Pattern Recognition Letters 129 (2020) 263–270

Contents lists available at ScienceDirect

Pattern Recognition Letters

journal homepage: www.elsevier.com/locate/patrec

Securing biometric user template using modified minutiae attributes☆

Syed Sadaf Ali[a,*], Iyyakutti Iyappan Ganapathi[a], Surya Prakash[a], Pooja Consul[b], Sajid Mahyo[c]

[a] Discipline of Computer Science and Engineering, Indian Institute of Technology Indore, Indore 453552, India
[b] Birla Institute of Technology and Science, Pilani K.K. Birla Goa Campus, India
[c] Ecole Internationale des Sciences du Traitement de l'Information, France

ARTICLE INFO

Article history:
Received 11 April 2019
Revised 11 September 2019
Accepted 27 November 2019
Available online 27 November 2019

Keywords:
Security
Privacy
Fingerprint
Authentication
Revocability
Biometrics

ABSTRACT

The minutiae points information of a fingerprint is generally saved directly in the database as a template for the user. It has been deduced through numerous research works that the original fingerprint of a user can be obtained from the minutiae points information. As the databases are prone to various attacks, their security becomes a huge concern in fingerprint based authentication systems. Hereby, a novel technique has been introduced which is based on the modification of the minutiae attributes. The user template generated through the proposed technique is extremely secure and robust. The proposed technique achieved 1.63%, 1%, and 2.43% EER under stolen-key attack scenario for FVC2002 DB1, FVC2002 DB2, and FVC2002 DB3 fingerprint databases respectively. The proposed technique achieved 0% EER under different-key scenario. Highly encouraging results are obtained that show the viability and effectiveness of the proposed technique.

1. Introduction

User authentication based on biometric provides various advantages [4]. Fingerprint is one of the most popular biometric trait, which is utilized for the user authentication. Though it is highly popular, there are many issues related to it [14]. There are various types of attacks possible on a authentication system based on fingerprints [14], out of which the attack on the database is one of the most destructive one. Most of the authentication systems that are based on the fingerprint save the minutia point (special points in fingerprint where ridges begin/end or bifurcate, as shown in Fig. 1a) attributes in the database as user template. Many research works have shown that from information of minutiae points original fingerprint can be constructed. Databases are prone to attacks, hence securing the user's biometric data is essential as it is non-revocable and cannot be changed if compromised. Enrollment and verification [18] are the two major steps involved in user authentication, a secure biometric based authentication system must depict revocability, diversity, security, and performance [19]. The main concept used to achieve them is to transform the user's biometric data *BD* by using a transformation function *TF* and a unique user key K_1, the transformed template $TF(BD, K_1)$ is saved as a template for the user in the database. If the template is compromised, then by modifying the user key from K_1 to K_2, a new user template $TF(BD, K_2)$ can be constructed.

Major contributions of the proposed scheme are given below:

- It gives a unique and secure representation of user template which is computed by the modification of minutiae attributes of the fingerprint of a user.
- The proposed technique is robust to translation and rotation, which is a major issue in other authentication schemes based on fingerprints.
- We have validated the proposed method on publicly available diverse and challenging databases. The obtained results are better as compared to the state-of-the-art literature techniques.
- The analysis of the proposed technique on different types of attacks shows its high revocability and diversity. In a situation where a user template is compromised, we can generate a new template for the user, which has no similarity to the earlier user template that has been compromised.

Remaining paper has been organized as follows. The next section contains a literature review of the available biometric template protection approaches. Section 3 introduces the proposed method. Section 4 includes the outcomes and the discussion, and the last section of the paper includes conclusions.

☆ "Editor:" Prof. G. Sanniti di Baja.

* Corresponding author.
E-mail address: phd1301101006@iiti.ac.in (S.S. Ali).

https://doi.org/10.1016/j.patrec.2019.11.037
0167-8655/

2. Literature review

Fingerprint reconstruction is possible from its minutiae points attributes [8], various frameworks present in the literature are mentioned below.

Cappelli et al. developed Minutia-Cylinder-Code (MCC) in [16], where the user fingerprint is utilized to produced a unique cylinder. Although this method is popular, the original fingerprint information of is insecure. Ferrara et al. suggested a safe MCC with a non-invertible conversion in [9]. Although the fingerprint data of the user is safe, the template cannot be revoked. Ferrara et al. introduced a different version of [16] in [10], which is based on the protection of the two-factor template. In [3] Liu and Zhao suggested matching in encrypted domain by utilizing MCC, it uses minimizing l_1. Ahmad et al. in [28] used local fingerprint features and applied many-to-one mapping for the protection of the user template. Jin et al. [32] used minutiae set in the form of a bit string, using a 3-tuple quantization which is based on polar grid. In [32], Jin et al. used minutia set bit string by applying the three tuple quantization to provide safety for the user template. In [24] a dense mapping based framework is introduced for security of fingerprint. Yang et al. in [31] designed a framework for the construction of a cancelable template that uses the Delaunay triangle and relies on the local fingerprint structure. In the [29] improved multi-line code (MLC) protects fingerprint templates based on minutiae points. Local structures on the basis of the Delaunay triangle are used in [31] for the construction of cancelable user templates.

