thus, along the perimeter of F_1, there is a point of intercession of the branch with F_1. We thus consider θ_j as the termination angle. All this is shown in figure 2.

The determination of this angle is done by applying the formula (7)

$$\varphi_i = Arccos\left(\frac{\overrightarrow{T_iP_0}.\overrightarrow{T_iP_1}}{T_iP_0 \times T_iP_1}\right) \tag{7}$$

In short, a matrix with N lines and 3 columns (8) corresponds to the N terminal points. Each termination is represented by a line the coordinates of the point and the angle of the branch are represented respectively at the termination and the columns.

$$\boldsymbol{v}_{b2} = \begin{pmatrix} u_1 & v_1 & \varphi_1 \\ u_2 & v_2 & \varphi_2 \\ \cdots & \cdots & \cdots \\ u_N & v_N & \varphi_N \end{pmatrix} \tag{8}$$ (Djara et al, 2009)

To make a summary, all the points can be represented by: M = $\left\{m_i\right\}_{i=1}^{N}$ whith $m_i = (u_j, v_i, \varphi_i, t_i)$ where N is the number of characteristic points, u_i, v_i are the u, v coordinates of the ith minutia, φ_i is orientation of the i^{th} minutia and t_i is the minutia type.

Since we have already described what are contactless fingerprint template and his usage for authentication, we will go through the state of the art in next section.

LITERATURE REVIEW

Generally classified as revocable biometrics (Ratha et al, 2007) 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 mytec (Tomko et al, 1996) and then this version evolved to become Mytec2 (Soutar et al, 1998), (Soutar et al, 1999). Their solutions are based on the correlation that proved to be insoluble in the sense of accuracy and security. Juels and Wattenberg (Juel et al,1999) have suggested their solution in order to achieve a cryptographic type by combining several techniques in the field of error-correcting codes and cryptography. The authors proposed in 'B.Teoh et al, 2007) a randomized dynamic quantization transformation to be applied to the characteristics of fingerprints extracted from a multi-channel Gabor filter so that they are binary. Following this, a scheme called Fingercode in which a fuzzy extractor based on a stable and ordered non-variable representation of biometric data is proposed by the authors in (T. Tong et al, 2007). Later, other authors in (Wang et al, 2016) have dimensioned the fuzzy vault system, in which the majority of the chaff points are augmented with the original data points so that the impostor cannot recognize the original data points from a safe. A fuzzy vault system that locks the points of minutiae called the "fingerprint vault" has been proposed by the authors in (A. Nagaret al, 2008)). Others in (A. Nagar et al, 2010), (E. Boult et al, 2007) have proposed a fuzzy vault based on improved security. They used the orientation of the points of detail. Other authors such as Ratha et al. have instead introduced revocable biometrics using non-invertible transformations of user characteristics. The authors in (D. Ahn et al, 2007) refined and combined encryption and feature transformation to provide the popular known user model called betoken biotop. As a first step some authors in (Wang et al, 2012) suggested a property transmutation approach based on the production of triplets starting from the minutiae of fingerprint characteristics. Other authors

have harmonised the symmetric hash function for k-triplets of a minutiae. This solution proved to be robust against multiple attacks; unfortunately its identification prowess has declined. 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 H. et al, 2013) suggest a device to identify a customer according to his position using radio frequency identification (RFID) systems. Some authors in (Sadhya 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 (E. Derman et al, 2016). 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 (Sadhya 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 (Sadhya 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 (Htran et al, 2017). An alignment free framework has been proposed by Wang and Hu (Wang et al, 2019) through the use of the non-invertible transformation for securing the templates that are cancelable. Another alignment invariant technique based on minutiae triplet is designed by Ahn et al. (Ahn et al, 2008). Tran et al. (Tran et al, 2017) have designed a method based on hybrid matcher for user authentication. Wang et al. (Wang S. et al, 2017)) used zoned minutia pair for local minutiae structure to design a scheme that computes cancelable user template. Boult et al. (Boult et al, 2007) have introduced Biotop biotoken, which are generated through encryption of user data. The fingerprint image is enhanced by Khan et al. in (Khan et al, 2017) by using anisotropic Gaussian. Ali et al. in (Ali et al, 2019) designed a technique in which secured fingerprint features are used, which has been further enhanced in (Ali et al, 2020). Ali et al. (Ali S et al, 2010) have designed a secure 3-dimensional secured user template through the relocation of minutiae points. The fingerprint features used are the translation/rotation variant.

Ali et al. (Ali S. et al 2019) have proposed Polynomial Vault, in which they used polynomial functions and the fingerprint to generate a polynomial function which is treated a user template. In this technique, all the minutiae points of a fingerprint are used, due to which it is not optimized. Fingerprint shell (Moujahdi et, 2014) has been introduced by Moujahdi et al., in this technique, the template computed has a 2D shell shape structure. Based on (Moujahdi et al), Ali and Prakash (Ali et al, 2015) proposed a technique with better recognition performance. However, features of a fingerprint are insecure in Fingerprint Shell (Lee S. et al, 2020), Ali et al. (Ali S. et al, 2019) designed a secure version of (Moujahdi et al, 2014) which was a 3D fingerprint shell and was much more secure than the 2D fingerprint shell (Moujahdi et al, 2014). It is observed that the ridge count for different minutiae points (with respect to the singular point) is found to be different. Ali et al. used it in (Ali S. et al, 2019) and added high randomness to the generated user template. The present frameworks for fingerprint-based biometrics are generally insecure and unoptimized. In some techniques, it is even possible to obtain the original biometric features information from the user template (Ali S. et al, 2019; Moujahdi et al, 2014). Apart from security, the available techniques usually use all the minutiae points for the template generation, leading to an unoptimized user template that makes the authentication system slow. Hence, in the proposed technique we have generated a highly robust and irreversible template for a user. The template generated by the proposed technique is a 3D shell and hence much stronger than a 2D fingerprint shell (Ali S. et al, 2019; Moujahdi et al, 2014). With other attributes of minutiae points of a fingerprint, we have used the quality of minutia point as well, leading

