KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 7 (2021) 497–500

www.elsevier.com/locate/icte

Design of a fingerprint template protection scheme using elliptical structures

Ilaiah Kavati[a], A. Mallikarjuna Reddy[b], E. Suresh Babu[a], K. Sudheer Reddy[c,*], Ramalinga Swamy Cheruku[a]

[a] *Department of CSE, National Institute of Technology, Warangal, India*
[b] *Department of CSE, Anurag University, Hyderabad, India*
[c] *Researcher (Independent), Hyderabad, India*

Received 4 February 2021; received in revised form 30 March 2021; accepted 1 April 2021
Available online 19 April 2021

Abstract

Although biometric authentication is viewed as more prominent than password or token-based methodology in identity verification, biometric templates are vulnerable to attacks. This paper proposes a new approach for securing fingerprint templates using elliptical structures generated from the fingerprint minutiae. Authors generate a feature vector from the ellipse and will be projected onto a 3D-space to compute a binary string. The resultant binary string is transformed to frequency domain (DFT) and multiplied with a user specific random matrix to make it permanently non-invertible and secure. The results show the efficacy of the proposed method for protecting the fingerprints.

Keywords: Fingerprint; Ellipse; Discrete Fourier transform; Template protection

1. Introduction

In the last decade, traditional systems such as tokens and passwords are most popular for personal authentication. But due to some demerits like loss of token or passwords by the user, once gained by an attacker can be used to deploy attacks [1]. To address these, biometric system has become widely popular. However if biometric trait of an individual is lost or gained by an attacker, it cannot be canceled because it is limited in humans (ten fingers, one face, etc.). Hence, the protection of individual's biometric traits is of utmost importance [1]. Ratha et al. first proposed the idea of cancellable biometrics. In cancellable biometric templates, we store the transformed templates in the database as opposed to storing the original templates. If the transformed template is compromised it does not reveal any information about the biometric data. Therefore it is significantly more secure to store transformed template into database as opposed to original biometric data [2]. The current biometric template protection methods can be categorized as follows:

Biometric cryptosystems: This system combine cryptography and biometrics to benefit from the strengths of both fields [3,4]. The data stored is independent to original templates and does not reveal any information about the original biometric template.

Watermarking approaches: When the traits of one biometric is embedded into the other biometric traits, then this approach is called watermarking [5,6]. This approach is hard to forge by the attacker as the watermarking information should be known by the attacker.

Cancellable template approaches: In this approach, the biometric features extracted are mapped to a predefined multi-dimensional matrix maps the feature vector [7–10]. By traversing the matrix a binary string is generated and is then transformed. This method is more secure compared to the methods discussed above.

2. Methodology

The proposed method follows these steps:

* Corresponding author.
E-mail addresses: ilaiahkavati@nitw.ac.in (I. Kavati), mallikarjunreddycse@cvsr.ac.in (A. Mallikarjuna Reddy), esbabu@nitw.ac.in (E. Suresh Babu), sudheercse@gmail.com (Sudheer Reddy K.), rmlswamy@nitw.ac.in (R.S. Cheruku).

Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2021.04.001

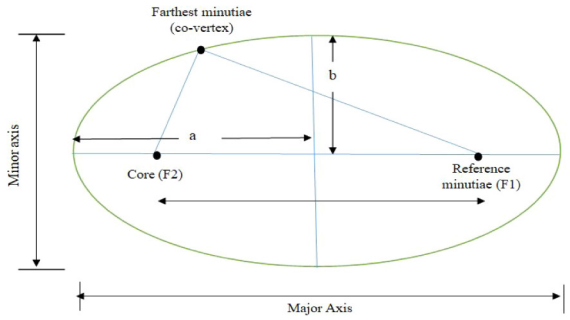

Fig. 1. Formation of ellipse (m_r as F1, core minutia as F2, and m_i as the co-vertex).