In [30], Yang et al. used the modified neighboring structures of Voronoi, known as the bio-cryptosystem, to make it an alignment-free method. A new framework has been proposed by Moujahdi et al. in [2], which is known as Fingerprint Shell. In this spiral curves are constructed from a fingerprint. The extension of [2] is proposed by Ali and Prakash [18] to improve recognition by using spiral curves. Two more secure versions of [2] are further proposed in [20,22]. Wong et al. in [29] introduced a method based on the minutiae point, which improved the multi-line code to protect the user template. In [33], Jin et al. integrated Randomized Graph-based Hamming Embedding (RGHE) to generate a binary fingerprint model. In [33], a framework has been designed using RGHE for the generation of binary user templates. In [30], the neighbor structure of Voronoi has been used by Yang et al. for an invariant alignment approach. In [11], a cancelable fingerprint template method is introduced that uses the nearest k-neighborhood structure. Wang and Hu have presented a system to produce a cancelable model and also a free alignment in [25]. Non-invertible transformation is used for the safety of the samples of the frequency bits. A method relying on Delaunay triangles is suggested for making the cancelable templates in [13]. Local minutiae structure, through zoned minutiae pairs, is used to make cancelable templates by Wang et al. [27]. Iyappan et al. proposed a framework for biometric identification based on the geometric statistical descriptor in [5,6]. Ali et al. introduced Polynomial Vault in [23], where a polynomial curve is produced from a user's fingerprint, which is used as a user model. In [12] a system based method is introduced, which rely on the merged framework to secure a user's fingerprint. Dave et al. introduced a technique for capturing and recognizing human biometric data in [7]. Wang et al. introduced a non-invertible transformation to binary fingerprint presentation in [26] to generate cancelable model. Ali et al. introduced a technique in [21] that uses secured fingerprint features as a user model. The features used in this method depends on the nearby minutia point for the feature securing phase, which reduces the efficiency. The proposed method by creating a highly safe user model with superior efficiency, overcomes the weaknesses of the above techniques.

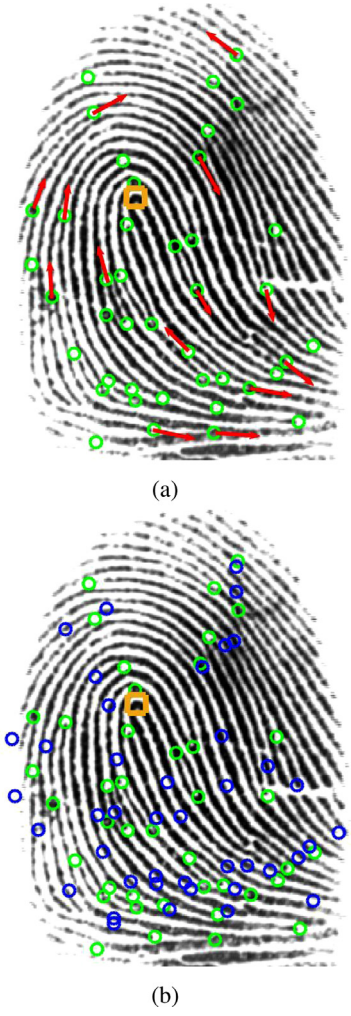


Fig. 1. An example of the attributes modification: (a) The green circles depict the original minutiae points and arrows show their orientation, whereas the yellow square shows the singular point, (b) Modified minutiae locations generated, the green circles show the original locations of the minutiae points whereas the blue circles show the modified locations for different minutiae points. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

3. Proposed technique

A secure user template is generated as the fundamental idea used to accomplish a secure authentication system. Using key-set $\{key_1, key_2, key_3\}$, the minutiae points' attributes along with the singular point information are used to build a secure user template. No user fingerprint data can be revealed from the secure template and using the same fingerprint image, another (very distinct template) template can be acquired using another user key set. The new template produced with the new user key set must not be similar to the user template that has been compromised. The 1 algorithm shows the steps engaged in creating a secure user template. The abscissa axis is represented in this paper by the u-axis, while the ordinate axis is represented in the 2D plane by the v-axis. The operation to create a secure user template is described below.

3.1. Extraction of features

Through appropriate sensors, fingerprint image is obtained from the finger of a user. By utilizing the captured fingerprint, desired

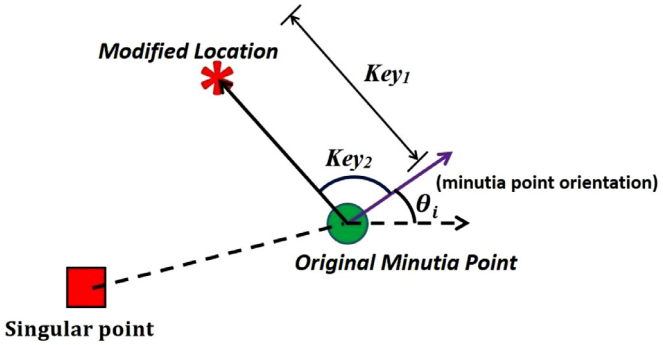


Fig. 2. Computation of the modified location using the keys key_1 and key_2.