to a highly secure and optimized user template. As only good-quality minutiae points (with better ridge termination or bifurcation (Ali S et al, 2019) are used, this makes the authentication system much faster. In case adversary gets the user template generated by the proposed technique, then it is not possible (computationally very hard) for the adversary to obtain the original fingerprint of a user from it; and the compromised user template can be easily replaced with a new template (very different from the compromised template) by changing the user keys.

INTRODUCTION TO DFT AND RANDOM PROJECTION

In this chapter, we will explain what is DFT and Random projection before use it for construction of our template.

DFT

Either a binary fingerprint sample (, C), translated by equation (9), indicating the binary biometric representation obtained from the fingerprints before transformation.

$$\boldsymbol{w_{bi}} = [C_i(0), C_i(1), ..., C_i(m-1)^X \tag{9}$$

where C(i) $\in$ {0,1}; and i ranges from 0 to (m-1), m representing the size of the template. Since $\mathrm{w_b}$ contains sensitive information relating to biometric characteristics, it must be secured. Since it is in binary form, it is possible to reduce the search space (during the revocable template inversion operation), especially when the y $\mathrm{b_i}$ elements are distributed in a non-uniform and scattered manner. Thus, the DFT could be applied to $\mathrm{w_{bi}}$ before the random projection is applied to it, so that a dense representation of the data is obtained at the end. We now take N-point DFT of $\mathrm{v_b}$ as shown in (10).

$$\boldsymbol{w_{Bi}} = M\boldsymbol{w_{bi}} \tag{10}$$

where M is a DFT matrix as shown in (11), and $N = 2^n$ and $\mathrm{N} \geq \mathrm{m}$. The value of $\mathrm{w_B}$ can be represented as shown in (11).

$$F = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & g & g^2 & \cdots & g^{(N-1)} \\ 1 & g^2 & g^4 & \cdots & g^{2(N-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & g^{(N-1)} & g^{2(N-1)} & \cdots & g^{(N-1)(N-1)} \end{bmatrix} \tag{11}$$

$$\boldsymbol{w_B} = [D(0), D(1), ...D(m-1)]^X \tag{12}$$

where $g = \exp(-j2\pi/N)$. The DFT matrix is a unitary matrix and the DFT operation is highly invertible. It is to be noted that purpose of taking DFT is just to scatter the sparsely distributed values of $\mathrm{w_{bi}}$.

Random Projection Technique

The Johnson-Lindenstrauss (JL) Lemma (Johnson &Lindenstrauss, 1984) and (Bingham & Maltoni, 2001) basically states that a set of points P in a higher-dimensional Euclidean space $\Re^N$ can be embedded into a lower-dimensional Euclidean space In such that the pair-wise distance of any two points is maintained approximately. The JL lemma is given as:

Let $\varepsilon \in (0,1)$ be given. For every set P of #(P) points in $\Re^N$, if n is a positive integer such that,

$$n > n_0 = o\left(\frac{\ln\left(\#\left(\mathrm{P}\right)\right)}{\mu^2}\right) \tag{13}$$

Then it can be concluded from equation (5), that there exists a Lipschitz mapping *f*: $\Re^N \rightarrow \Re^n$ such that

$$\left(1-\boldsymbol{\mu}\right)\boldsymbol{x}-\boldsymbol{y}^2 \leq \boldsymbol{f}\left(\boldsymbol{x}\right)-\boldsymbol{f}\left(\boldsymbol{y}\right)^2 \leq \left(1+\boldsymbol{\mu}\right)\boldsymbol{x}-\boldsymbol{y}^2 \tag{14}$$

for all $x, y \in P$.

The function *f* is a linear mapping represented by $k \times d$ matrix ψ which has its components drawn randomly from specific probability distributions. Hence it is clear that the statistical characteristics required for recognition can be preserved even while changing the original form of the data. The matrices which satisfy (14) for any given set of points P are as follows (provided n satisfies the condition of JL lemma):

a) The entries $\psi_{i,j}$ of Ψ are realizations of independent Gaussian random variables;
b) The entries $\psi_{i,j}$ of Ψ are realizations of ± 1 Bernoulli random variables with a probability of 0.5;
c) The entries $\psi_{i,j}$ of Ψ are realizations of related distributions including values of $\pm\sqrt{3}$ (each with a probability of 0.167) and 0 (with a probability of 0.67);

All the three matrices have proved to provide successful projection matrices which end up in similar results. But we have used Gaussian projections in our experiments. The process of projecting the binary biometric representation v_B on random matrix Ψ is defined as:

$$T_B(d \times N) = \psi(d \times k) v_B(k \times N) \tag{15}$$

The pair-wise distances between the vectors must be preserved before and after transformation. The extent of preservation of pair-wise distances between the vectors highly depends upon the projection vectors $\omega_i \in \Psi$. According to JL lemma, the critical property of the random projection matrix is that its column vectors ω_i must be orthogonal to each other. This can be achieved by using Gram Schmidt orthogonalization technique. But this technique increases the computational complexity to a great magnitude.

