Multimedia Tools and Applications (2023) 82:22795–22813
https://doi.org/10.1007/s11042-023-14576-x

FinCaT: a novel approach for fingerprint template protection using quadrant mapping via non-invertible transformation

Eain Ul Sehar[1] · Arvind Selwal[1] · Deepika Sharma[1]

Received: 19 August 2021 / Revised: 18 December 2021 / Accepted: 31 January 2023 /
Published online: 13 February 2023

Abstract
The employment of various technologies for secured human authentication in the recent years has led to rapid expansion of biometric-based recognition. Among all biometrics, the fingerprint recognition systems (FRS) hold the largest market share and have been used in numerous computing applications such as forensic, governance, and securing critical infrastructure. Though biometric systems provide plentiful benefits over the traditional identification systems but these are also susceptible to various adversarial attacks. The most crucial among all the attacks involves security breaches of stored templates in a central database that may either degrade the overall performance or result in a complete failure of the FRS. To countermeasure these attacks, template protection mechanisms are designed that mitigate the masquerade attacks or template thefts. In this study, we present a novel cancellable approach for fingerprint template protection (FinCaT) using the novel notion of quadrant mapping via a non-invertible transformation function. Our method transforms original fingerprint templates to highly secured templates by using quadrant mapping that maps minutia points by using distinct parameters in each quadrant. The FinCAT approach yields high revocability and diversity as the compromised template of a genuine user can be replaced with a newly generated secured template. The approach is experimentally evaluated on the FVC 2002 fingerprint benchmark dataset. Our technique demonstrates decent performance in terms of an equal error rate (EER) of 5.95% and a recognition accuracy of 94.05%, which is promising as compared to similar state-of-the art template protection techniques.

Keywords Cancellable biometrics · Template attacks · Template protection · Fingerprint · Quadrant mapping

✉ Eain Ul Sehar
eaini97@gmail.com

[1] Department of Computer Science and Information Technology, Central University of Jammu, Jammu & Kashmir 181143, India

1 Introduction

The biometric-based human recognition provides a genuine solution to the problems encountered in the identity representations of traditional token-based and knowledge-based systems. The significance of biometric science in today's society has been augmented by the necessity for extensive identity management systems whose operability depends on the precise ascertainment of a person's identity in relation to certain distinct applications [13]. The physical and behavioral traits (biometric traits) of an individual like fingerprint, face, iris, hand geometry, voice, gait, etc. have exhibited tremendous potential to distinguish between an adversary and a genuine person [37]. Among all the biometric traits, the fingerprint biometric has shown tremendous potential to substitute the conventional password or token-based security and person identification system. A fingerprint comprises of a specific pattern of interspersed ridges and valleys [9]. A feature set derived from these patterns is stored as a template in the template database in the fingerprint biometric system. The fingerprint biometric systems hold the largest market share in biometrics and have been used in diverse applications.

Besides providing secured authentication, the fingerprint-based biometric systems are also susceptible to a variety of attacks. Ratha et al. [25] in their study identified eight different types of attack points in a typical fingerprint biometric system [33–35]. Among all, the attack on the fingerprint templates in the database is the most severe and adverse, which may completely degrade the performance of the overall fingerprint biometric system. The fingerprint biometric trait being finite in number, any jeopardy in the fingerprint database results in permanent loss of the identity of an individual [8, 26]. The safeguarding of fingerprint template database is an onerous and crucial issue [22, 31]. To counter measure these attacks on the fingerprint template database, two broad template protection approaches have been proposed in the literature, feature transformation [5, 11, 20, 24, 27, 28, 40, 42] and biometric cryptosystem [15, 17, 23, 29, 30, 39]. The latter one requires a key to convert the template into a secured template using encryption and decryption. In cryptosystem-based template protection, some universal details about the biometric template, known as helper data, are stored. This helper data is required to draw out a key from the query feature-set during the process of matching. Where as in transformation-based template protection, a transformation function (F) is used to transmute a raw template (T) into protected-template (F (T, K)) and the transmuted template is stored in a database. Mostly, the transformation function uses an arbitrary key K as an input parameter. Before the matching, the input query feature (Q) is transmuted into protected query (F (Q, K)) using the same transformation function (F) and the transmuted query (F (Q, K)) is compared with the transmuted template (F (T, K)) [2].

In comparison to cryptosystem-based template protection, the transformation-based approaches are more popular and it requires less effort for the transformation purposes. Particularly, a lot of research work is being carried out in the field of cancellable biometrics since the last decade. One of the important issues is to design a template protection scheme that yields better performance as well as satisfies the ideal characteristics such as revocability, diversity, security and accuracy. To the best of our knowledge, several pioneer contributions from researchers have witnessed significant improvement in cancellable fingerprint template protection. One of the key concerns is to design a template security technique that besides securing the templates satisfies the ideal characteristics such a revocability, irreversibility and higher performance. Moreover, existing fingerprint

cancellable template protection schemes exhibit the problem of trade-off among various ideal parameters such as security versus revocability, size of security template vs. security, and etc. Therefore, these limitations motivated us to design a novel transformation-based cancellable template security scheme for fingerprint-based systems (FinCaT). Broad motivation of this work is to present an efficient solution that satisfies the features of an ideal template protection scheme with higher security through our proposed quadrant mapping and a non-invertible function.

The prime contributions of this study are underlined as:

i. We present a novel transformation-based template protection for scheme fingerprint trait that satisfies majority of the design criteria for an ideal template protection scheme.
ii. Our FinCaT method utilizes the proposed quadrant mapping via a non-invertible transformation function and the minutia points in each quadrant are transformed distinctly.
iii. The performance evaluation of the proposed FinCAT technique is also carried out on the FVC 2002 benchmark dataset.
iv. The security and comparative analysis of the proposed FinCaT technique demonstrates promising performance as compared to other similar methods.

The list of symbols and acronyms used in this study is provided in the Table 7 under Appendix section of this article.

The rest of the paper is structured as follows: Section 2 provides a brief literature survey of various state-of-the-art transformation-based template protection schemes. Section 3 discusses the proposed template protection scheme and the algorithms. Section 4 present the template database used, the result analysis and inferences followed by the conclusions in Section 5.