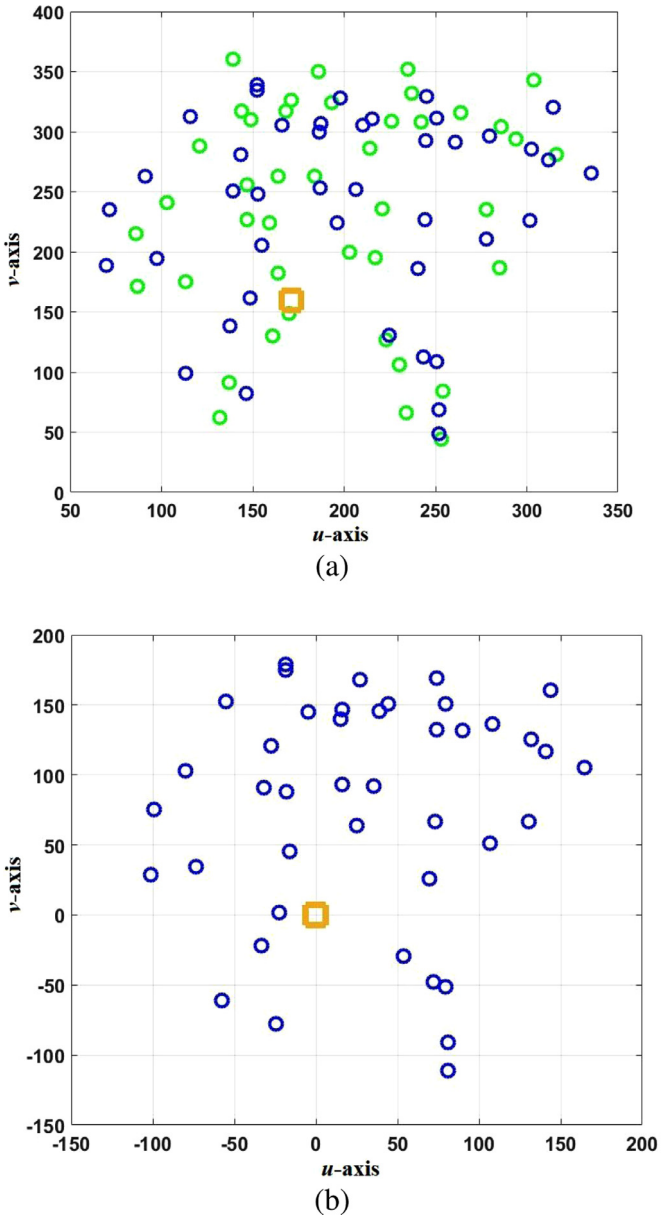


Fig. 3. Translation invariance: (a) Initial modified minutiae locations (yellow square represents the singular point location, green circles represents the real locations of minutiae points, and blue circles represents the modified locations), (b) Translation of modified locations such that the singular point moves to origin. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

features are been extracted. Here we extract the minutiae points and the singular point, as depicted in Fig. 1a.

3.2. Computation of secure user template

In the proposed technique secure user template is computed by storing the modified locations corresponding every minutia point of fingerprint. The modified location corresponding to a minutia point is computed by using its real location and the key-set $\{key_1, key_2, key_3\}$. Let there be *numb* number of minutiae points present in a fingerprint that are represented as $Minutia_{count}$ (*count* ranges from 1 to *numb*). Here $Minutia_{count} = \{u_{count}, v_{count}, \theta_{count}, type_{count}\}$, where u_{count} represents the abscissa magnitude, v_{count} represents the ordinate magnitude, θ_{count} represents the orientation magnitude and $type_{count}$ represents the type (ridge bifurcation, starting, or ending) of $count^{th}$ minutia point. For the generation of modified location corresponding to a minutia point $Minutia_{count}$, user specific keys key_1 and key_2 are used along with the original location and the orientation information of the minutia point. Fig. 2 pictorially shows the procedure involved. The modified location (u'_{count}, v'_{count}) of $Minutia_{count}$ (as shown in Fig. 2) is key_1 units away from the real location of the minutia point (u_{count}, v_{count}) and makes an angle of key_2° with respect to the orientation-vector of the minutia point $Minutia_{count}$ in counter-clockwise direction. Fig. 1b shows an example of modified locations generation. Formally, u'_{count} and v'_{count} values are computed as follows.

$$u'_{count} = u_{count} + (key_1 \times \cos(key_2 + \theta_{count}))$$
$$v'_{count} = v_{count} + (key_1 \times \sin(key_2 + \theta_{count}))$$

To decrease the effect of translation due to intra-subject variation, singular point location $(u_{singular}, v_{singular})$ is being used. Every location in the template is relocated in such a way that the singular point of the new template moves to the origin as depicted in Fig. 3a and b. Formally, the new value for (u'_{count}, v'_{count}) after the relocation is given as follows.

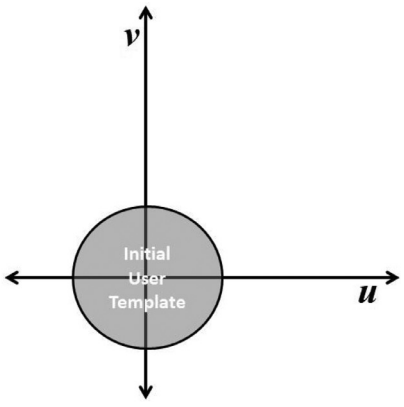
$$u'_{count} = u'_{count} - u_{singular}$$
$$v'_{count} = v'_{count} - v_{singular}$$

Corresponding to every singular point (there are usually one to four singular points in a fingerprint) a template is computed and stored in the database/repository while enrolling a user and every template is compared with the query (probe) template at the time of authentication.

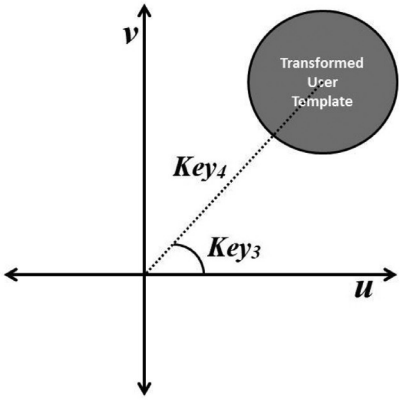
3.3. Enhancing security

Security of the template computed in the previously is enhance through utilization of two more keys key_3 and key_4, where key_3 is a completely new user key while key_4 is computed using the values of key_1, key_2, and key_3. The key key_4 is represented as a 48-bit integer and is computed using the integral values of key_1, key_2, and key_3. The sixteen least significant bits of key_4 are obtained from $\lfloor key_1 \rfloor$, middle sixteen bits are obtained from $\lfloor key_2 \rfloor$ whereas the sixteen most significant bits come from $\lfloor key_3 \rfloor$. Every modified location is first rotated by key_3° with respect to the origin and then translation is performed in which they are moved by key_4 units with respect to origin making an angle of key_3° with respect to *u*-axis as depicted in Fig. 4. This effectively mean that the abscissa value of a modified minutia location is raised by $key_4 \times \cos(key_3)$ whereas the ordinate value is raised by $key_4 \times \sin(key_3)$. Formally, the value of key_4 is given below.

$$key_4 = \lfloor key_3 \rfloor \times (2)^{32} + \lfloor key_2 \rfloor \times (2)^{16} + \lfloor key_1 \rfloor$$



(a)



(b)

Fig. 4. Enhancement of the security of a user template: (a) Initial template of a user, (b) Security enhanced template generated using keys key_3 and key_4.