Several measures have been proposed to reduce the computational complexity. (Har-pele & Indyk, 2012) have reported that the condition of orthogonally must be eliminated while using random projections to approximate nearest-neighbor in Euclidean space of higher dimension. As an extension

to proof, they used a random projection matrix whose column entries are independent random variables with Gaussian distribution. The projection of such a matrix has possesses chi-square distribution with *k*-degrees of freedom. Further the tail estimates for this distribution can be used to prove that the pair-wise distance between any two points is not distorted by a factor more than $(1 \pm \sigma, \text{ where } 0<\sigma<1)$. Hence it is clear that a random projection matrix whose elements are normally distributed preserve the pair-wise distance between vectors even after transformation. This reduces the computational complexity of generating random matrix since the orthogonality condition is dropped.

PROPOSED SYSTEM FOR GENERATION OF COMPLEX CONTACTLESS CANCELABLE FINGERPRINT TEMPLATE

In this section we will use the DFT and random projection to build our complexe contactless cancelable fingerprint template.

Generation of Contactless Binary Fingerprint Template

The input fingerprint image from sensor is pre-processed using enhancement and binarization techniques. Then the binarized image is subjected to thinning process so that the ridges become one pixel wide. The ridges are thin curved lines in fingerprint, which may bifurcate or terminate. These bifurcations and terminations are called minutia. Each and every fingerprint has about 70-150 minutia points. Let E_1 and E_2 be two sets of minutiae.

(a) The set E_1:

This set gathers the terminating minutiae detected and validated. For each termination, two characteristics are extracted:

- The position of the termination in the image: coordinates (u_i, v_i),
- Orientation θ_j linked to the outgoing branch of the point as shown in Figure 2.

$E_1 = \{T_i = (u_i, v_i, \varphi = [C_i(0), C_i(1), \ldots, C_i(m-1)^X{}_i)\ i \in [1 \ldots N]\}$
N is the number of terminations detected and validated.

(b) The set E_2:

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

- The coordinates (u_j, v_j) the bifurcation point
- The three angles φ_{1j}, φ_{2j} et φ_{3j} as shown in Figure 3.

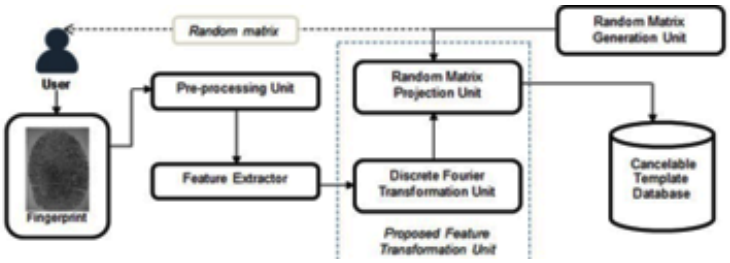
$E_2 = \{B_j = (u_j, v_j, \varphi_{1j}, \varphi_{2j}, \varphi_{3j})\ ; j \in [1 \ldots M]\}$

M is the number of bifurcations detected and validated. Here, u_i and v_i, φ_i ranging from [0,2 π], and φ represent the position, the orientation, and the type of minutiae (bifurcation or termination), respectively. The binary fingerprint template (v_b) is generated using these minutia points as shown in (Wang et al, 2014).

System Model Using Proposed Technique

Enrolment and verification are the two processes suggested by our template through the following biometric scheme (Figure 4)

Figure 4: Determination of bifurcation angles (Djara etal,2009)



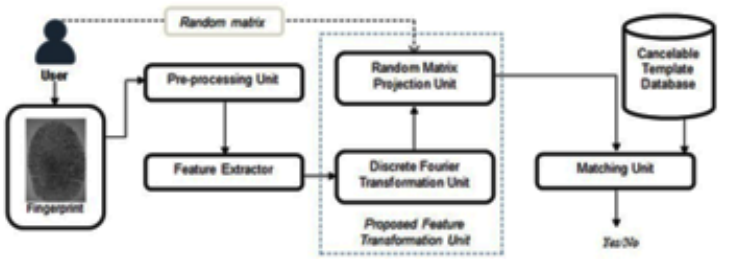
The proposed technique allows a revocable model to be generated from a binary fingerprint to obtain a non-contact revocable specimen, which can be modeled mathematically with reference to our proposed system (using equations (16), (17) and (18)) as below:

$$Q_{Bi} = \Psi M w_{bi} \tag{16}$$

In short, the generation of the revocable contactless fingerprint template is generated by applying the extracted characteristics to the FTD. To check the accuracy of the customer (in the transformation domain) we transform a query binary fingerprint template (say Q_q) into querry contactless cancelable fingerprint template (say Q_q) using equation (17). To confirm the binary matching of the samples, the distance Q_B and Q_q (L(Q_B, Q_q)) will have to be calculated so that:

$$\mathrm{L}\left(\mathrm{Q_B},\ \mathrm{Q_q}\right) = \frac{\mathrm{l}\left(Q_{\mathrm{B}},\ Q_{\mathrm{q}}\right)}{\left(\mathrm{w}(\mathrm{Q_B}) - \ \mathrm{w}\left(Q_{\mathrm{q}}\right)\right)} \tag{17}$$

Figure 5. Block Diagram of Proposed Technique (Enrolment Phase)



$$\mathrm{R} = \begin{cases} 1, L\left(\mathrm{Q}_{\mathrm{B}},\ \mathrm{Q}_{\mathrm{q}}\right) < Q \\ 0, otherwise \end{cases} \tag{18}$$

where Q is a predefined threshold. Equation (18) gives the value of *L*. If R=1 then the templates and as represented by Equation (10).