2 Related work

In this section, we review and analyze some of the state-of-the-art (SOTA) transformation-based template protection techniques. For generating a cancellable and rescindable fingerprint template, polar-grid based 3-tuple quantization (PGTQ) was proposed by Jin et al. in 2012, wherein a set of minutiae points is transformed into bit-string. Cao & Jain [8] has revealed that it is possible to rebuild the image from the fingerprint template that stores the information about minutiae points in raw and the rebuilt image can be utilized in intruding the biometric systems. Wang et al. [41] used partial discrete Fourier transform (DFT) and handmade transform in order to generate a secured fingerprint template from the minutiae points. However, the recognition performance is affected by the consequential degradation of the distinguished fingerprint features in the course of transformation. Ali et al. [4] proposed a distinctly secure scheme, which utilizes the location information regarding the minutia points to create a protected user template. Security analysis proves that this technique is very sturdy and reliable. In 2019, Atighehchi et al. proposed an improved Biohashing algorithm in which the projection matrix is produced by integrating the secret and biometric data. The proposed technique has been evaluated on FVC2002 DB1 fingerprint database, PolyFKP (knuckle print database) and VEINEGY database (dorsal hand vein

database). The experimental analysis shows that by combining the secret with biometric data, the proposed scheme has reduced the impact of the stolen-token attack. Kho et al. [19] proposed a binary cancellable fingerprint template based on an alignment-free minutiae descriptor, Partial Local Structure (PLS) and Permuted Randomized Non-Negative Least Square (PR-NNLS) optimization problem. The PLS descriptor is concatenated with the PR-NNLS to guarantee non-invertibility and cancellability of the proposed fingerprint template.

In 2020, Trivedi et al. improvised their method proposed in [36] by using Delaunay triangulation of minutiae points and user key. Some feature which does not contain any information regarding the location of minutia points is elicited from the triangle so as to obtain a non-invertible template. A modified symmetric hash method was proposed by Ajish & Anil Kumar [2] in which a key value is used as a multiplication parameter. The modified symmetric hash function is a combination of salting and non-invertible transformation. An advanced feature transformation technique was recently proposed by Jacob et al. [12], which uses DNA based encoding methodology. The Z pattern generation has been used for implementing the transformation followed by the DNA codec. Abdullahi et al. [1] proposed a novel technique for the generation of a reliable and sturdy hash from a fingerprint image using Fourier-Mellin transform and fractal coding. The proposed technique has been evaluated on FVC2002 and FVC2004 fingerprint databases. The experimental results show an average EER of 2.3325% in all six databases. The proposed method shows sturdiness and resilience to confidentiality and security attacks. Much recently, alignment-free cancellable fingerprint templates with dual protection, composed of the window-shift-XOR model and the partial discrete wavelet transform were designed by Shahzad et al. [32]. The window-shift XOR model effectively defends the ARM with simple operations and is combined with the partial DWT to provide dual protection and enhance matching performance. The designed cancellable templates satisfy non-invertibility, diversity and revocability and show superior recognition accuracy. Trivedi et al. [38] proposed a non-invertible transformation technique which uses the local geometry of the minutiae. The proposed technique introduces minutiae triangulation in which minutia points are grouped into sets to generate triplets of minutiae forming a triangle. The proposed method has been evaluated on FVC2000, FVC2004 and FVC2006 databases and produces an EER of 5.57, 2.56 and 0.478, respectively. This method satisfies all the design criteria of an ideal template protection scheme except for the revocability property. A revocable Minutia Cylinder Code-based fingerprint template protection technique has been proposed by Bedari et al. [7], which involve the utilization of a dynamic random key model known as Dyno-key model. The proposed method has been evaluated using FVC2002, FVC2004 and FVC2006 databases and yields better results in terms of EER in comparison with the existing techniques. Kavati et al. [18] proposed a novel fingerprint protection technique in which elliptical structures of minutia points are used. The proposed technique yields good results in terms of FAR and FRR. A comparison among various template security schemes is depicted in Table 1.

3 The proposed FinCAT approach

In this section, we present the framework and algorithms for our novel FinCAT method. The proposed cancellable mechanism in a fingerprint-based system is explained through a

Table 1 An overview of state-of-the-art transformation-based template protection schemes

Authors (Year)	Key concept	Dataset used	Performance (EER)	Observations	
				Strength	Weakness
Jin et al. [16]	Fingerprint binary vector using Polar-grid based 3-tuple quantization (PGTQ)	FVC2002(DB1 &DB2) and FVC2004(DB1 & DB2)	EER = 1.19%, 6.94%, 8.66% & 16.35% for respective databases	The proposed template has attained a good level of reliability	The performance deterioration as a consequence of many-to-one mapping could not be rectified
Wang et al. [41]	Generation of protected template using Partial DFT and handmade transform	FVC2002(DB1, DB2 & DB3)	EER = 1%, 2% & 5.2% for respective databases	Satisfied all the design criteria for cancellable biometrics	The recognition performance is affected by the consequential degradation of the distinguished fingerprint features in the course of transformation
Ali et al. [4]	A distinctly secure scheme that utilizes location information of the minutiae points	FVC2002(DB1, DB2 & DB3)	EER = 2%, 1% & 3.1% for respective databases	The proposed template shows good recognition accuracy	Reduces efficiency
Atighehchi et al. [6]	An improved Bio-hashing algorithm in which the projection matrix is produced by integrating the secret and biometric data	FVC2002 DB1, PolyFKP and VEINEGY	EER = 3.72% for FVC2002 database	Reduces the impact of stolen-token attack	Performance deterioration due to the assumption of random secret
Kho et al. [19]	An innovative transformation mechanism based on minutiae descriptor called Partial Local Structure (PLS) and Permuted Randomised Non-Negative Least Square (PR-NNLS) optimization	FVC2002(DB1, DB2, DB3 & DB4) and FVC2004(DB2)	EER = 0.01%, 0.06% 3.61%, 5% & 4.51% for respective databases	Satisfied all four design criteria for cancellable biometrics and avoided performance deterioration	Suffers from slight security-performance trade-off
Trivedi et al. [37]	Delaunay triangulation of minutiae points and user key to generate a cancellable fingerprint	FVC2002 (DB1 & DB2)	EER=1.2% & 2.1% for respective databases	The template is rescindable, distinctive, secure and also provides good recognition performance	_
Ajish and Kumar [3]	Modified symmetric hash method	FVC2004 DB3	Accuracy reaches to 96.09%	The modified hashed fingerprint templates are more secure than the existing hashed fingerprint templates	Vulnerable to reversibility attacks

Table 1 (continued)

Authors (Year)	Key concept	Dataset used	Performance (EER)	Observations	
				Strength	Weakness
Abdullahi et al. [1]	A secure robust hash using Fourier-Mellin transform and fractal coding	FVC2002 (DB1, DB2 &DB3) and FVC2004 (DB1, DB2 & DB3)	EER = 0.364%, 0.538%, 2.395%, 2.348%, 5.925% & 2.365% for respective databases	The proposed method shows sturdiness and resilience to confidentiality and security attacks	Incapable of detecting malicious tampering in biometric samples
Shahzad et al. [32]	Window-shift-XOR model and the partial DWT for designing alignment-free cancellable fingerprint templates with dual protection	FVC2002 (DB1, DB2 & DB3), FVC2004 (DB1 & DB2)	EER = 0%, 0%, 1.63%, 7.35% & 4.69% for respective databases	The proposed method tackles the ARM attack and satisfies all the requirements for cancellable biometrics	The designed transformation doesn't directly protect the minutiae set.

two phase process via enrollment and authentication. The framework of the proposed FinCAT approach is shown in Fig. 1, where the system comprises of two phases namely; enrollment and verification. In the enrollment phase, a user identity is stored in the system database in the form of a secured template (X_t) by applying our security algorithm. A similar mechanism is employed during authentication phase, where the presented transformed template (Q_t) is compared with stored template (X_t) of the user through a matching algorithm. The transformed templates are differently mapped through the notion of quadrant-mapping and non-invertible transformation function. It results into a more compact and secured template as original 2D features is mapped to a 1D space. An original 2D template of size n × 3 (i.e. n minutia points) extracted by the feature extractor is transformed by FinCAT to more secured template of size n.

