Cancelable Template Generation Using the Tetrahedron-based Transformation Technique

A. Yoogesh
Department of Computer Applications, SRM Institute of Science and Technology, Trichy, India
a.yoogesh@gmail.com

A. Rama Prasath
Department of Computer Applications, SRM Institute of Science and Technology, Trichy, India
ramaprasath.a@ist.srmtrichy.edu.in (corresponding author)

Received: 18 June 2025 | Revised: 6 August 2025 and 19 August 2025 | Accepted: 20 August 2025

 DOI: https://doi.org/10.48084/etasr.12814

ABSTRACT

Fingerprint-based authentication systems are widely used across various domains because of their reliability and uniqueness. However, storing fingerprint minutiae as templates in a database poses significant security and privacy risks. Various studies indicate that fingerprints can be reconstructed from stored templates, which underscores the need for stronger template protection schemes. Cancelable fingerprint templates are among the best solutions to ensure that no original information is disclosed if a template is compromised. This study introduces a novel Tetrahedron-based Transformation Technique (TBTT) designed to generate irreversible and cancelable fingerprint templates. The method applies a geometric transformation to divide the plotted minutiae into three triangular parts, after which each segment undergoes a separate rotation in a defined order. The proposed approach produces a robust cancelable template that is resistant to inversion and reconstruction, while addressing risks associated with cross-matching, linking, and template inversion. Comprehensive experiments were conducted on benchmark datasets from the Fingerprint Verification Competition 2004 (FVC2004), including all accessible fingerprint images. The average recognition accuracy for datasets DB1 to DB4 is 98.86%, 95.23%, 96.17%, and 94.73%, respectively, with an average recognition time of 0.24 ms. The results demonstrate that the proposed method provides high matching accuracy and significantly improves template security.

Keywords-cancelable biometrics; fingerprint template; feature transformation; template security; fingerprint authentication; non-invertibility

I. INTRODUCTION

The increasing use of digital services has placed more focus on authenticating an identity. With the growing rate of data breaches and cyber threats, there has been a discernible shift toward ensuring that authentication systems are secure at the foundational level. In this digital world, authentication is an essential component of system security. The act of authenticating an identity has changed from passwords and PINs to biometric characteristics. Fingerprint traits are commonly favored for identity verification due to their ease of acquisition, simplicity in processing, and reliability. Because fingerprints provide distinctive features, only minimal data are required for subsequent processing, which must be securely retained in a protected format. The templates in cloud storage are secured by cancelable biometrics, where each fingerprint is distorted. The demand for secure biometric systems has increased awareness among researchers to develop improved biometric pattern recognition and protection schemes. The proposed Tetrahedron-based Transformation Technique (TBTT) generates a cancelable fingerprint template, a widely used method for securing the characteristics of a fingerprint.

The TBTT employs a localized geometric transformation technique, which partitions the minutiae points into triangular subregions, and a fixed sequence rotates each of these regions. This approach guarantees that the resultant template is non-invertible. Prior to rotation, the approach realigns the small regions with the centroid of their triangles to preserve the internal spatial connections. This contributes to making the template more secure. To maintain deterministic randomization, the index of each point is calculated modulo a fixed factor. The method keeps the local structure intact while breaking up the global structural patterns by changing the positions of small points in a systematic manner. The TBTT ensures that recreating the original minutiae arrangement remains computationally impractical.

Figure 1 illustrates the procedure of TBTT utilized in the development of the cancelable template. Despite potential obfuscation of the global configuration, the center-aligned rotation technique ensures the preservation of local intra-triangle minutiae geometry. Notwithstanding the potential compromise of certain altered templates, the TBTT ensures that the reconstruction of the original minutiae layout remains

computationally infeasible. The center-aligned rotation method preserves the local intra-triangle minutiae geometry and the global configuration. This method makes it possible to create several unlinkable and cancelable templates from a single fingerprint, which improves privacy and allows templates to be canceled in biometric systems. To assess the novel TBTT, it is essential to review notable approaches suggested in recent years, each contributing unique strategies to securing fingerprint schemes.