We choose the binary fingerprint template, DFT matrix and random matrix with the same dimension for convenience.

Process Stages Implied in The Suggested Approach

The entry data in the proposed system corresponds to the characteristics extracted from the user's fingerprint. The phases implied in the registration step and the checking stages are outlined below.

ü **Stages entailed in the registration round:**

1. Generation of N-point DFT of R_{Bi} from DFT unit based on equation (10) and result is R_{Bi}

Stage 2: Generation of Ω using Random transformation units

2. The projection of Ω on R_{Bi} stands for random projection unit which acts as feature transformation unit.
3. T_{B} is kept in the databank.
4. For verification sake, we give the random matrix to the user.

ü **Verification Stages**

1. Generation of N-point DFT of w_{bi} using DFT unity
2. The projection of Ω (entered by client) by the functionality transformation unit on R_{Bi}, and produces a query model called Q_{qi}
3. Correspondence between Q_{Bi} and Q_{qi} based on equation (10) and a decision (yes/no) is made as to whether or not it is the client

Comparison of Fingerprints in the Transformed Domain

In order to protect the original features of the fingerprints in the transformation domain, the fingerprint comparison for revocable data in the transformation domain is performed. Therefore a fingerprint authentication request is evaluated through identical identification procedures, i.e. the extraction and subsequent transformation of the characteristics of the fingerprint model. In other words, the contactless fingerprint models are constructed from equation (10), followed by quantification and modulo (3) operation. The partial FFT (17) is then applied to the binary vector. Let us choose the letter "t" and "q" as a subscript to distinguish the model from the query for clarity.

RESULTS AND DISCUSSIONS

Image Dataset

We evaluated our proposed model against several other publicly available and usable databases such as DB1 and DB2 from FVC2002 and FVC 2004. All available information is presented in Table 1. We used MATLAB R2015a. Tests for authenticity and deception were conducted on all four databases. We used the first image of each finger from each database was used as a reference image. The query is assimilated with every second image from the database. Thus, we had 199 original scores and ((100*99)/2) =4950 perpetrator scores for each database.

Table 1. Details of the datasets used in experimentation

Details	FVC2002 DB1	FVC2002 DB2	FVC2004 DB1	FVC2004 DB2
No. of fingers	100	100	100	100
No. of images of each finger	8	8	8	8
Size of image	388×374	296×560	640×480	328×364
Image format	Tagged Image File Format	Tagged Image File Format	Tagged Image File Format	Tagged Image File Format

Complexity Analysis

The reduction of the complexity of our technique has been achieved through the use of DFT and random projection. Let's consider O(.), the computational complexity of an algorithm. Our method takes into account a DFT with N points and a random projection. The (Proaski & Manolaski, 1996) Radix-2FFT algorithm allows the implementation of N-point FFT. We evaluate the Radix-2FFT algorithm at a complexity of O((ln(N))/Nln2). We estimate the computational complexity of the random projection at O((k-1)dN) and the overall complexity is evaluated at O[N((ln(N))/(ln(2))+kd)] In view of the above we can conclude that the low computational complexity of our model gives it the properties of being suitable for devices with limited memory and power such as mobile phones.

Matching-Performance Analysis

We evaluate performance through the calculation of the error rate (EER) which is evaluated as a function of the false reject rate (FRR) and the false acceptance percentage (FAR). These different percentages are used to evaluate the matching performance of the original and transformed specimens. We calculate the FRR and the FAR respectively using equations (19) and (20).

$$FRR=(\text{Number of failed rejections})/(\text{Number of legitimate access attempts})\times 100 \quad (19)$$

$$FAR=(\text{Number of false acceptances})/(\text{Number of imposter attempts})\times 100 \quad (20)$$

FRR=1-GAR

We match the evaluated FRR with the same specimens stored in the database for an extracted feature packet. To evaluate the FAR, a revocable fingerprint specimen is compared with all specimens in the database. We equate the ERR to the error trade-off between FAR and FRR, which means that FAR and FRR are agitated from a threshold value. The inverse proportional to the ERR value indicates the performance of the system. By comparing the EER of a model transformed by (Wang & Hu, 2016; Jin & Hu, 2014)) with that of the revocable contactless fingerprint models, the EER of the contactless fingerprint models is more efficient and better. In order to generate revocable fingerprint models transformed into binary format, we used a Hamming integration technique based on a randomized graph. In order to produce a complex vector fingerprint model, a blind identification system was introduced by (Wang & Hu, 2016). Table 2 presents the comparative results.