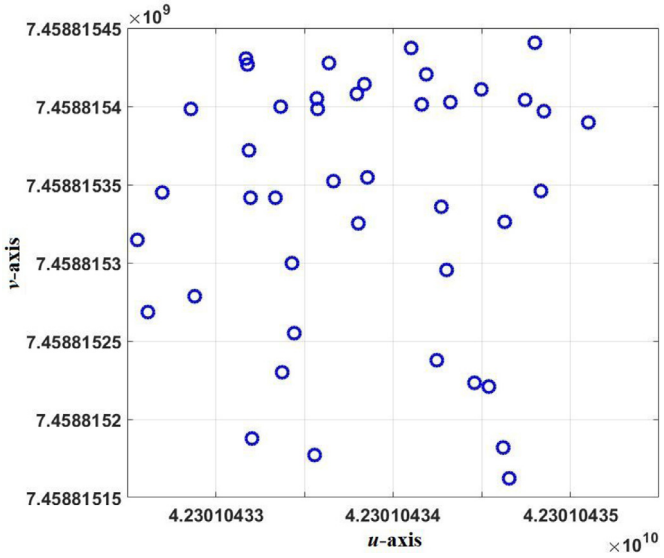
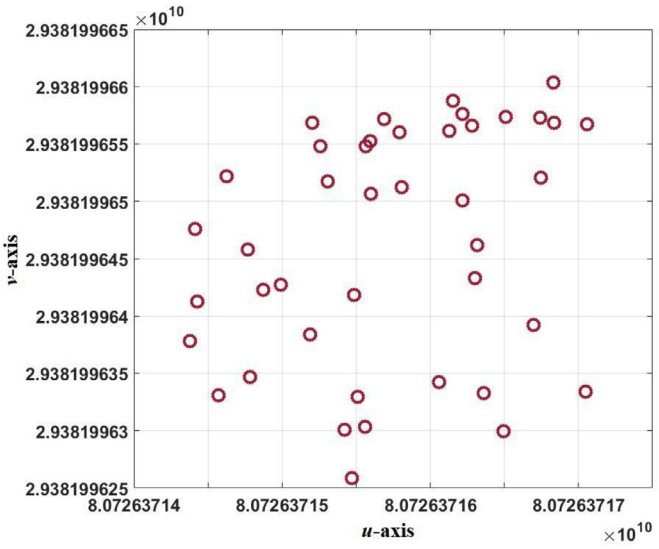


Fig. 5. Final template for a user computed by utilizing the one shown in Fig. 3b, with the help of keys key_3 and key_4.

Further, the new location (u'_{count}, v'_{count}) of a minutia point with enhanced security can be given as follows.

$$\begin{bmatrix} u'_{count} \\ v'_{count} \end{bmatrix} = \begin{bmatrix} cos(key_3) & -sin(key_3) \\ sin(key_3) & cos(key_3) \end{bmatrix} \times \begin{bmatrix} u'_{count} \\ v'_{count} \end{bmatrix}$$



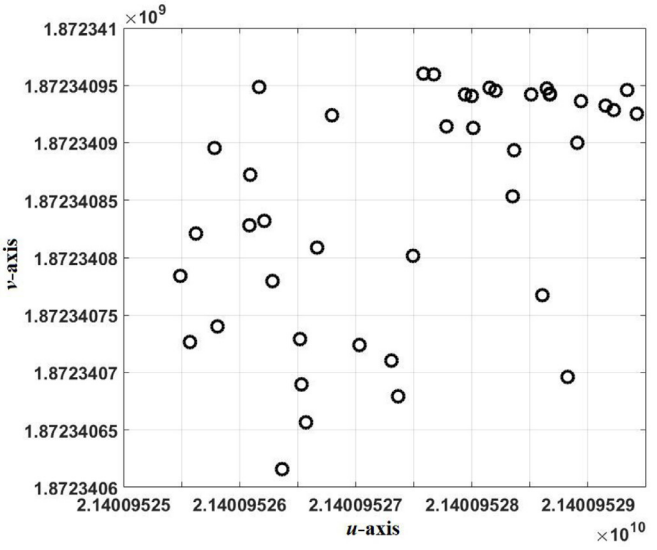


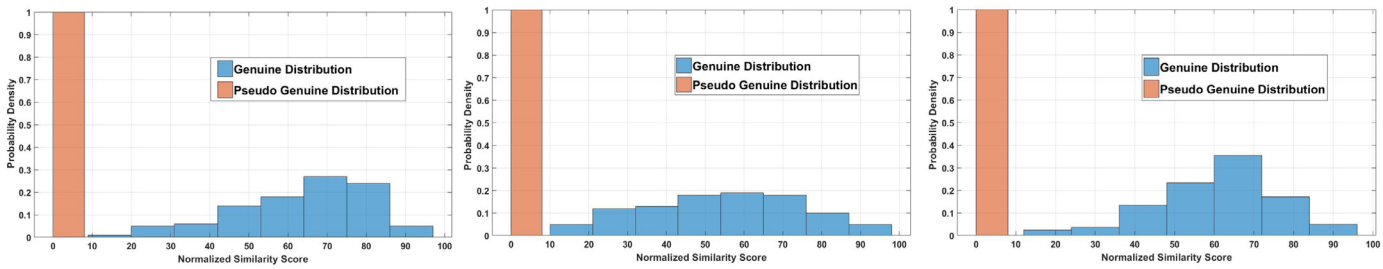
Fig. 6. Secure user templates generated from the fingerprint shown in Fig. 1a, with different key-set values.

$$u'_{count} = u'_{count} + (key_4 \times \cos(key_3))$$
$$v'_{count} = v'_{count} + (key_4 \times \sin(key_3))$$

The final user template generated from the modified locations represented in Fig. 3b is depicted in Fig. 5. This template with the enhanced security is save in the database/repository during enrollment and further utilized for user verification.