2.1. Minutiae extraction from fingerprint image

We use the VeriFinger SDK [11] to extract the minutiae from the fingerprints. Minutiae are the most significant points present in the fingerprint which helps in deciding the uniqueness of it. Various types of minutiae are present in each fingerprint such as ridge ending, bifurcation, core and delta. However, the delta is not present in most of the users fingerprints compared to core. Hence in the proposed approach we consider core along with ridge ending and bifurcation. Every minutia m_i present in a fingerprint has its (x_i, y_i) coordinates in a plane and its orientation (θ_i) with respect to x axis which helps in recognizing one fingerprint from another.

2.2. Construction of ellipse and feature set extraction

Let $M = \{m_1, m_2, .., m_i, .., m_k\}$ be the minutiae set of a fingerprint, where k is the number of minutia present in that fingerprint. Each $m_i \in M$ as a reference, a set of ellipses are constructed as follows:

i. Let m_r be the reference minutia. Select n farthest minutiae points of it in Euclidean space.
ii. For each farthest point m_i, we construct an ellipse as shown in Fig. 1.

The following ellipse features are extracted:
- l_{ri} = major axis + minor axis $i.e.,\ \ 2a + 2b$
- θ_{ri} = Orientation of the farthest minutia
- Ellipse area $(A_{ri}) = \pi * \frac{majoraxis}{2} * \frac{minoraxis}{2}\ i.e.,\ \ \pi * a * b$

We can represent the extracted elliptical feature set of a fingerprint as $X = \{X_1, X_2, \ldots, X_r, \ldots . X_k\}$, where $X_r = [\{l_{r1}, \theta_{r1}, A_{r1}\}, \{l_{r2}, \theta_{r2}, A_{r2}\}, \ldots \{l_{rn}, \theta_{rn}, A_{rn}\}]$.

2.3. Projection/mapping on to a 3D space and generate a binary string

We generate a binary string for each feature vector $X_i = (l_{ri}, \theta_{ri}, A_{ri})$ by mapping it on to a 3D space. Each feature of order three can be plotted onto 3D space by mapping length, orientation and ellipse area along three axes. The range of length axes is [0 - α] where α denotes max length, range of orientation is [0 - 360°] , range of ellipse area is [0 - β] where

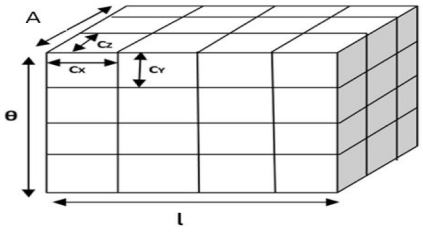

Fig. 2. Mapping feature set onto a 3D-space.

β denotes max area of ellipse. The cell size of 3D space are partitioned into C_x, C_y, C_z as shown in Fig. 2. The number of cells in the 3D space is $N_c = P \times Q \times R$, where $P = \lfloor \frac{max(l_{ij})}{C_X} \rfloor$, $Q = \lfloor \frac{2\pi}{C_Y} \rfloor$ and $R = \lfloor \frac{max(A_{ij})}{C_Z} \rfloor$.

Now, we can find which cell in 3D space include the feature points $(l_{ij}, \theta_j, A_{ij})$ by calculating the values (x_i, y_i, z_i) where $x_i = \frac{l_{ij}}{C_X}$, $y_i = \frac{\theta_j}{C_Y}$ and $zi = \frac{A_{ij}}{CZ}$. Note x_i, y_i, z_i indicates the index values on 3D space. We will get the binary string by traversing all the cells of the 3D space. If at least one point falling in the cell, consider it as the binary '1', otherwise binary '0'. Therefore, the length of the binary string B_S will be equal to the number of cells present in the 3D space i.e., $L = P \times Q \times R$.

2.4. Feature transformation

The generated binary string must be secured by making it non-invertible because if the binary string is compromised the vector can be constructed. So, as to take care of this issue we will transform this binary string into frequency domain by using DFT. Since, the size of binary string is L, we need to perform L-point DFT on binary string (B_S) to get the frequency domain vector.

$$D_i = \sum_{w=0}^{L-1} B_s e^{\frac{-j2\pi iw}{L}} \qquad \forall i = 0, 1, 2, \ldots, L-1 \qquad (1)$$

where $X = e^{\frac{j2\pi w}{L}}$ is the first complex of Nth root of 1.