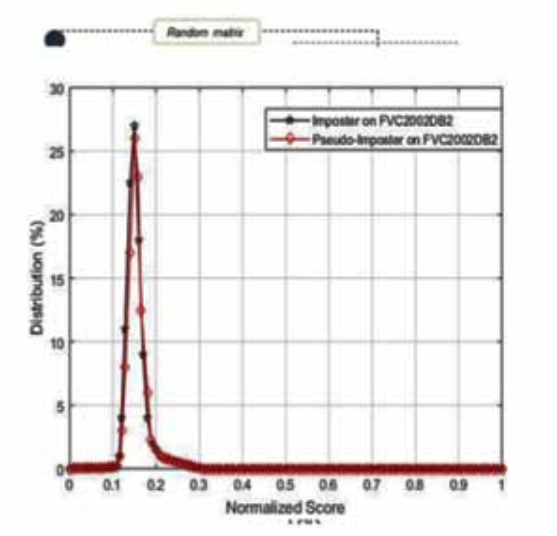
Table 2. EER (%) Comparison

Methods	FVC2002 DB1	FVC2002 DB2	FVC2004 DB1	FVC2004 DB2
(Jin, Lim, Teoh, and Goi, 2014)	4.36	1.77	-	21.82
(Wang, and Hu, 2016)	3	2	-	-
Proposed System	1.25	2.54	8.62	12.28

Non-Invertibility Analysis

An important property of revocable biometric systems that ensures the transformation applied is one-sided is inversibility. Indeed, the transformation must not be reversible. In other words, the specimen obtained after T_{Bi} transformation must not provide the information of the original binary V_{Bi} specimen. Let us suppose that the T_{BI} matrix and the random V_{Bi} matrix have been stolen by a forger, i.e. the malicious person tries by all means to identify the transformation process and to find the original biometric characteristics from the clues he has in his possession. Since our specimen offers in this sense almost indeterminate solutions, as presented by (Wang & Hu, 2012) infinity of solutions to V_{Bi} is thus offered. The possibility of recovering the original binary biometric properties is too thin. Figures (3-a) and (3-b) show the receiver operating characteristic (ROC) for each data set in the stolen take scenario. We compare the OCR of the non-contact revocable fingerprint specimen (post-processing) with that of the original model (pre-processing). We can clearly observe the similarity of the specimen recognition performance for the FVC2002 DB1 and DB2 databases, while they are not at all similar for the FVC2002-2004 DB1 and DB2 databases due to the poor image quality.

Figure 6. ROC curves for FVC2002 DB1, DBs2, DB3 and FVC 2004 DB2 in the lost-key scenario



Diversity Analysis

From each database, different revocable specimens (e.g. T_1 and T_2) were obtained using the random matrices. We then evaluate the correlation (Δ) between each pair of revocable models based on equation (22). Let us call the correlation index (Δ') the average of all the values from $\boldsymbol{\delta}$ that correspond to the revocable patterns generated by each respective fingerprint. The $\boldsymbol{\delta}$' values for the revocable patterns for each CVF database have been stored in Table 3. It should be noted that two different specimens extracted from the same fingerprint sample using different random matrices share 0.22% of the mutual information and all this is possible when $\boldsymbol{\delta}$'=0.0021

$$\delta\left(T_1, T_2\right) = \frac{T_1\bar{T}_2 + \bar{T}_1 T_2}{\| T_1 \|_2 + \left\| T_2 \right\|_2} \tag{22}$$

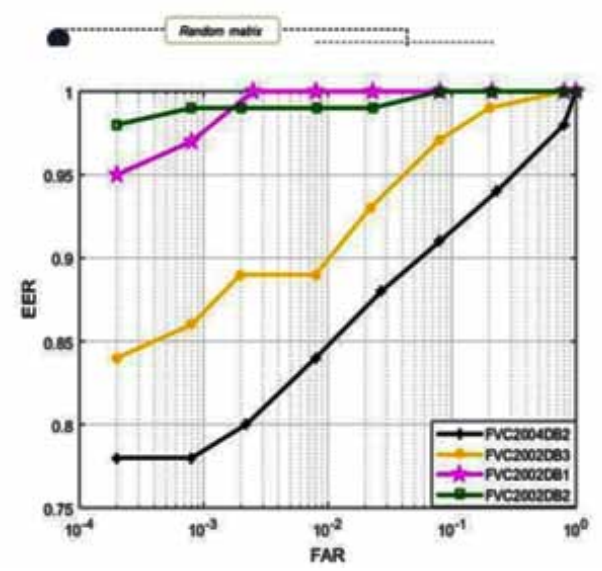
Table 3. Correlation Coefficients of Templates

Database	Δ
FVC2002 DB1	0.0021
FVC2002 DB2	0.0023
FVC2004 DB1	0.0018
FVC2004 DB2	0.0024

Revocability and Diversity

Revocable biometric data have a sine qua non property which is revocability. When a stored template is overwritten, it is important that the old template is deleted and a new template is generated to succeed the old one so that there is no match between the old and new template despite the fact that it is from the same fingerprint. It should be noted that diversity is closely related to revocability. By the concept of diversity it should be understood that no matter how many transformed models are derived from the same fingerprint, there should be no correlation between the new and the old model. In order to evaluate the difference from the old one and same fingerprint, we conduct the revocability and diversity tests to measure their correlation. A total of 51 transformed models were generated from a single fingerprint image of each finger in FVC2002 DB2 using keys of different parameters. We compared these pseudo-print templates to the original specimen. We present a distribution of malware by contrasting it with the distribution of clients when each user in our database has a different key. It is clear that the malware distribution is very close to the client distribution. The mean and standard derivation of the malware distribution are 0.1540 and 0.1499 (mean) and 0.0165 (standard derivation) respectively of the distribution of imposters. We notice through these results that the newly generated models have no link with the compromised model and present a difference between them (one from the other) as they come from the same fingerprint.