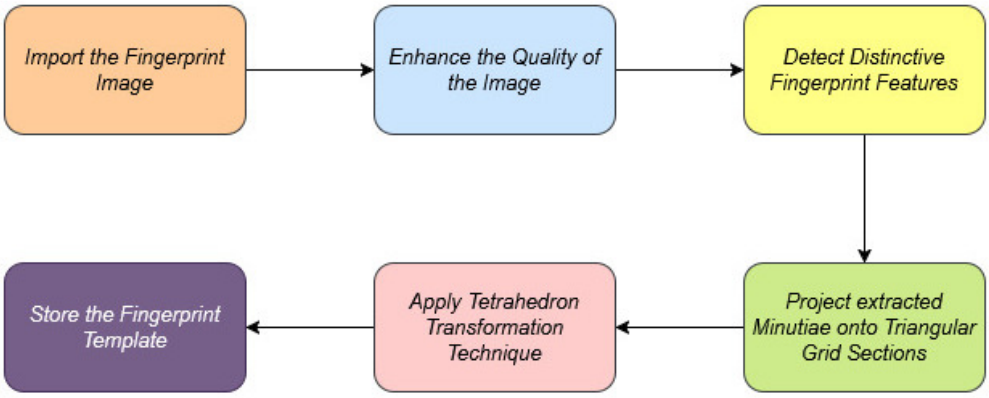


Fig. 1. TBTT procedure for generating cancelable fingerprint templates.

Fusing the fingerprint features extracted using the Delaunay triangulation mechanism with a user-specific key and bit string was proposed in [1]. Similarly, authors in [2] proposed coupling minutiae locations, orientation maps, and a key array from the user to form a non-invertible template. The algorithm in [3] claims that the combination of the Fibonacci Q-matrix with a hyper-chaotic method generates a secure non-invertible scheme. However, the accuracy of fingerprint recognition can be affected by complex transformation techniques. To address this, pairing the Linear Discriminant Analysis (LDA) with Principal Component Analysis (PCA) has been shown to provide better recognition performance [4]. The HHACOFM algorithm determines the similarity between input and cached patterns [5] and is reported to achieve efficient fingerprint recognition. Fuzzy logic, paired with a novel rotation-normalization step, enhances robustness against image distortions [6], whereas in [7], a deep learning network was trained to output fingerprints as fixed-length codes, accelerating large-scale searches. To further enhance security, authors in [8] proposed a dual authentication method integrated with Internet of Things (IoT) technologies that fuses three fingerprints in sequence to improve authentication. Additionally, authors in [9] employed Local Binary Pattern (LBP) feature extraction and biometric cryptographic key generation to safeguard the biometric parameters.

Authors in [10] described an asymmetric cipher mechanism that simultaneously encrypts two fingerprint templates using a double decomposition approach in the cross-transform domain. Authors in [11] applied a bloom filter to the result of binary features XOR key set, which helps generate a protected and irreversible template. Authors in [12] employed a double-layered method to protect the biometric template using graph theory and chaotic logistic mapping. Authors in [13] encrypted the image via confusion and diffusion to achieve a better-distorted result and ensure high security based on Shannon's principle. Authors in [14] proposed a method of integrating wavelet transform with a singular-value decomposition technique to protect fingerprint information.

The above discussion highlights the current trends in securing fingerprints. Building upon these foundations, the subsequent section elaborates on the proposed TBTT.

II. PROPOSED METHODOLOGY

The proposed TBTT begins with preprocessing and proceeds through various stages, ultimately transforming the raw fingerprints into a cancelable template. Initially, the acquired fingerprint image is converted to a grayscale format. This step is essential for subsequent filtering and enhancement phases. The preparation phase is critical for ensuring consistency, especially when managing datasets that encompass a variety of image formats. The enhancement pipeline commences with the application of Fast Fourier Transform (FFT) and Log-Gabor-based techniques to emphasize ridge patterns while reducing noise. The process of binarization converts the enhanced image into a logical matrix suitable for ridge analysis. The estimation of orientation is performed utilizing gradient-based methodologies, followed by the application of smoothing techniques to guarantee accurate identification of ridge directions, particularly in regions characterized by noise. An adaptive filter utilizes the procedure of frequency estimation and smoothing to determine the local frequency of ridges. When ridge filters are set up with local orientation and frequency maps, they make fingerprint texture more distinct, which enhances contrast and facilitates later steps. The augmented image passes through a median filter to obtain a clear image, removing any residual noise while preserving ridge characteristics. The process of binarization transforms the grayscale image into a more accurate binary mask for subsequent morphological procedures. Skeletonization renders ridge structures only one pixel wide, resulting in a simpler structure of fingerprints while retaining important pattern information.

To encompass the primary fingerprint region, a convex hull approach is applied over the skeletonized image. This hull approach removes extraneous noise outside the fingerprint boundary. A masked variant of the skeletonized image is achieved. The effectiveness of the convex hull mask is assessed through the metric Intersection over Union (IoU). This score evaluates the accuracy of the convex hull in exhibiting the structure of the fingerprint. In the later phase, adaptive histogram equalization improves the contrast of the fingerprint for precise segmentation. The process of adaptive thresholding subsequently facilitates the binarization of the image, thereby accentuating the most prominent characteristics. The Region of Interest (ROI) is determined by computing the bounding box of the connected component within the enhanced original image. This ROI defines the main fingerprint pattern while removing unnecessary background noise.