3.1 Enrollment phase

During enrollment phase, a fingerprint image Ft(x, y) is obtained from the sensor and some requisite preprocessing is performed on it. The minutia features are acquired from the enhanced fingerprint image and lastly, the transformation function is applied on the feature vector to acquire a secured template. The notion behind the proposed FinCAT technique is explained through a systematic manner and the four broad steps are: (i) Pre-processing, (ii). Feature extraction (iii) Quadrant mapping and (iv) Non-invertible transformation function.

i. *Pre-processing*

The standard of input fingerprint images greatly determines the accuracy of minutiae extraction algorithms. Hence, several quality enhancement techniques are applied over the images to improve their quality such as estimation of local ridge orientation and frequency helps in predicting the missing ridge line & improving the ridge separations, segmentation is

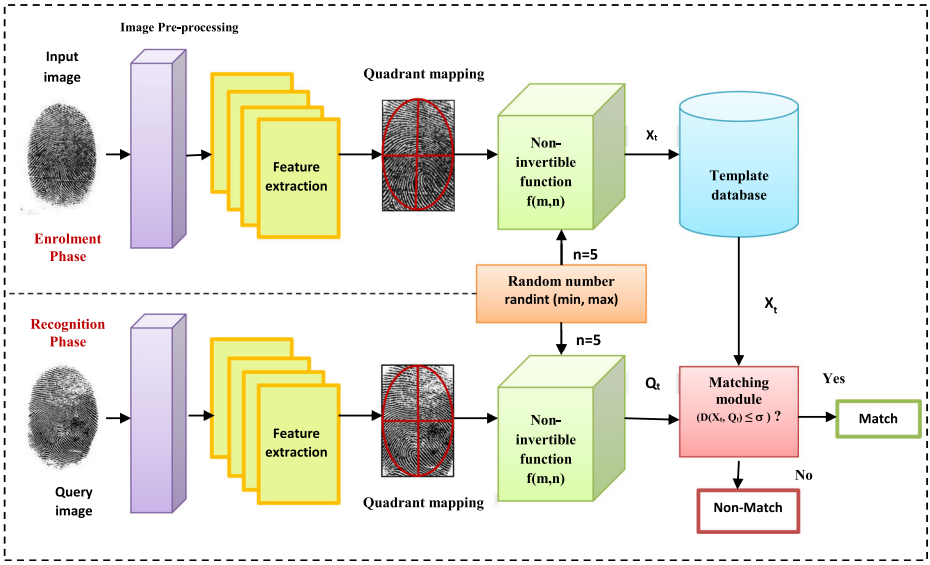

Fig. 1 Framework of the proposed FinCaT approach

used to separate the area of the fingerprint from the background and singular regions are also detected. Binarization of fingerprint image is done to convert the gray-scale image into black and white image, which provides sharper and clearer contours in the image.

ii. *Feature extraction*

The enhanced fingerprint image is subjected to the thinning operation, which removes selected foreground pixels from the digital image resulting in a thin skeleton fingerprint image. This skeleton fingerprint image is provided as an input to the feature extractor, say φ. Among the local fingerprint features, the bifurcation minutiae (where a ridge gets divided into two ridges) and termination minutiae (ridge ending points) feature points are most widely used. The coordinates of these minutia feature points are obtained as follows. If a pixel is on a thinned ridge and eight-connected, its value is 1, otherwise it is 0. Suppose a pixel (x, y) lies on a ridge and H_0: H_7 be its eight neighbors, then Eq. 1 [14] is applied.

$$\text{Type of ridge} = \left\{ \sum_{j=0}^{7} H_j = 1 | (x, y) \text{ is ridge termination} \right\} \left\{ \sum_{j=0}^{7} H_j > 2 | (x, y) \text{ is ridge bifurcation} \right\} \quad (1)$$

The orientation 'θ' of the minutiae is acquired as the computation of the angle between the ridge line and the horizontal axis of the minutiae coordinate position (x, y). Hence, the feature vector V_t (x_t, y_t, θ_t) is obtained.

iii. *Quadrant mapping*

The quadrant mapping is defined as a process in which a Euclidean coordinate system is divided into 4 distinct quadrants. A quadrant is 1/4th of a coordinate plane as shown in Fig. 2. The quadrant mapping is applied over the feature vector V_t (x_t, y_t, θ_t) containing different minutiae, obtained in the feature extraction phase.

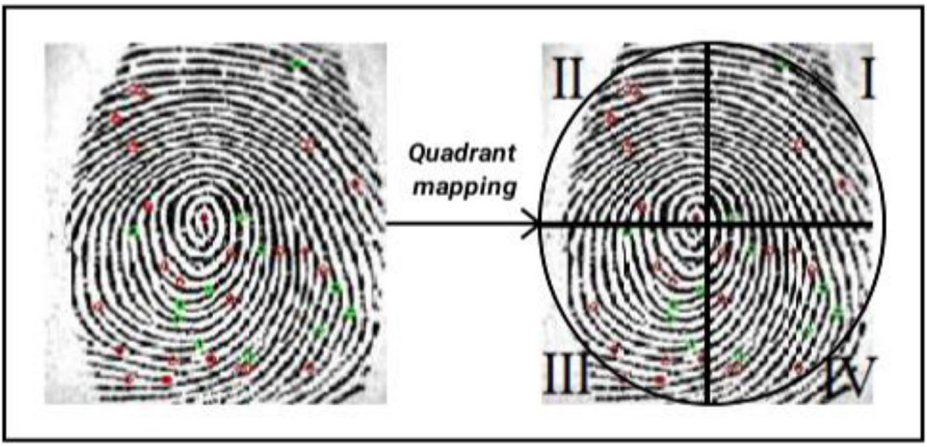

Fig. 2 An illustration of our proposed quadrant mapping

With the origin (0, 0) and θ ranging from 0° to 360°, the feature vector is divided into four quadrants I (0°- 90°), II (90°- 180°), III (180°- 270°) and IV (270°- 360°). The transformation function, when applied to distinct quadrants, takes different limit values for each quadrant in order to acquire a non-invertible template. The limit values of the transformation function are set as per the quadrant.