Figure 7. Pseudo-imposter and imposter distributions for FVC2002 DB2



Security Analysis

Since data from contactless fingerprints (the minutiae matrix) is very sensitive information, we need to protect it with our technique for securing fingerprint templates. Protecting E_i means protecting the binary string $\left\{\overline{d_c(\alpha)}\right\}_{\alpha=0}^{\overline{s-1}}$ where 1 represents the quantized E_i. Our suggested technique provides enhanced security on two levels. We ensure the security of the first layer by decreasing the length of $\left\{\overline{d_c(\alpha)}\right\}_{\alpha=0}^{\overline{s}-1}$ using modular arithmetic (3), with a shortened binary uncertainty increase $\left\{\overline{d_a(\alpha)}\right\}_{\alpha=0}^{\overline{s}-1}$. Thus the entries of $\left\{\overline{d_a(\alpha)}\right\}_{\alpha=0}^{\overline{s}-1}$ would be due to the event that the starting value is either due to the modular exercise or both as analyzed in section III.1. Thus this first layer of protection helps to drastically reduce ARM risks. Changing the S parameter will cause $\left\{\overline{d_a(\alpha)}\right\}_{\alpha=0}^{\overline{s}-1}$ or similarly $\overline{d}_a$ in (4) to vary from one application to another. Since b is the input of the partial DFT, if b_c is different in different applications, it would be totally useless for a malicious person to collect several revocable samples h in order to launch ARM attacks, because ARM would only work if the same value of b was used in all target applications. The FTD (10) constitutes in itself the second layer of security set in motion by the proposed technology and involves a sub-determined set of linear equations. Since the partial DFT matrix M in (10) is of full row but deficient column row, nullity(M)=N - row(M)=N - Y (10). Is also a solution (10), any vector of the form d_α + f provided that it belongs to the null space of M and there is an infinity of solution for f. On the other hand, in this situation, the solutions are not infinite but rather they are always numerous. This is demonstrated by doing an analysis of the solutions of the under-determined system (10) taking into account the number of basic (or fixed) variables and the number of free variables. Given that rank(M)=Y, there are R fixed variables and (N-Y) free variables for (10) we can express the system solution as fixed variables for (10) and we can express the fixed solution of the system with respect to the free variables. Consider a single binary vector, e.g. b_c, can be indicated for the solution of (17), contrasting it with vectors whose values are real or complex, the free (N-Y) values can take values of 0 or 1. We then have 2N-Y possibilities for b_c, between which the real b_c solution. Let's take a look, for example, at some of the values we have experienced. For example, let's take N=214 and Y=800 and we get 2N-Y=215584, proof that it is very unlikely to succeed in finding the true solution d_α among 215584 possible binary value solutions, even if k_α and M in (17) are both known.

CONCLUSION

We have suggested a random projection-based approach by designing non-contact revocable fingerprint specimens based on complex biometric templates applied to the non-contact fingerprint specimen. These sample fingerprint features are sometimes very difficult to find. The method developed is very robust. Thus in such cases, the DFT extends the spectrum and sufficiently reduces the dispersion. The specific properties of robust fingerprint transformations have been achieved by our revocable non-contact fingerprint specimen, namely revocability, diversity, non-invertibility and comparison performance. An approach based on the application of binary biometric feature transformation functions. The next challenge therefore remains on the IT side and especially for systems with low memory capacity such as smart phones. This is a significant advance compared to other revocable models that are vulnerable to ARM attacks (Djara et al, 2009). Evaluating our new model compared to the FVC2002 DB1, DB2 and DB3 and FVC2004 DB2 models, it appears that the new method offers better performance than those presented in the state of the art. The installation of a revocable and secure non-contact model requires intense work especially against ARMs, especially when it requires a reduction in dimensions. More robust techniques are needed to enable contactless biometrics to truly combat ARM attacks. The use of polynomial vaulting techniques seems to indicate promising and more robust avenues.

FUNDING AGENCY

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

REFERENCES

Abundiz-Pérez, F., Cruz-Hernández, C., Murillo-Escobar, M. A., López-Gutiérrez, R. M., & Arellano-Delgado, A. (2016, July 31). A Fingerprint Image Encryption Scheme Based on Hyperchaotic Rössler Map. *Mathematical Problems in Engineering*.

Ahn, D., Kong, S. G., Chung, Y. S., & Moon, K. Y. (2008). Matching with secure fingerprint templates using non-invertible transform. Proc of CISP.

Ali, S. S., Baghel, V. S., Ganapathi, I. I., & Prakash, S. (2020). Robust biometric authentication system with a secure user template. *Image and Vision Computing*, *104*, 104004.

Ali, S. S., Iyappan, G. I., Mahyo, S., & Prakash, S. (2019). Polynomial Vault: A secure and robust ðngerprint based authentication. *IEEE Transactions on Emerging Topics in Computing*. Advance online publication. doi:10.1109/TETC.2019.2915288

Ali, S. S., Iyappan, G. I., & Prakash, S. (2018). Robust technique for ðngerprint template protection. *IET Biom.*, *7*, 536–549.