3.4. Template matching for verification

During verification, a single template is constructed from the query image in which the singular point nearest to the centre of the fingerprint image is considered. The obtained template is matched to all templates (model templates) that are there (with respect to different singular points) in the database/repository for a particular user. Once the matching with all the templates is completed, the best matching score obtained is considered for final authentication. In order to compute the similarity score, the number of corresponding points present in the model template and the query template are calculated with the help of Hausdorff Distance (HD) [1]. Two points in different templates are considered



(a) DB1 database (b) DB2 database (c) DB3 database

Fig. 7. Histograms of Genuine/Pseudo-Genuine score distributions for the proposed technique on FVC2002 databases.

to be matched, if their HD is smaller than a defined threshold. The final similarity score is the minimum of the percentage of number of matching points that are obtained in the two matching (query template to model template and vice-versa). Suppose $numb_q$ points are present in the query template and $numb_s$ points are present in the model template. Further, let us consider that $mnumb_q$ ($mnumb_q \leq numb_q$) points of the model template gets matched, and $mnumb_s$ ($mnumb_s \leq mnumb_s$) points of the query template gets matched. Formally similarity score can be given as follows.

$$Similarityscore = \min\left(\frac{mnumb_s}{numb_s}, \frac{mnumb_q}{numb_q}\right) \times 100$$

If the obtained match score is found to be more than a specified threshold then the query and the model template are considered to be matching and authentication succeeds. In order to reduce the variation due to rotation, the query template of the user is rotated from $-\delta^\circ$ to $+\delta^\circ$ (by increasing 1° in each iteration) with respect to center point $(key_4 \times \cos(key_3), key_4 \times \sin(key_3))$ of the query and is matched with the model (stored) template. The final match score is the best score obtained from all the comparisons. The value of δ has been kept as 60 in our experiments.

4. Result analysis

The proposed technique has been evaluated using FVC2002 DB1, FVC2002 DB2, and FVC2002 DB3 databases [21]. All these databases consist 100 subjects and from every subject eight fingerprints samples are obtained. The proposed technique has been analyzed using 1-vs-1 protocol [20], were we have chosen two samples per subject randomly. The major terms calculated for the proposed technique are False Rejection Rate (FRR), Genuine Acceptance Rate (GAR), False Acceptance Rate (FAR), and Equal Error Rate (EER) [23]. For the statistical analysis of the proposed technique the χ^2 (Chi-square), t-test, and Kolmogorov-Smirnov test values [23] are calculated. The minutiae point extraction trial version of *VeriFinger* SDK [15] has been used. The proposed technique has been evaluated for its revocability, diversity, security, and recognition performance.

4.1. Revocability

Any framework is considered to be revocable if it can generate multiple templates from the same biometric data. Fig. 6 shows an example where two very different user templates which have been obtained from same fingerprint for different key-sets. Though both the templates are of the same user, they are totally different. Further the revocability of the proposed technique has been analyzed through revoked template attack [21] (Attack-I and Attack-II), where from a compromised template adversary tries to authenticate itself. The results obtained are given in Table 1, which shows the percentage of revoked template attacks that are successfully carried out under Attack-I and Attack-II scenarios. The outcomes shows that the proposed technique is highly revocable.

Table 1
Revoked template attack (values show the percentage of successful attacks).

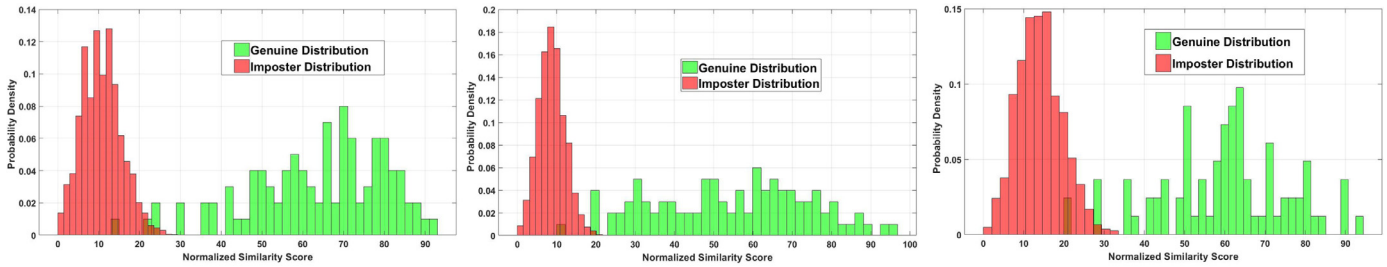
Database	Attack-I	Attack-II
FVC2002 DB1	0.00	0.00
FVC2002 DB2	0.00	0.00
FVC2002 DB3	0.00	0.00

4.2. Diversity

When there is no linkability between templates generated by a technique using same biometric data and different key-sets, then that technique is considered to be diverse. To demonstrate the diversity, two different systems are considered with two different mutually exclusive key-sets. For the first system (System 1), values of key_1, key_2, and key_3 are randomly chosen in the range of $key_1 \in [10, 250]$, $key_2 \in [10, 25]$ and $key_3 \in [10, 25]$ and for second system (System 2), $key_1 \in [35, 65]$, $key_2 \in [35, 65]$ and $key_3 \in [35, 65]$ for different users. To compute Pseudo-Genuine score, templates generated from System 1 and System 2 using the same biometric data are compared. Fig. 7 depicts the Genuine/Pseudo-Genuine scores distribution, which are well separated. As observed from Figs. 6 and 7, there is no linkability between templates generated by the proposed technique using same biometric data and different key-sets. This depicts the capability of the proposed technique to handle cross matching attack [19] and its effectiveness in terms of diversity.