Now, we get a D_i as a $L \times 1$ vector and $D = \{D_0, D_1, D_2, \ldots D_{L-1}\}^T$. Now to make the complex vector D non-invertible, a random matrix (R) which is specific to a user is generated by using a chosen pin of that user. R is a $p \times q$ matrix where $p < q$ and $q = L$. Finally, a complex vector T of size $p \times 1$ is computed where $T = R \times D$. During verification, same random matrix is generated using the same user's pin. By performing above steps for all the remaining vectors in X i.e., $X = \{X_1, X_2, X_3, \ldots . X_k\}$, we get the transformed templates as $T = \{T_1, T_2, T_3, \ldots T_k\}$.

2.5. Matching

The query template is compared with the corresponding enrolled template to give the matching score s, where $0 \leq s \leq 1$. 0 means total mismatch while 1 indicates a perfect match. Let $T' = \{T'_1, T'_2, T'_3, \ldots T'_m\}$ be the query template,

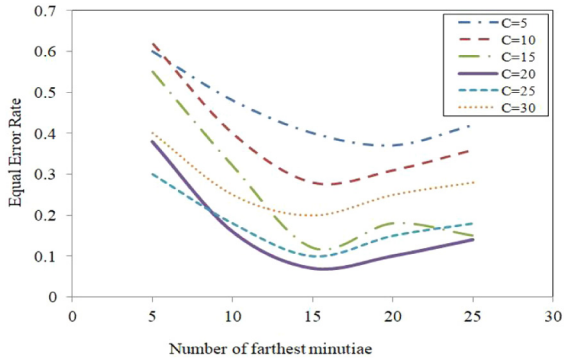

Fig. 3. Equal error rate of DB1 for varying n (number of farthest minutiae) and C (i.e., cell sizes).

the matching score between the enrolled and query template is given by

$$s(T, T') = 1 - d(T, T') \tag{2}$$

where $d(T, T')$ is the distance between enrolled and query template and is given by

$$d(T, T') = \frac{\|T_i - T'_j\|_2}{\|T_i\|_2 + \|T'_j\|_2} \tag{3}$$

where $\|.\|_2$ denotes the 2-norm.

3. Experimental result and analysis

This method have been experimented with the following benchmark databases: FVC 2002 DB1, DB2, DB3. Each database consists 800 impressions of 100 users. The proposed method is evaluated using FRR (False rejection rate), FAR (False acceptance rate) and EER (Equal error rate). Experiments have been conducted on DB1 to observe the EER by varying the number of farthest minutiae considered n and different cell sizes C_x, C_y, C_z (Fig. 3). It can be seen that when $n = 15$ and cell sizes $C_x = 20$, $C_y = 20$, $C_z = 20$, the error rate is minimum. Hence, in all our experiments these values are considered as optimal. To analyze the proposed method in terms of cancellable templates we considered following properties: Accuracy, and Security Analysis.

3.1. Accuracy

To evaluate the accuracy of our proposed elliptical method we consider two cases. First, when each user will be assigned a different key i.e., a unique specific key to each user. This process is known as plain verification. The EER value for this scenario is ideal i.e., it shows the EER as 0% for all three datasets. Second, when any one of the genuine user's key is stolen or lost and the attacker got that key and is trying to perform verification. In this scenario, we obtained an optimal EER values of 7.3%, 5.13% , 12.36% for FVC 2002 DB1, FVC 2002 DB2 and FVC 2002 DB3 respectively. EER graphs for FVC 2002 DB1, DB2 and DB3 are shown in Figs. 4–6. ROC(Receiver Operating Characteristics) show the trade off between FAR and Genuine Acceptance Rate (1-FRR) in a graphical way (Fig. 7). The area occupied below the ROC curve can be used to decide the proposed method performance. The area is more, performance is good. It can also observed from Table 1 that, the proposed work performs well compared to few other existing works.