iv. Non-invertible transformation function

The feature vector generated by feature extraction module is transformed to a secured fingerprint template through a non-invertible function. Initially, the coordinates (i.e. x & y) of the minutiae points are concatenated to obtain a single coordinate using the Eq. 2:

$$z = x_t^2 + y_t^2 \tag{2}$$

A transformation function is applied over the four quadrants of the feature vector which takes the concatenated coordinate value 'z' and a random number 'n' as the parameters. The random number is generated using randint (min,max) function in python. The transformation function is given in Eq. 3:

$$\mathrm{f(m,n)} = \int_0^{2\pi} z \sin n\theta \; d\theta \tag{3}$$

The transformation function applied over the four quadrants takes different limits in order to make the feature vector non-invertible. The transformed minutiae in different quadrants are appended together in a secure template X_t. Hence, a secured fingerprint template X_t is generated which is stored in the template database. The whole procedure can be understood with the help of an example. Suppose an image F_t (x, y) is obtained from the fingerprint sensor. After pre-processing and feature extraction, a feature vector V_t (x_t, y_t, θ_t) is obatined, where (x_t, y_t) is the minutiae location and θ_t is the minutiae orientation. Let a minutia point be V_j^k (2, 3, 33°). Here, z = 1^2 + 2^2 = 5. Let n be 4. As θ = 33°, it lies in the first quadrant. So, the following transformation function would be applied to it.

$$1(\mathrm{m,n}) = \int_0^{\frac{\pi}{2}} z \sin n\theta \; d\theta = \int_0^{\frac{\pi}{2}} 5 \sin 4\theta \; d\theta = 5|{-}\cos 4\theta \times 4|_0^{\frac{\pi}{2}}$$

$$= -20\left|\cos\left(4 \times \frac{\pi}{2}\right) - \cos(4 \times 0)\right| = -20|cos2\pi - cos0| = -20(1-1) = 0$$

All the transformed minutiae values of the feature vector are appended in a single template X_t which is a non-invertible fingerprint template. The secure template is stored in the fingerprint template database. The algorithm for enrollment is given in Algorithm 1. The algorithm takes a fingerprint image as an input. For each image, the feature extractor extracts different features like minutiae location & orientation and these values are stored in a feature vector. For each minutia point, Eq. 2 is applied to concatenate the coordinate values into a single coordinate. After utilizing the quadrant mapping, the minutiae in each quadrant are transformed into secured minutiae. The secured minutiae are appended to a list in order to obtain a secured minutiae template. Thereafter, the resultant secured minutiae template is stored in the template database. An example showing the procedure of our algorithm is shown in Table 2, where original template is converted to corresponding secured template.

Table 2 A depiction of original minutia point and their secured values

Raw template			Secured template
x	y	θ	
1	10	0°	505
4	18	30°	1360
9	2	120	425
15	5	207	3000
22	6	190	1560
3	8	45	219
2	20	17	404
10	1	326	−1853

Algorithm 1 Algorithm for enrollment

Input: Fingerprint image $F_t(x, y)$
Output: Secured template X_t
Begin
  for i= 1 to t, **do**
    $\boldsymbol{V_i^s(x_i, y_i, \theta_i) \leftarrow \varphi(F_i)}$
    for j= 1 to t, **do**
      for k= 1 to s, **do**
        Concatenate x and y to obtain a single coordinate;
        $\boldsymbol{z = x_k^2 + y_k^2}$
        Select a random number (n)
        if $\boldsymbol{(V_j^k.\theta, 0° \le \theta \le 90°)}$
          $f^1(m,n) = \int_0^{\pi/2} \boldsymbol{z \sin n\theta \, d\theta}$
        else if $\boldsymbol{(V_j^k.\theta, 91° \le \theta \le 180°)}$
          $f^2(m,n) = \int_{\pi/2}^{\pi} \boldsymbol{z \sin n\theta \, d\theta}$
        else if $\boldsymbol{(V_j^k.\theta, 181° \le \theta \le 270°)}$
          $f^3(m,n) = \int_{\pi}^{3\pi/2} \boldsymbol{z \sin n\theta \, d\theta}$
        else if $\boldsymbol{(V_j^k.\theta, 271° \le \theta \le 360°)}$
          $f^4(m,n) = \int_{3\pi/2}^{2\pi} \boldsymbol{z \sin n\theta \, d\theta}$
        end
        X_t = []
        X_t = X_t.append(f^1, f^2, f^3, f^4)
      end
    end
    Store the secured template X_t in database
  end
end

3.2 Verification phase

Through the process of verification phase, an alike course as in the enrollment phase occurs in order to transform a query fingerprint image into a secured query template. The secured query template is compared with the stored template in the database by a matching algorithm and the similarity score

that is a Euclidean distance between two given templates. The result of the match/ non-match is generated based on the similarity score between the two templates. The Match_score $d(X_t^i, Q_t^i)$ may be computed by using Eq. 4

$$d(X_t^i, Q_t^i) = \sqrt{\left(f_i^1 - f_i^{1'}\right)^2 + \left(f_i^2 - f_i^{2'}\right)^2 + \left(f_i^3 - f_i^{3'}\right)^2 + \left(f_i^4 - f_i^{4'}\right)^2} \quad (4)$$

If the distance between the two templates is less or equal to a given threshold, say σ, the user is accepted otherwise user is rejected. The matching algorithm collates the query template with the secured template stored in the database. The collation is done by calculating the Euclidean distance between the respective minutiae points of the two templates. The algorithm to calculate the match_score is given in Algorithm 2.

Algorithm 2 Algorithm for verification

Input: Query image $I_t^i(x, y)$, Secured template X_t^i
Output: Match_score
Begin
  for i= 1 to t, **do**
    $V_i^s(x_i, y_i, \theta_i) \leftarrow \varphi(I_i)$
    for j= 1 to t, **do**
      for k= 1 to s, **do**
        Concatenate x and y to obtain a single coordinate;
        $z = x_k^2 + y_k^2$
        Select a random number (n)
        if $(V_j^k.\theta, 0° \le \theta \le 90°)$
          $f^{1'}(m,n) = \int_0^{\pi/2} z \sin n\theta \, d\theta$
        else if $(V_j^k.\theta, 91° \le \theta \le 180°)$
          $f^{2'}(m,n) = \int_{\pi/2}^{\pi} z \sin n\theta \, d\theta$
        else if $(V_j^k.\theta, 181° \le \theta \le 270°)$
          $f^{3'}(m,n) = \int_{\pi}^{3\pi/2} z \sin n\theta \, d\theta$
        else if $(V_j^k.\theta, 271° \le \theta \le 360°)$
          $f^{4'}(m,n) = \int_{3\pi/2}^{2\pi} z \sin n\theta \, d\theta$
        end
        Q_t^i= []
        Q_t^i = Q_t^i.append($f^{1'}$, $f^{2'}$, $f^{3'}$, $f^{4'}$)
      end
    end
    Match_score = $d(X_t^i, Q_t^i)$ = $\sqrt{(f_i^1 - f_i^{1'})^2 + (f_i^2 - f_i^{2'})^2 + (f_i^3 - f_i^{3'})^2 + (f_i^4 - f_i^{4'})^2}$
    if $(d(X_t^i, Q_t^i) \le \sigma)$
      User accepted
    else
      User rejected
    end
  end
end

4 Result analysis and discussions

This section discusses the database and the performance metrics used to assess the performance of the proposed FinCaT technique. It also provides the details about the different experiments performed to calculate the results.