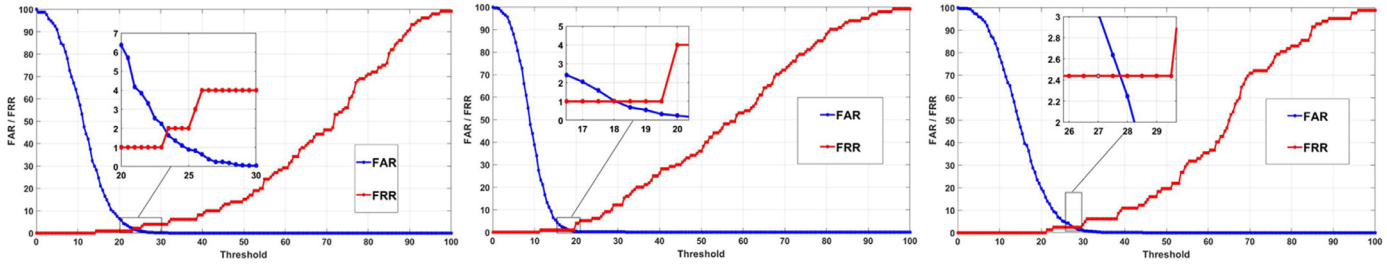
4.3. Security

A technique is terms as secure if it does not reveal any information/data related to the original biometric data of a user, even if the attacker gets the user template. In the proposed technique, if an adversary gets the user template as well as the values of key-set $\{key_1, key_2, key_3\}$, then only information that the adversary posses is that the original minutia point location is on a circle which has radius key_1 and is centred at the modified location obtained utilizing the user template and the key-set. A circle has innumerable points, hence innumerable original minutia point locations are possible. Instead of innumerable locations suppose only 360 original minutia point locations are possible on a circle which has radius key_1 and is centred at the modified location, that means 360 possible locations for every minutia point. If there exist *numb* minutiae points in a fingerprint then a total of 360^{numb} (where *numb* is usually more than 10 making 360^{numb} very large) possibilities exist to map the minutiae locations obtained from the compromised template to original minutia locations. Apart from this the minutia orientation and type information is not saved anywhere. This



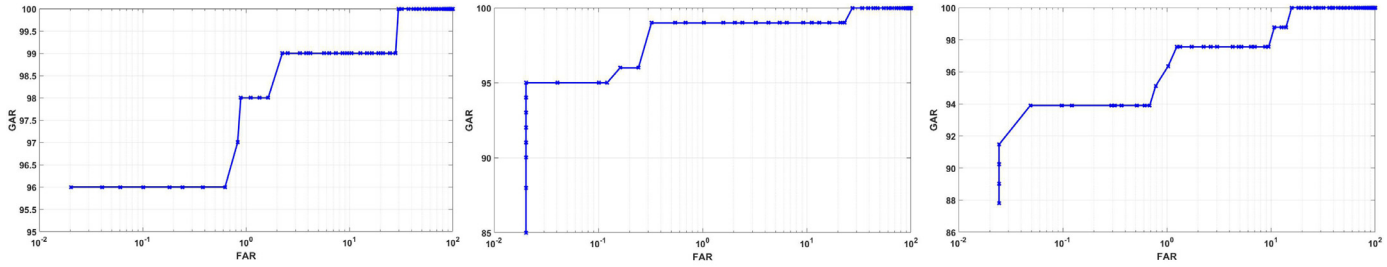
(a) DB1 database (b) DB2 database (c) DB3 database

Fig. 8. Histograms of Genuine/Imposter score distributions for the proposed technique under stolen-key attack scenario on FVC2002 databases.



(a) DB1 database (b) DB2 database (c) DB3 database

Fig. 9. Plots of FAR/FRR vs. Threshold for the proposed technique on FVC2002 databases, under stolen-key attack scenario.



(a) DB1 database (b) DB2 database (c) DB3 database

Fig. 10. ROC plots for the proposed technique on FVC2002 databases, under stolen-key attack scenario.

shows that practically it is infeasible for adversary to obtain the original biometric data of a user. Hence, the proposed technique is secure and less vulnerable.

4.4. Recognition performance

The proposed technique has been evaluated for both the stolen-key attack scenario (the same key-set value allocated to each user) and the different-key scenario (where separate key-set values are allocated to distinct users).

Fig. 8 represents the Genuine / Imposter score distribution histogram while Fig. 9 displays the FAR / FRR vs. Threshold plots obtained under the stolen-key attack for the proposed technique. Fig. 10 indicates the operating characteristic of the receiver (ROC) curves [17] under the proposed technique's stolen-key attack. The EER values in Table 2 are used to compare the proposed technique with various methods for the stolen-key attack. From Table 2, it can be seen that for FVC2002 DB3, our results are much superior to the same obtained by other techniques whereas, for FVC2002 DB1 and DB2 databases, the results obtained by our technique are comparable with other techniques. It is important to note here that the quality of the images in FVC 2002 DB3 are the poorest among all the databases and our proposed technique is performing the best in this database. Moreover, it is to be noticed that while using 1-vs-1 protocol, we have randomly selected two samples per subject whereas in other techniques, authors have either considered first two samples or two best samples of a subject for experimentation. In this sense, our results are robust and more reliable.

Table 2
Comparison of EER values for the proposed method with various stolen-key attack methods (values are in percentage).

Various techniques	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3
Sandhya et al. [12]	2.19	1.6	6.14
Wang et al. [27]	0.19	1	4.29
Wang et al. [26]	1	2	5.2
Sandhya et al. [13]	3.96	2.98	6.89
Wang and Hu [25]	3	2	7
Sandhya and Prasad [11]	4.71	3.44	8.79
Jin et al. [33]	4.36	1.77	–
Yang et al. [30]	3.38	0.59	9.80
Yang et al. [31]	5.93	4	
Jin et al. [32]	5.19	5.65	–
Wang and Hu [24]	3.5	4	7.5
Ahmad et al. [28]	9	6	27
Ali et al. [21]	2	1	3.1
Proposed Technique	**1.63**	**1**	**2.43**

The value of the t-test and of the χ^2 test obtained in the stolen-key attack for the proposed technique is shown in Table 3. The analysis values of Kolmogorov-Smirnov are shown in Table 4 when comparisons are made between the proposed method and various

Algorithm 1 Secure template generation.