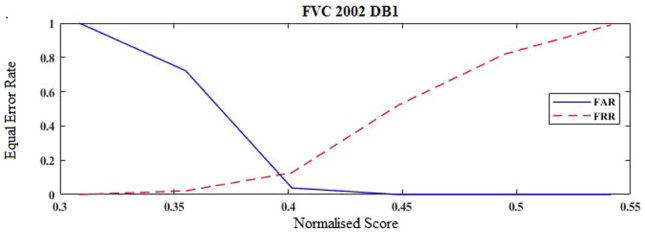

Fig. 4. Equal error rate for DB1.

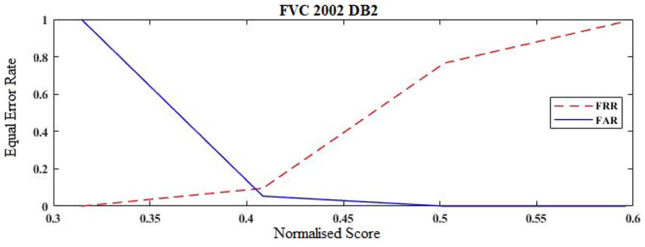

Fig. 5. Equal error rate for DB2.

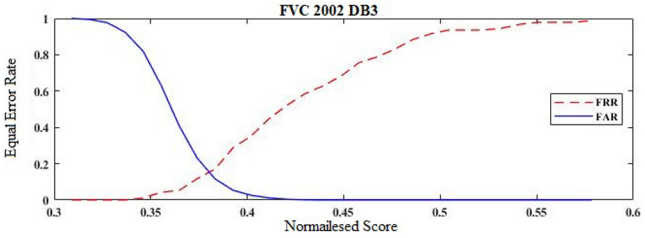

Fig. 6. Equal error rate for DB3.

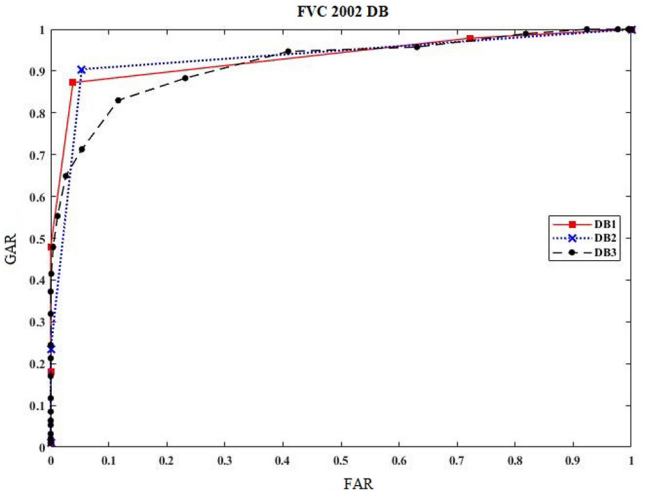

Fig. 7. ROC curve for different datasets.

Table 1
EER (%) of different approaches for DB1, DB2, DB3.

Approach	DB1	DB2	DB3
T. Ahmed et al. [7]	9	6	27
M. V. Prasad et al. [8]	7.85	5.29	17.55
Proposed	7.3	5.13	12.36

3.2. Security analysis

The most important property to verify under security analysis is non-invertibility and is done using brute force attack. Let the attacker is able to reveal the vector X_r. The vector X_r has the following two ellipse properties: (i). Sum of major and minor axis ($i.e.$, $2a + 2b$) and (ii). Area of ellipse ($i.e.$, $\pi \times a \times b$). By solving these, attacker can get value of a, b and hence can form an ellipse. Now, the main task for the attacker is to guess the location of reference minutia. But, it can be anywhere on the boundary of ellipse in the whole image. Let for FVC 2002 DB2, where image size is 296×560 and let average length of a, b are 10, 5. Therefore, total attempts required to guess correct location of one reference minutia is $296 \times 560 \times \pi \times 10 \times 5 = 26$ million attempts. Since we are considering $n = 15$ farthest minutiae for a single reference minutia, then total attempts to find out the locations of all the 15 minutia is 26 million $\times$ 15 = 4 billion attempts. Hence, the proposed elliptical method performs quite good even though if any feature vector got leaked.