Ali, S. S., Iyappan, G. I., & Prakash, S. (2019). Fingerprint Shell construction with impregnable features. *Journal of Intelligent & Fuzzy Systems*, *36*, 4091–4104.

Ali, S. S., Iyappan, G. I., Prakash, S., Consul, P., & Mahyo, S. (2020). Securing biometric user template using modiðed minutiae attributes. *Pattern Recognition Letters*, *129*, 263–270.

Ali, S. S., & Prakash, S. (2015). Enhanced Fingerprint Shell. Proceedings of the SPIN 2015, 801–805.

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

Ali, S. S., & Prakash, S. (2019). 3-Dimensional Secured Fingerprint Shell. Pattern Recognition Letters, *126*, 68–77.

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

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

Ali, S. S., & Prakash, S. (2017). Fingerprint Shell Construction with Prominent Minutiae Points. In *Proceedings of the COMPUTE 2017*. ACM.

Bahuguna, R. (1996). *Fingerprint verification using hologram matched filterings*. Presented at the 8th Meeting Biometric Consortium, San Jose, CA.

Balasubramanian, C., Selvakumar, S., & Geetha, S. (2014, December 1). High payload image steganography with reduced distortion using octonary pixel pairing scheme. *Multimedia Tools and Applications*, *73*(3), 2223–2245. doi:10.1007/s11042-013-1640-4

Bingham, E., & Mannila, H. (2001). Random projection in dimensionality reduction: applications to image and text data. In *Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 245-250). ACM.

Bolle, R. M., Connell, J. H., & Ratha, N. K. (2002, December 31). Biometric perils and patches. *Pattern Recognition*, *35*(12), 2727–2738.

Boult, T. E., Scheirer, W. J., & Woodworth, R. (2007). Revocable fingerprint biotokens: Accuracy and security analysis. In *Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on 2007 Jun 17* (pp. 1-8). IEEE.

Boult, T. E., Scheirer, W. J., & Woodworth, R. (2007). Revocable fingerprint biotokens: Accuracy and security analysis. *Proceedings of the CVPR* 2007, 1–8.

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

Capelli, Lumini, Maio, & Maltoni. (1999). Fingerprint classification by directional image partitioning. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 21*(5).

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.

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

Deriche, R. (1987). Optimal edge detecting using recursive filtering. *Proceedings first international Conference on Computer vision,* 501-505.

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

Djara, T., & Vianou, A. (2009). *Fingerprint Registration Using Zernike Moments: An Approach for a Supervised Contactless Biometric System.* Academic Press.

Djara, T., & Vianou, A. (2009). *Fingerprint Registration Using Zernike Moments: An Approach for a Supervised Contactless Biometric System*. Academic Press.

Farina, A., Kovacs-Vajna, Z. M., & Leone, A. (1999). fingerprint minutiae extraction from skeletonized binary images. *Pattern Recognition*, *32*, 877–889.

Feng, J., & Jain, A. K. (2011). Fingerprint Reconstruction: From Minutiae to Phase. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *33*(2), 209–223.

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. (2014). A two-factor protection scheme for MCC fingerprint templates. *Proc. of BIOSIG 2014*, 1–8.

Fingerprint Verification Competition. (2002). Available: http://bias.csr.unibo.it/fvc2002/

Fingerprint Verification Competition. (2004). Available: http://bias.csr.unibo.it/fvc2004/

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

Golub, G. H., & Van Loan, C. F. (1996). *Matrix Computations* (3rd ed.). Johns Hopkins Univ. Press.

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.

Halici, U., & Onguin, G. (1996, October). Fingerprint classification through self-organizing feature maps modified to treat uncertainties. *Proceedings of the IEEE*, *84*(10).

Har-Peled, S., Indyk, P., & Motwani, R. (2012). Approximate Nearest Neighbor: Towards Removing the Curse of Dimensionality. *Theory of Computing*.

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

Hong, L., Wan, Y. F., & Jain, A. K. (1998, August). fingerprint image enhancement: Algorithm and performance evaluation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *20*(8), 777–789.

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

Jain, A. K., Hong, L., Pankati, S., & Bolle, R. (1997, September). An identity-authentication system using fingerprints. *Proceedings of the IEEE*, *85*(9).

Jin, A. T., Ling, D. N., & Goh, A. (2004, November 30). Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, *37*(11), 2245–2255.

Jin, Z., Lim, M. H., Teoh, A. B., & Goi, B. M. (2014, June 1). A non-invertible randomized graph-based hamming embedding for generating cancelable fingerprint template. *Pattern Recognition Letters*, *42*, 137–147.

Jin, Z., Teoh, A. B., Goi, B. M., & Tay, Y. H. (2016, August 31). Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation. *Pattern Recognition*, *56*, 50–62. doi:10.1016/j.patcog.2016.02.024

Johnson, W.B., & Lindenstrauss, J. (1984). Extensions of Lipschitz mappings into a Hilbert space. *Contemporary Mathematics, 26*, 189-206.

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

Juels, A., & Wattenberg, M. (1999). A fuzzy commitment scheme. Proc of CCS.

Kaur, H., & Khanna, P. (2015). Gaussian random projection based non-invertible cancelable biometric templates. *Procedia Computer Science, 54*, 661-70.