Required Input: Number of minutiae points = *numb*, $Minutia_{count}$ $\{u_{count}, v_{count}, \theta_{count}\}$ (*count* ranges from 1 to *numb*),and user key-set $\{key_1, key_2, key_3\}$
Obtained Output: *Secure template (ST)*
/* *Computation of key* key_4 *for template security enhancement* */
$key_4 = \lfloor key_3 \rfloor \times (2)^{32} + \lfloor key_2 \rfloor \times (2)^{16} + \lfloor key_1 \rfloor$
for *count* = 1 to *numb* **do**
    /* *Computation described in Section 3.2.* */
    $u'_{count} = u_{count} + (key_1 \times \cos(key_2 + \theta_{count}))$
    $v'_{count} = v_{count} + (key_1 \times \sin(key_2 + \theta_{count}))$
    /* *Decreasing variation due to translation* */
    $u'_{count} = u'_{count} - u_{singular}$
    $v'_{count} = v'_{count} - v_{singular}$
    /* *Computation described in Section 3.3.* */
$$\begin{bmatrix} u'_{count} \\ v'_{count} \end{bmatrix} = \begin{bmatrix} cos(key_3) & -sin(key_3) \\ sin(key_3) & cos(key_3) \end{bmatrix} \times \begin{bmatrix} u'_{count} \\ v'_{count} \end{bmatrix}$$
    $u'_{count} = u'_{count} + (key_4 \times \cos(key_3))$
    $v'_{count} = v'_{count} + (key_4 \times \sin(key_3))$
end for
/* *abscissa values of ST* */
$ST(1, :) = \{u'_1, u'_2, \ldots, u'_n\}$
/* *ordinate values of ST* */
$ST(2, :) = \{v'_1, v'_2, \ldots, v'_n\}$

Table 3
The test values of *t*-test and χ^2 obtained in a stolen-key attack for the proposed technique.

Databases	*t*-test	χ^2 test
FVC2002 DB1	106.54	21.78
FVC2002 DB2	104.26	57.32
FVC2002 DB3	79.42	11.89

Table 4
Comparison of Kolmogorov–Smirnov test values of the proposed method with different methods under the stolen-key attack.

Various techniques	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3
Sandhya et al. [12]	0.96	0.97	0.89
Ali et al. [21]	0.9792	0.9843	0.9490
Sandhya et al. [11]	0.91	0.93	0.75
Moujahdi et al. [2]	0.7812	–	–
Sandhya et al. [13]	0.9208	0.9404	0.8655
Proposed Technique	**0.9813**	**0.9856**	**0.9582**

methods of the stolen-key attack. The proposed technique is also evaluated for the different-key scenario where for experimentation the key values are randomly selected in the range of $key_1 \in [5, 45]$, $key_2 \in [0, 360]$ and $key_3 \in [0, 360]$. The EER values for the proposed technique are compared with different techniques for the different-key scenario in Table 5, where 0.00% percent for all databases has been achieved by the proposed technique. Table 6 shows the values obtained under the proposed technique for the *t*-test and χ^2 test. The test values of Kolmogorov-Smirnov compare the proposed technique with different techniques under the different key scenario is given in Table 4. The FVC2002 DB1, DB2 and DB3 fingerprint databases contain huge intra-subject translation and rotation variations. On these databases, the technique proposed is very accurate, showing its robustness to translation and rotation. More than 1000 different key range values and similar results were carried out in experiments. The above results clearly demonstrate the superior performance of the technique proposed.

Table 5
Comparison of the EER values of the proposed technique with several different-key scenario techniques (values are in percentage).

Various techniques	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3
Cappelli et al. [9]	0	0	2
Sandhya et al. [11]	0	0	3.65
Ali et al. [21]	0	0	0
Liu and Zhao [3]	0	0	–
Sandhya et al. [13]	0	0	1.65
Ferrara et al. [9]	0	0.02	3.43
Sandhya et al. [12]	0	0	1.65
Wong et al. [29]	0	0	–
Jin et al. [32]	0	0	–
Proposed technique	**0**	**0**	**0**

Table 6
The *t*-test and χ^2 test values obtained for the proposed technique under different-key scenario.

Databases	*t*-test	χ^2 test
FVC2002 DB1	262.29	∞
FVC2002 DB2	189.32	∞
FVC2002 DB3	228.42	∞

Table 7
Kolmogorov–Smirnov test values comparison of the proposed technique with various techniques under the different-key scenario.

Various techniques	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3
Moujahdi et al. [2]	0.9934	–	–
Sandhya et al. [11]	1	1	0.93
Sandhya et al. [13]	1	1	0.9691
Sandhya et al. [12]	1	1	0.93
Proposed technique	**1**	**1**	**1**

5. Conclusion

Fingerprint based authentication is highly popular; however, it has security and privacy issues. Generally minutiae points information of a fingerprint is directly used as a user template, which is highly insecure as databases are prone to attacks. This paper proposed a novel fingerprint authentication technique which is based of minutiae points attributes modification using a unique user key. User template generated is highly revocable and extremely secure. The proposed technique achieved 1.63%, 1%, and 2.43% EER under stolen-key attack scenario for FVC2002 DB1, DB2, and DB3 fingerprint databases respectively. The proposed technique achieved 0% EER under different-key scenario. It has been observed from the experimental evaluations that a significant enhancement has been achieved in terms of performance and security that depicts the robustness and viability of the proposed technique. The proposed technique gives good recognition performance and can handle intra-subject variation due to rotation/translation. Hence, it can be termed as an efficient technique which is extremely secure and robust.

Declaration of Competing Interest

There is no conflict of interest.