4.1 Benchmark FVC2002 database

The majority of the methods have employed FVC2002 database to evaluate the results of their presented techniques. Therefore, the FVC2002 [21] database is used for the performance assessment of the proposed template and some sample images are shown in Fig. 3. A total number of 550 fingerprint samples are available in this dataset that were captured through optical sensor, capacitive sensor and SFinGv 2.51. The performance of fingerprint template security schemes using FVC databases is evaluated using two different protocols [10], namely FVC protocol and 1vs1 protocol. The detail of the FVC2002 dataset is summarized in Table 3.

4.2 Performance evaluation parameters

Among several parameters for designing and evaluating the proposed FinCAT approach, we use key parameters such as: quadrant mapping based on angle of the minutia feature, a transformation function, and a random number for design of FinCAT. Whereas, the threshold, false accept rate (FAR), false reject rate (FRR), equal error rate(ERR), DET curve, and ROC are used for performance evaluation. The random number is used to generate a new secured template for the user in the case when it is compromised in the dataset. The quadrant mapping and a non-invertible function ensure the more secured as well as diverse transformed template for a user. The threshold is used to evaluate our approach for effectiveness in flexible as well as more critical scenarios. On the other hand, FAR, FRR, ERR and Recognition accuracy are used for measuring the error rate of the approach so that a comparison with other similar approaches may also be carried out. Additionally, ROC and DET measures are used to find the ERR measures as some existing methods also have been evaluated on these protocols. The performance of the proposed template protection technique is evaluated using different performance metrics that are explained briefly as follows.

i. **False acceptance rate (FAR):** FAR is the fraction of imposter users accepted by the biometric system. The imposters are allowed to access the system. The value of FAR should be as low as possible.

   FAR = ((Accepted imposters) / (Total imposter trials)) × 100

ii. **False rejection rate (FRR):** FRR is the fraction of genuine users rejected by the biometric system. Although the users are genuine, they are forbidden to access the system. The value of FRR should be low.

   FRR = (Genuine users rejected) / (Total genuine trials) × 100

iii. **Genuine accept rate (GAR):** It is the proportion of genuine users felicitously accepted by the biometric system. The value of GAR should be high. It is calculated as 1 – FRR.

iv. **Equal error rate (EER):** If the performance of the system needs to be most accurate, the FAR and FRR curves must not superimpose on each other. So, the value where FAR becomes alike to FRR, the ratio is called the equal error rate. The EER value should be low.

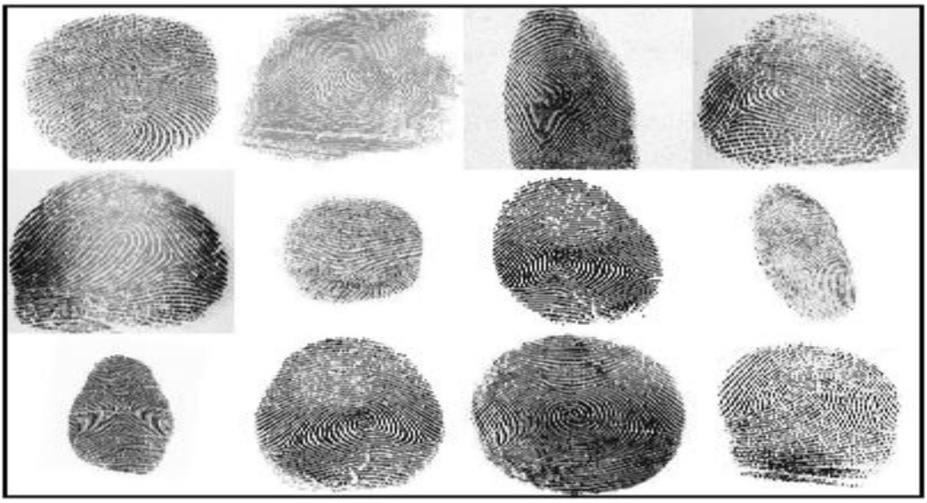

Fig. 3 Few sample images of FVC2002 database

4.3 Performance of FinCaT

In this section, we evaluate the performance of our proposed FinCaT technique through a series different experiment.

4.3.1 Recognition accuracy at different thresholds

The overall recognition accuracy of the proposed approach is evaluated after the calculation of FAR and FRR values. The FAR and FRR values are plotted against different thresholds. This gives the EER curve. EER is the point where the ratio of FAR is almost alike to the FRR and the performance of our technique is depicted in Table 4. The GAR of FinCAT at various thresholds is illustrated in Table 5. Moreover, the efficacy of FinCaT can be obeserved from Fig. 4 that shows its performance in terms of FAR versus FRR.

4.3.2 ROC evaluation for FinCaT

Receiver Operating Characteristic (ROC) curve is the graphical representation of the relationship between the Genuine Accept Rate (GAR) and the False Accept Rate (FAR). The ROC graph plots the GAR (on the Y axis) and FAR (on the X axis) for a range of

Table 3 An illustration of FVC2002 database with specifications

Database		Sensor Type	Image size	Resolution	Number of samples	Number of impressions per sample
FVC2002	**DB1**	Optical Sensor	388×374	500 dpi	110	8
	DB2	Optical Sensor	296×560	560 dpi	110	8
	DB3	Capacitive Sensor	300×300	500 dpi	110	8
	DB4	SFinGe v2.51	288×384	about 500 dpi	110	8

Table 4 Performance of the FinCaT technique at different thresholds

Threshold (%)	FAR	FRR	Recognition accuracy (%)
0.6	0.041	0.150	90.45
0.65	0.055	0.100	92.25
0.7	0.069	0.050	94.05
0.75	0.097	0.025	93.90
0.8	0.111	0.021	93.40