62. Khan, T. M., Bailey, D. G., Khan, M. A. U., & Kong, Y. (2017). Efðcient Hardware Implementation For Fingerprint Image Enhancement Using Anisotropic Gaussian Filter. *IEEE Transactions on Image Processing*, *26*, 2116–2126.

Kim, S., Lee, D., & Kim, J. (2001). Algorithm for detection and elimination of false minutiae in fingerprint images. Lecture Notes in Computer Science, 2091, 235-240.

Lee, S., & Jeong, I. R. (2020). On the Unlinkability of Fingerprint Shell. *Security and Communication Networks*, *2020*, 8256929.

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. (1998). *Neural Network based filtering in fingerprints*. IEEE.

Marr & Hildreth. (1980). Theory of edge detection. *Processing of the royal society of London, B204*, 187-217.

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

Moujahdi, C, (2014). Fingerprint shell: Secure representation of fingerprint template. *Pattern Recognition Letters*, *45*(1), 189–196. doi:10.1016/j.patrec.2014.04.001

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

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. *Proc. of ICPR 2008*, 1–4.

Patel, V. M., Ratha, N. K., & Chellappa, R. (2015, September). Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, *32*(5), 54–65. doi:10.1109/MSP.2015.2434151

Proakis, J. G., & Manolakis, D. G. (1996). *Digital Signal Processing: Principles, Algotithms, and Applications*. Prentice Hall.

Ratha, N., Chikkerur, S., Connell, J., & Bolle, R. (2007). Generating cancelable414 ðngerprint templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 29*, 561–72.

Ratha, N., Chikkerur, S., Connell, J., & Bolle, R. (2007). Generating cancelable ðngerprint templates. Pattern Analysis and Machine Intelligence. *IEEE Transactions on*, *29*, 561–572.

Ratha, N., Connell, J., Bolle, R. M., & Chikkerur, S. (2006). Cancelable biometrics: A case study in fingerprints. In *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on 2006 Aug 20* (Vol. 4, pp. 370-373). IEEE.

Ratha, Connell, & Bolle. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, *40*(3), 614–634.

Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, *2011*, 1–25.

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. *Proc. of ICB 2015*, 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., & Goklani, H. (2010). Image Registration using NSCT and Invariant Moment. *International Journal of Image Processing*.

Serief, C. (2009). Robust feature points extraction for image registration based on the non-subsampled contourlet transform. *International Journal Electronics Communication*, *63*(2), 148–152.

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

Soutar, Roberge, Stoianov, Gilroy, & Kumar. (1998). Biometric encryption: Enrollment and veriðcation procedures. In *Aerospace/Defense Sensing and Controls*. International Society for Optics and Photonics.

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

Stojanov, R., Gilroy Soutar, G., Roberge, D., & Kumar, V. (1998). Biometric encryption using image processing. SPIE. *Optical Security and Counterfeit Deterrence Techniques H.*, *3314*, 178–188.

Teoh, A. B., & Yuang, C. T. (2007, October). Cancelable biometrics realization with multispace random projections. *IEEE Transactions on Systems, Man, and Cybernetics. Part B, Cybernetics*, *37*(5), 1096–1106.

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

Thanki, R., & Borisagar, K. (2014, October 1). Security of Biometric Data Using Compressed Watermarking Technique. *Iranian Journal of Electrical and Computer Engineering*, *4*(5), 758. doi:10.11591/ijece.v4i5.6646

Tisse, Martin, Torres, & Robert. (2001). *Système automatique de reconnaissance d'empreinte digitales, sécurisation de l'authentification sur carte à puce*. http://hdl.handle.nett/2042/13225

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 fingerprint matcher. Proc of ICIC.

59. Tran, M. H., Duong, T. N., Nguyen, D. M., & Dang, Q. H. (2017). A local feature vector for an adaptive hybrid ðngerprint matcher. Proceedings of the ICIC, 249–253.

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, December 31). Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach. *Pattern Recognition*, *45*(12), 4129–4137.

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. (2014, March 31). Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. *Pattern Recognition*, *47*(3), 1321–1329.

Wang, S., & Hu, J. (2016, June 30). A blind system identifaication approach to cancelable fingerprint templates. *Pattern Recognition*, *54*, 14–22.

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

Zannou Sourou V. Boris is a doctoral student at the Doctoral School of Engineering Sciences. He previously completed a master's degree in Telecommunications at the Polytechnic School of Yaoundé then a master's degree in computer science at the Institute for Training and Research in Computer Science of the University of Abomey-Calavi. He also obtained a master's degree in Physics at the Faculty of Sciences and Technology of the University of Abomey-Calavi preceded by a license in Physics. his fields of interest are computer security, the computer network, connected objects, artificial intelligence, biometrics.

Tahirou Djara holds a doctorate in computer science, signal and image processing from the University of Abomey-Calavi. He is currently a lecturer at CAMES universities and currently the head of the Computer and Telecommunications Engineering department of the Abomey-Calavi Polytechnic School. He is the author of numerous articles of high caliber and also occupies high positions in the administration of his country Benin. He is interested in biometrics, application development, computer programming, computer network.

Antoine Vianou is a full professor of Engineering Sciences. Previously Engineer in Electrical Engineering where he became a doctor. Author of multitudes of articles he contributes enormously to the development of his country through the various positions he has held. Previously vice-rector of the University of Abomey-Calavi, he is currently director of the Doctoral School of Engineering Sciences of the University of Abomey-Calavi.