References

[1] A.A. Taha, A. Hanbury, An efficient algorithm for calculating the exact hausdorff distance, IEEE Trans. PAMI 37 (2015) 2153–2163.
[2] C. Moujahdi, G. Bebis, S. Ghouzali, M. Rziza, Fingerprint shell: secure representation of fingerprint template, Pattern Recognit. Lett. 45 (2014) 189–196.

[3] E. Liu, Q. Zhao, Encrypted domain matching of fingerprint minutia cylinder–code (MCC) with l_1 minimization, Neurocomputing 259 (2017) 3–13.
[4] G.I. Iyappan, S. Prakash, I.R. Dave, P. Joshi, S.S. Ali, A.M. Shrivastava, Ear recognition in 3D using 2D curvilinear features, IET Biom. 7 (6) (2018) 519–529.
[5] G.I. Iyappan, S.S. Ali, S. Prakash, Geometric statistics-based descriptor for 3D ear recognition, Vis. Comput. (2018).
[6] G.I. Iyappan, S.S. Ali, S. Prakash, Multi-resolution local descriptor for 3d ear recognition, in: Proc. of BIOSIG 2019, 2019, pp. 1–8.
[7] I.R. Dave, G.I. Iyappan, S. Prakash, S.S. Ali, A.M. Shrivastava, 3d ear biometrics: acquisition and recognition, in: Proc. of INDICON 2018, 2015, pp. 801–805.
[8] J. Feng, A.K. Jain, Fingerprint reconstruction: from minutiae to phase, IEEE Trans. PAMI 33 (2) (2011) 209–223.
[9] M. Ferrara, D. Maltoni, R. Cappelli, Noninvertible minutia cylinder-code representation, IEEE Trans. IFS 7 (6) (2012) 1727–1737.
[10] M. Ferrara, D. Maltoni, R. Cappelli, A two-factor protection scheme for MCC fingerprint templates, in: Proc. of BIOSIG 2014, 2014, pp. 1–8.
[11] M. Sandhya, M.V.N.K. Prasad, k-nearest neighborhood structure (k-NNS) based alignment-free method for fingerprint template protection, in: Proc. of ICB 2015, 2015, pp. 386–393.
[12] M. Sandhya, M.V.N.K. Prasad, Securing fingerprint templates using fused structures, IET Biom. 6 (3) (2017) 173–182.
[13] M. Sandhya, M.V.N.K. Prasad, R.R. Chillarige, Generating cancellable fingerprint templates based on Delaunay triangle feature set construction, IET Biom. 5 (2) (2016) 131–139.
[14] 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.
[15] Neurotechnology, Verifinger SDK, http://www.neurotechnology.com.
[16] R. Cappelli, M. Ferrara, D. Maltoni, Minutia cylinder-code: a new representation and matching technique for fingerprint recognition, IEEE Trans. PAMI 32 (12) (2010) 2128–2141.
[17] R. Dwivedi, S. Dey, Score-level fusion for cancelable multi-biometric verification, Pattern Recognit. Lett. (2018).
[18] S.S. Ali, S. Prakash, Enhanced fingerprint shell, in: Proc. of SPIN 2015, 2015, pp. 801–805.
[19] S.S. Ali, S. Prakash, Fingerprint shell construction with prominent minutiae points, in: Proc. of COMPUTE 2017, ACM, 2017, pp. 91–98.
[20] S.S. Ali, S. Prakash, 3-dimensional secured fingerprint shell, Pattern Recognit. Lett. 126 (2019) 68–77.
[21] S.S. Ali, G.I. Iyappan, S. Prakash, Robust technique for fingerprint template protection, IET Biom. 7 (6) (2018) 536–549.
[22] S.S. Ali, G.I. Iyappan, S. Prakash, Fingerprint shell construction with impregnable features, J. Intell. Fuzzy Syst. 36 (5) (2019) 4091–4104.
[23] S.S. Ali, G.I. Iyappan, S. Mahyo, S. Prakash, Polynomial vault: a secure and robust fingerprint based authentication, IEEE Trans. Emerg. Top. Comput. (2019).
[24] S. Wang, J. Hu, Alignment-free cancelable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach, Pattern Recognit. 45 (12) (2012) 4129–4137.
[25] S. Wang, J. Hu, A blind system identification approach to cancelable fingerprint templates, Pattern Recognit. 54 (2016) 14–22.
[26] S. Wang, G. Deng, J. Hu, A partial hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations, Pattern Recognit. 61 (2017) 447–458.
[27] S. Wang, W. Yang, J. Hu, Design of alignment-free cancelable fingerprint templates with zoned minutia pairs, Pattern Recognit. 66 (2017) 295–301.
[28] T. Ahmad, J. Hu, S. Wang, Pair-polar coordinate-based cancelable fingerprint templates, Pattern Recognit. 44 (10) (2011) 2555–2564.
[29] W.J. Wong, A.B.J. Teoh, M.L.D. Wong, Y.H. Kho, Enhanced multi-line code for minutiae-based fingerprint template protection, Pattern Recognit. Lett. 34 (11) (2013) 1221–1229.
[30] W. Yang, J. Hu, M. S. W. Stojmenovic, An alignment-free fingerprint bio-cryptosystem based on modified voronoi neighbor structures, Pattern. Recognit. 47 (3) (2014) 1309–1320.
[31] W. Yang, J. Hu, S. Wang, J. Yang, Cancelable fingerprint templates with Delaunay triangle-based local structures, in: Cyberspace Safety and Security, Springer International Publishing, 2013, pp. 81–91.
[32] Z. Jin, A.B.J. Teoh, T.S. Ong, C. Tee, Fingerprint template protection with minutiae-based bit-string for security and privacy preserving, Expert Syst. Appl. 39 (6) (2012) 6157–6167.
[33] Z. Jin, M.H. Lim, A.B.J. Teoh, B.M. Goi, A non-invertible randomized graph-based hamming embedding for generating cancelable fingerprint template, Pattern Recognit. Lett. 42 (2014) 137–147.