Table 5 Performance in terms of GAR against different thresholds

Threshold	GAR
0.6	0.850
0.65	0.900
0.7	0.950
0.75	0.975
0.8	0.979

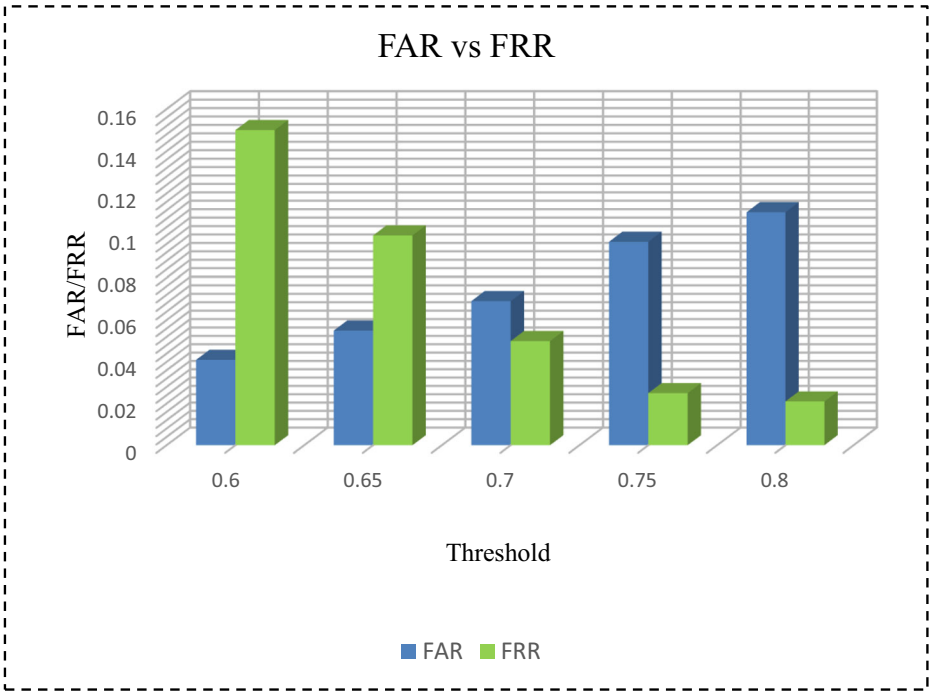

Fig. 4 Error rate of FinCaT at different thresholds

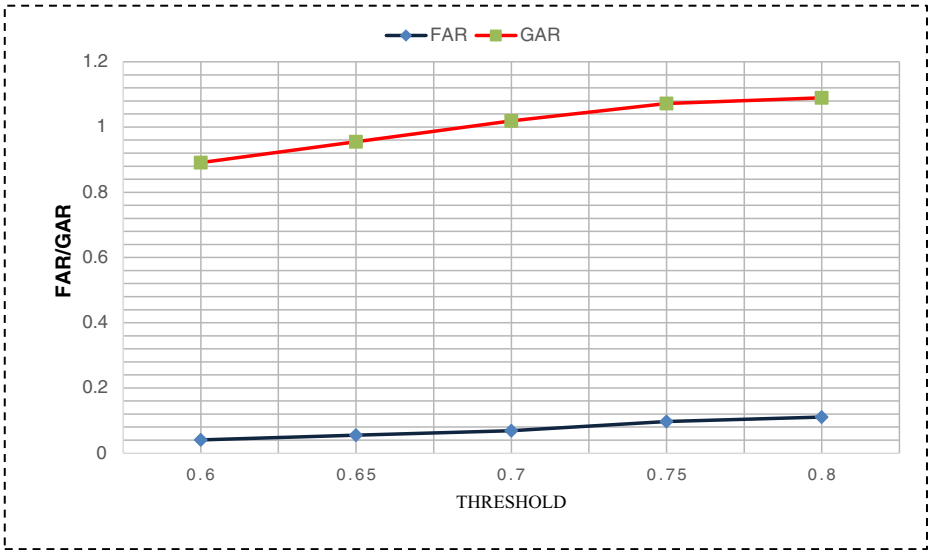

Fig. 5 A representation of ROC evaluation for FinCaT

threshold values. The best performance curve in the ROC graph is the one which is nearer to the top and the performance of our algorithm is shown in Fig. 5 [43].

4.3.3 DET curve evaluation for FinCaT

Detection Error Trade–off (DET) is the graphical plot of error rates for a range of thresholds, i.e. the graphical plot of False Reject Rate (on the Y axis) vs False Accept Rate (on the X axis)

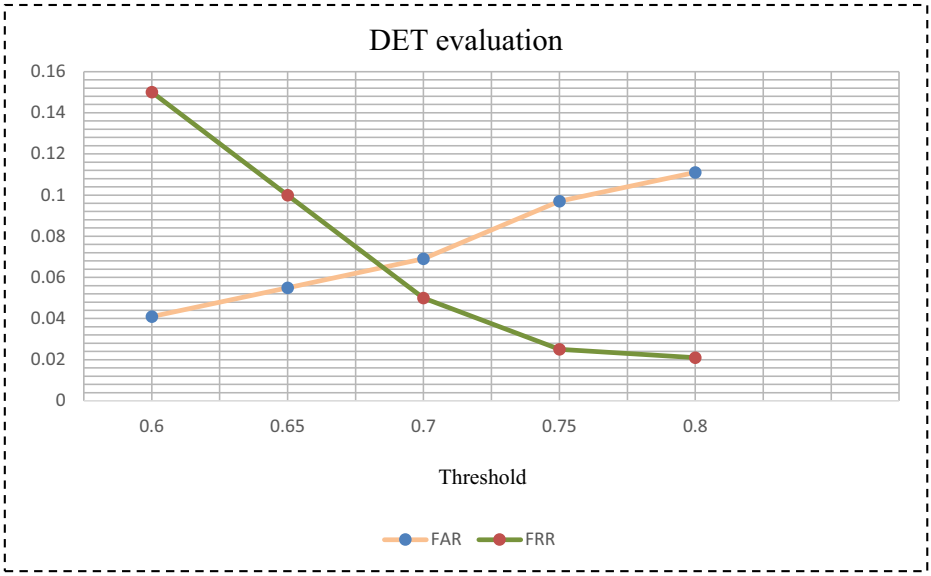

Fig. 6 DET curve evaluation of FinCaT

for a range of threshold values. The best performance curve in the DET graph is the one which close to the bottom (X axis) and it is depicted in Fig. 6.

4.3.4 Equal error rate evaluation for FinCaT

The EER is measured as the equal or at least equal or the minimum distance between the FAR and FRR. In the table 5.2, the FAR and FRR values are calculated with respect to the threshold values. The difference between the FAR and the FRR is minimum when the threshold value is 0.7. Hence, it is chosen as the decision threshold. The equal error rate (EER) at this threshold is calculated as 5.95%. Also, the recognition accuracy at this threshold value is calculated as 94.05%.