4. Concluding remarks

In this work, a new method for alignment free cancellable fingerprint templates was proposed using ellipse structure. Ellipse was formed by selecting one of the minutiae and core point of the fingerprint as focal points and the farthest minutia as the co-vertex. This method performs well because instead of storing spatial information of the fingerprints such as distance or orientation between minutia, etc., we are storing the ellipse attributes in transformed form such that even though if any stored template got leaked, the original fingerprint information will not be revealed to the attacker. This method also performs well in terms of FAR and FRR. However for the fingerprints which does not possess a core point this method will not be suitable and is the main limitation of this work.

CRediT authorship contribution statement

Ilaiah Kavati: Data curation, Writing - original draft, Software, Validation. **A. Mallikarjuna Reddy:** Supervision, Visualization, Investigation. **E. Suresh Babu:** Data curation, Writing - original draft, Software, Validation. **K. Sudheer Reddy:** Conceptualization, Methodology, Writing - review & editing. **Ramalinga Swamy Cheruku:** Conceptualization, Methodology.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A.K. Jain, K. Nandakumar, A. Nagar, Biometric template security, EURASIP J. Adv. Signal Process. 2008 (2008) 1–17, http://dx.doi.org/10.1155/2008/579416.
[2] N.K. Ratha, J.H. Connell, R.M. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Syst. J. 40 (3) (2001) 614–634, http://dx.doi.org/10.1147/sj.403.0614.
[3] B. Alam, Z. Jin, W.-S. Yap, B.-M. Goi, An alignment-free cancelable fingerprint template for bio-cryptosystems, J. Netw. Comput. Appl. 115 (2018) 20–32, http://dx.doi.org/10.1016/j.jnca.2018.04.013.
[4] P.S. Chanukya, T. Thivakaran, Multimodal biometric cryptosystem for human authentication using fingerprint and ear, Multimedia Tools Appl. 79 (1) (2020) 659–673, http://dx.doi.org/10.1007/s11042-019-08123-w.
[5] R. Mothi, M. Karthikeyan, Protection of bio medical iris image using watermarking and cryptography with wpt, Measurement 136 (2019) 67–73, http://dx.doi.org/10.1016/j.measurement.2018.12.030.
[6] M.V. Prasad, I. Kavati, A secure palmprint authentication system using chaotic mixing and watermarking, Int. J. Biom. 6 (4) (2014) 321–334, http://dx.doi.org/10.1504/IJBM.2014.067124.
[7] T. Ahmad, J. Hu, S. Wang, Pair-polar coordinate-based cancelable fingerprint templates, Pattern Recognit. 44 (10–11) (2011) 2555–2564, http://dx.doi.org/10.1016/j.patcog.2011.03.015.
[8] M.V. Prasad, J.R. Anugu, C. Rao, Fingerprint template protection using multiple spiral curves, in: Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics, Springer, 2016, pp. 593–601, http://dx.doi.org/10.1007/978-81-322-2538-6_61.
[9] A.K. Trivedi, D.M. Thounaojam, S. Pal, Non-invertible cancellable fingerprint template for fingerprint biometric, Comput. Secur. 90 (2020) 101690, http://dx.doi.org/10.1016/j.cose.2019.101690.
[10] H. Ashiba, F. Abd El-Samie, Implementation face based cancelable multi-biometric system, Multimedia Tools Appl. 79 (41) (2020) 30813–30838, http://dx.doi.org/10.1007/s11042-020-09529-7.
[11] Neurotec-Biometric-4.3, Neurotechnology VeriFinger-SDK, URL http://www.neurotechnology.com/verifinger.html/.