4.4 Comparison against similar techniques

The EER values of the proposed template scheme are calculated and compared with the EER values of other state-of-the-art template protection techniques for evaluation of the comparable performance. The performance comparison with existing techniques is depicted in Table 6.

4.5 Analysis of the FinCAT

The proposed technique provides better performance in terms of low error rate and high accuracy. Moreover, our FinCAT technique provides high cancellability that implies that the secured template is cancellable in nature. It infers that if the secured template is compromised, the old template can be revoked and a new generated template will be replaced instead of the compromised one. As a simple non-invertible function is used for transformation purposes as well as for the matching of templates that result in low computational complexity of the proposed technique. The original 2D feature vectors are transformed to a 1D vector that results in a compact representation of the stored templates, which further improves matching performance. The transformed templates are highly secured as it is challenging to guess the exact content of the secured template by an adversary through reverse engineering. Moreover, if an adversary is able to compromise the template, it is arduous to reconstruct the original biometric template. Therefore, masquerade attacks are significantly countered by the FinCAT. Although the proposed template protection scheme has several benefits but it still suffers from some limitations. First, the proposed approach provides limited accuracy of approximately 94.6% that may be improved. Additionally, the FinCAT approach needs to be evaluated on other recent fingerprint benchmark databases.

Table 6 Performance comparison in terms of EER with existing techniques

Author(s)	EER (%) with FVC2002 dataset
Jin et al. [16]	4.06
Wang et al. [40]	2.74
Ali et al. [4]	2.03
Atighehchi et al. [6]	3.72
Kho et al. [19]	2.17
Trivedi et al. [37]	1.65
Shahzad et al. [32]	1.63
Our proposed FinCaT technique	***5.95***

5 Conclusions

The security and privacy of fingerprint-based systems have become one the key issue due to their susceptibly to diverse range of attacks. In this study, we proposed a novel fingerprint cancellable template protection scheme to countermeasure the template database attacks. Our method utilizes a non-invertible transformation function to create a cancellable fingerprint template with the aim of escalating the security of the FRS. It can be observed that our non-invertible transformation function distorts the location of the minutia point and represent it as a single numerical point that boost the security of the original fingerprint template. The transformation function applied over the four quadrants takes different limits in order to make the feature vector non-invertible. Since the proposed secured template does not contain the minutiae's dimensional location, it is safe from fingerprint reconstruction. Our FinCAT approach yields comparable performance through secured templates in database with high revocability and diversity. The approach provides compact representation of the secured templates that require low storage as well as improved matching rate. In future, we plan to conduct more extensive experiments to evaluate FinCAT on other benchmark fingerprint datasets such as FVC 2004 and FVC 2006, and etc. Moreover, the work may be extended where the FinCAT may be applied to other biometrical traits such as iris, face and hand geometry.

Appendix

Table 7 Some symbols and acronyms with their description

Symbol/ Acronym	Meaning
DET	Detection error trade–off
DFT	Discrete Fourier transform
Dpi	Dots per inch
EER	Equal error rate
FAR	False acceptance rate
FRR	False reject rate
FRS	Fingerprint recognition system
FinCaT	Fingerprint Cancellable Template
GAR	Genuine accept rate
ROC	Receiver operating curve
PolyFKP	knuckle print database
H_j	jth Neighbor
x, y	Coordinate location of minutiae
θ	Orientation of minutiae
$F_t(x, y)$	Input fingerprint image
$I_t(x, y)$	Query fingerprint image
φ	Feature extractor
Σ	Summation
V_t (x_t, y_t, θ_t)	Feature vector
z	Concatenated value of location coordinates
n	Random number
X_t	Secured fingerprint template
Q_t	Secured query template
σ	Threshold for matching

Declarations

Conflict of interest All the authors declare that they do not have any conflict of interest.

References

1. Abdullahi SM, Wang H, Li T (2020) Fractal coding-based robust and alignment-free fingerprint image hashing. IEEE Trans Inf Forensics Secur 15:2587–2601. https://doi.org/10.1109/TIFS.2020.2971142
2. Ajish S, Anil Kumar KS (2020) Security and performance enhancement of fingerprint biometric template using symmetric hashing. Computers and Security 90:101714. https://doi.org/10.1016/j.cose.2020.101714
3. Ajish S, AnilKumar KS (2023) Performance enhancement of symmetric hashed fingerprint template using dynamic threshold matching algorithm. Int J Biometrics 15(1):78–100. https://doi.org/10.1504/ijbm.2023.127726
4. Ali SS, Ganapathi II, Prakash S (2018) Robust technique for fingerprint template protection. IET Biometrics 7(6):536–549. https://doi.org/10.1049/iet-bmt.2018.5070
5. Ali SS, Ganapathi II, Prakash S, Consul P, Mahyo S (2020) Securing biometric user template using modified minutiae attributes. Pattern Recogn Lett 129:263–270. https://doi.org/10.1016/j.patrec.2019.11.037
6. Atighehchi K, Ghammam L, Barbier M, Rosenberger C (2019) GREYC-hashing: combining biometrics and secret for enhancing the security of protected templates. Futur Gener Comput Syst 101:819–830. https://doi.org/10.1016/j.future.2019.07.022
7. Bedari A, Wang S, Yang W (2021) Design of Cancelable MCC-Based Fingerprint Templates Using Dyno-Key Model. *Pattern Recogn*:108074. https://doi.org/10.1016/j.patcog.2021.108074
8. Cao K, Jain AK (2015) Learning fingerprint reconstruction : from minutiae to image. IEEE Trans Inf Forensics Secur 10(1):104–117. https://doi.org/10.1109/TIFS.2014.2363951
9. Chaurasia P, Kohli R, Garg A (2014) Biometrics minutiae detection and feature extraction. Illustrated ed. Lambert Academic Publishing, Chisinau
10. Ferrara M, Maltoni D, Cappelli R (2012) Noninvertible minutia cylinder-code representation. IEEE Trans Inf Forensics Secur 7(6):1727–1737. https://doi.org/10.1109/TIFS.2012.2215326
11. Gao Q, Zhang C (2017) Constructing cancellable template with synthetic minutiae. IET Biometrics 6(6): 448–456. https://doi.org/10.1049/iet-bmt.2016.0192
12. Jacob IJ, Betty P, Darney PE, Raja S, Robinson YH, Julie EG (2021) Biometric template security using DNA codec based transformation. Multimed Tools Appl 80(5):7547–7566. https://doi.org/10.1007/s11042-020-10127-w
13. Jain AK, Nandakumar K, Nagar A (2008a) Biometric template security. EURASIP J Adv Signal Process 2008:579416. https://doi.org/10.1155/2008/579416
14. Jain AK, Flynn P, Ross A (2008b) Handbook of biometrics, vol 2008. Springer. https://doi.org/10.1007/9780-387-71041-9
15. Jha DP (2016). Proposed encryption algorithm for data security using matrix properties. 2016 Icicccs, 86–90. https://doi.org/10.1109/ICICCS.2016.7542316
16. Jin Z, Jin Teoh AB, Ong TS, Tee C (2012) Fingerprint template protection with minutiae-based bit-string for security and privacy preserving. Expert Syst Appl 39(6):6157–6167. https://doi.org/10.1016/j.eswa.2011.11.091
17. Juels A, Drive C, Wattenberg M, Street W (1999) A fuzzy commitment scheme. *6th ACM conference on computer and communications security,* 28–36. https://doi.org/10.1145/319709.319714
18. Kavati I, Reddy AM, Babu ES, Reddy KS (2021) Design of a fingerprint template protection scheme using elliptical structures. ICT Express 2021:4–7. https://doi.org/10.1016/j.icte.2021.04.001
19. Kho JB, Kim J, Kim IJ, Teoh ABJ (2019) Cancelable fingerprint template design with randomized non-negative least squares. Pattern Recogn 91:245–260. https://doi.org/10.1016/j.patcog.2019.01.039
20. Kho JB, Teoh ABJ, Lee W, Kim J (2020) Bit-string representation of a fingerprint image by normalized local structures. Pattern Recogn 103:107323. https://doi.org/10.1016/j.patcog.2020.107323
21. Maio D, Maltoni D, Cappelli R, Wayman JL, Jain AK (2002) FVC2002 : Second Fingerprint Verification Competition FVC2002. Second Fingerprint Verification Competition January 2008. https://doi.org/10.1109/ICPR.2002.1048144
22. Manzoor SI, Selwal A (2018) An analysis of biometric based security systems. 2018 fifth international conference on parallel, distributed and grid computing (PDGC), 4, 306–311. https://doi.org/10.1109/PDGC.2018.8745722
23. Mehmood R, Selwal A (2020) Polynomial based fuzzy vault technique for template security in fingerprint biometrics. Int Arab J Inf Technol 17(6):926–934

24. Rajan RA, Kumaran P (2019) Fingerprint template security using angle-based transformation functions. *IEEE international conference on intelligent techniques in control, optimization and signal processing, INCOS 2019*. https://doi.org/10.1109/INCOS45849.2019.8951335
25. Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40(3):614–634. https://doi.org/10.1147/sj.403.0614
26. Ross A, Shah J, Jain AK (2005) Towards reconstructing fingerprints from minutiae points. Biometric Technology for Human Identification II, 5779, 68–80. https://doi.org/10.1117/12.604477
27. Sarkar A, Singh BK (2021) A multi-instance cancelable fingerprint biometric based secure session key agreement protocol employing elliptic curve cryptography and a double hash function. Multimed Tools Appl 80(1):799–829. https://doi.org/10.1007/s11042-020-09375-7
28. Sehar EU, Selwal A, Sharma D (2021) FinCaT: fingerprint cancellable template protection remediation schemes, challenges, and future directions. 2021 fourth international conference on computational intelligence and communication technologies (CCICT), 260–267. https://doi.org/10.1109/CCICT53244.2021.00056
29. Selwal A, Gupta SK (2017) Low overhead octet indexed template security scheme for multi-modal biometric system. J Intell Fuzzy Syst 32(5):3325–3337. https://doi.org/10.3233/JIFS-169274
30. Selwal A, Kumar S (2016) Fuzzy analytic hierarchy process based template data analysis of multimodal biometric conceptual designs. *Procedia Comput Sci 85*(Cms):899–905. https://doi.org/10.1016/j.procs.2016.05.280
31. Selwal A, Gupta SK, Surender, Anubhuti (2015) Performance analysis of template data security and protection in biometric systems. 2nd international conference on recent advances in Engineering & Computational Sciences (RAECS) 2015, 1–6. https://doi.org/10.1109/RAECS.2015.7453302
32. Shahzad M, Wang S, Deng G, Yang W (2021) Alignment-free cancelable fingerprint templates with dual protection. Pattern Recogn 111:107735. https://doi.org/10.1016/j.patcog.2020.107735
33. Sharma D, Selwal A (2020) On data-driven approaches for presentation attack detection in iris recognition systems. In: Singh PK, Singh Y, Kolekar MH, Kar AK, Chhabra JK, Sen A (eds) Recent Innovations in Computing. ICRIC 2020, Lecture Notes in Electrical Engineering, p 701. https://doi.org/10.1007/978-981-15-8297-4_38
34. Sharma D, Selwal A (2021a) An intelligent approach for fingerprint presentation attack detection using ensemble learning with improved local image features. *Multimed Tools Appl* 81:22129–22161. (issue 0123456789). Springer US. https://doi.org/10.1007/s11042-021-11254-8
35. Sharma D, Selwal A (2021b) FinPAD : State-of-the-art of fingerprint presentation attack detection mechanisms, taxonomy and future perspectives. Pattern Recogn Lett 152(March 2005):225–252. https://doi.org/10.1016/j.patrec.2021.10.013
36. Trivedi AK, Thounaojam DM, Pal S (2018) A robust and non-invertible fingerprint template for fingerprint matching system. Forensic Sci Int 288:256–265. https://doi.org/10.1016/j.forsciint.2018.04.045
37. Trivedi AK, Thounaojam DM, Pal S (2020) Non-invertible cancellable fingerprint template for fingerprint biometric. Comput Secur 90:101690. https://doi.org/10.1016/j.cose.2019.101690
38. Trivedi AK, Thounaojam DM, Pal S (2021) A novel minutiae triangulation technique for non-invertible fingerprint template generation. Expert Syst Appl 186:115832. https://doi.org/10.1016/j.eswa.2021.115832
39. Uludag U, Pankanti S, Prabhakar S, Jain AK (2004) Biometric cryptosystems: issues and challenges. Proc IEEE 92(6):948–959. https://doi.org/10.1109/JPROC.2004.827372
40. Wang S, Yang W, Hu J (2017) Design of Alignment-Free Cancelable Fingerprint Templates with zoned minutia pairs. Pattern Recogn 66:295–301. https://doi.org/10.1016/j.patcog.2017.01.019
41. Wang S, Deng G, Hu J (2017a) A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. Pattern Recogn 61:447–458. https://doi.org/10.1016/j.patcog.2016.08.017
42. Wong WJ, Teoh ABJ, Kho YH, Wong ML (2016) Kernel PCA enabled bit-string representation for minutiae-based cancellable fingerprint template. Pattern Recogn 51:197–208. https://doi.org/10.1016/j.patcog.2015.09.032
43. Yang S, Berdine G (2017) The reciever operating characteristic (ROC) curve. Southwest Respir Crit Care Chron 5(19):34–36. https://doi.org/10.12746/swrccc.v5i19.391