This study introduces a new TBTT function as a spatial transformation technique that manipulates the original spatial configuration of the bifurcation points of a fingerprint image. Although it displaces the spatial configuration, the orientation of each bifurcation remains geometrically coherent within localized areas. The first step splits the Feature of Interest (FoI) area of the fingerprint into triangles that create a grid pattern. The image is divided into 16 uniform segments following a grid pattern, as shown in (1), (2), and (3):

- Original set of points:

$$T = \{P_i = (x_i, y_i)\}_{i=1}^{N} \subset \mathbb{R}^2 \quad (1)$$

- Image width and height:

$$W, H \in \mathbb{N}$$

- Number of triangle divisions per axis:

$$n = 4 \quad (2)$$

- Segment size along each axis:

$$\Delta x = \left|\frac{W}{n}\right| \; \Delta y = \left|\frac{H}{n}\right| \quad (3)$$

The pixel coordinates of bifurcation points along the x (horizontal) and y (vertical) axis within each region are specified. Equations (4), (5), and (6) describe the geometric transformation applied to each triangular region: The rectangular region corresponding to row $\boldsymbol{r}$ and column $\boldsymbol{c}$ is denoted as $R_{r,c}$, where $1 \leq r, c \leq n$. The minimum and maximum coordinates along the x-axis are calculated as:

$$x_{min}^{r,c} = (C-1)\Delta x + 1, \; x_{max}^{r,c} = \min(C.\Delta x, W) \quad (4)$$

and along the y-axis as:

$$y_{min}^{r,c} = (r-1)\Delta y + 1, \; y_{max}^{r,c} = \min(r.\Delta y, H) \quad (5)$$

The centroid of each rectangular region is computed as:

$$c^{r,c} = \left(\frac{(x_{min}^{r,c} + x_{max}^{r,c})}{2} - \frac{(y_{min}^{r,c} + y_{max}^{r,c})}{2}\right) \quad (6)$$

A predetermined rotation is applied to each region $R_{r,c}$. First, the points within a region are translated so that the centroid of the region is positioned at the origin (0,0) to simplify calculations. A rotation matrix corresponding to a fixed angle is then applied to the coordinates of these points. The rotation angle θ_t is usually as 60 degrees (π/3 radians) After the rotation, the points are translated back to their original centroid positions. The rotation angle for each region is determined as:

$$R_{r,c} \; with \text{ index } t = (r-1)n + c \quad (7)$$

$$\theta_t = \frac{\pi}{3}(t \bmod 3) \quad (8)$$

A clockwise rotation is performed by applying the rotation angle θ_t in the sine and cosine functions. In this process, the algorithm adjusts the orientation of the input vectors rather than their magnitude, which helps improve the matching accuracy of the fingerprint.

The rotation angle is determined by the region index. For instance, the initial region may exhibit a rotation of 0 degrees, the next region 60 degrees, the following region 120 degrees, and so on, in a cyclical manner.

The mathematical equations for the final transformed template are given in (9) and (10):

$$p_i = (x_i, y_i) \in T \quad (9)$$

If $p_i \in R_{r,c}$, the transformed point p_i' is:

$$p_i' = R_t(p_i - c^{r,c}) + c^{r,c} \quad (10)$$

This scheme preserves spatial coherence within each triangular region while intentionally disrupting it across different regions. As a result, the global topology of the bifurcation points cannot be aligned with the initial fingerprint topology, even though local arrangements are only minimally altered. The scrambling process is deterministic; thus, if the actual scrambling parameters (specifically, the division of the grid or the sequence of rotations) could be identified, it would be possible to theoretically reverse the transformation. However, without a definite scrambling pattern, reconstructing the original template from the scrambled points would be computationally demanding.

Moreover, the local implementation of rotation in selective regions maintains compactness and minimizes the spreading of points, reducing information loss. Instead of simple randomization or complete displacement, TBTT balances security and reliability: structural disorientation provides protection, whereas limited local changes preserve matching performance. The degree of scrambling is quantified by calculating the correlation coefficient between the original bifurcation templates and the corresponding scrambled template. A low coefficient indicates effective scrambling, which enhances the security of stored fingerprint templates without significantly affecting their matching accuracy after unscrambling.

III. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, the performance assessment results of the TBTT are presented. The proposed TBTT was developed and implemented using MATLAB R2024b and the preprocessing, feature extraction, transformation, and matching were simulated using custom MATLAB scripts. The technique was evaluated using standard biometric performance metrics: False Acceptance Rate (FAR), False Rejection Rate (FRR), accuracy,

and Genuine Acceptance Rate (GAR). These metrics are sufficient to assess the reliability and overall strength of the system.

The Fingerprint Verification Competition 2004 (FVC2004) datasets used in this work are publicly available and were retrieved from the official Fingerprint Verification Competition website [15]. Table I presents the details of the sensor, image resolution, and DPI.

TABLE I. DETAILS OF FVC2004 DATASETS AND SENSOR SPECIFICATIONS

FVC2004 dataset	Equipment	Resolution (in pixels)	DPI
DB1	CrossMatch V300	640 × 480	500
DB2	Digital Persona U.are.U 4000	328 × 364	500
DB3	Atmel FingerChip	300 × 480	512
DB4	SFinGe v3.0	288 × 384	~500

A. *Performance Metrics*

The ability of the proposed TBTT method to differentiate actual and fraudulent users was calculated using average accuracy, FAR, FRR, and GAR. Time complexity was also calculated to evaluate the performance of the proposed TBTT. Lower FAR indicates better security. FAR is calculated using:

$$\text{FAR} = \frac{\text{FP}}{\text{FP+TN}} \quad (11)$$

The proposed TBTT method exhibits minimal acceptance of impostor individuals. FRR measures how often the system incorrectly rejects legitimate users and is calculated as:

$$\text{FRR} = \frac{\text{FN}}{\text{TP+FN}} \quad (12)$$

GAR assesses the correct acceptance of legitimate users and is calculated as:

$$\text{GAR} = \frac{\text{TP}}{\text{FP}} \quad (13)$$

Table II presents the computed values. Table III compares the Equal Error Rate (EER) between the existing system based on random quantization and improved bloom filter [11] and the proposed TBTT method. The evaluation includes EER, pipeline execution time, and matching accuracy. the performance values for random quantization and improved bloom filter were directly adopted from [11] as baseline standards, without re-implementation, to allow a fair comparison.

TABLE II. PERFORMANCE METRICS OF THE PROPOSED TBTT METHOD ON FVC2004 DATASETS

FVC2004 dataset	Average accuracy	FAR	FRR	GAR
DB1	98.86	0.63	0.92	99.08
DB2	95.23	1.68	2.37	97.63
DB3	96.17	1.31	1.76	98.24
DB4	94.73	1.58	2.03	97.97

From Table III, it is evident that the EER of the proposed technique is significantly lower than that of the existing system, indicating higher reliability in identifying genuine and impostor attempts. Table IV provides a comparison of the time complexity between the existing and proposed methods. The comparison shows that the proposed TBTT method executes the pipeline and matches the query fingerprint more efficiently than the existing system [11]. Figures 2 to 6 present a comparative analysis of the different performance metrics.

TABLE III. EER COMPARISON OF THE PROPOSED TBTT METHOD WITH THE EXISTING METHOD [11]

FVC2004 dataset	Existing method [11]		EER (proposed TBTT)
	ERR (same key)	ERR (different key)	
DB1	2.25	1.16	0.78
DB2	3.46	2.32	2.03
DB3	3.30	1.71	1.54
DB4	-	-	1.81

TABLE IV. TIME COMPLEXITY COMPARISON (IN SECONDS) BETWEEN THE EXISTING METHOD [11] AND THE PROPOSED TBTT METHOD

FVC2004 dataset	Existing method [11]		Proposed TBTT method	
	Pipeline execution	Matching	Pipeline execution	Matching
DB1	0.01627	0.01435	0.01491	0.01248
DB2	0.01632	0.01429	0.1523	0.01371
DB3	0.01628	0.01436	0.1476	0.01265
DB4	-	-	0.01542	0.01352

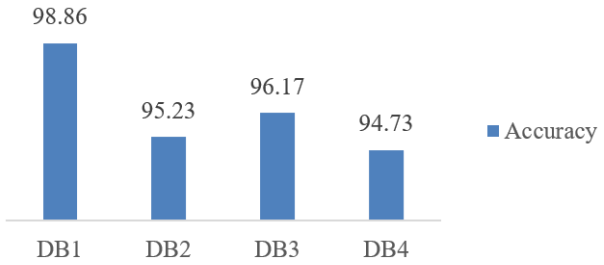


Fig. 2. Average accuracy of proposed TBTT method on FVC2004 datasets.

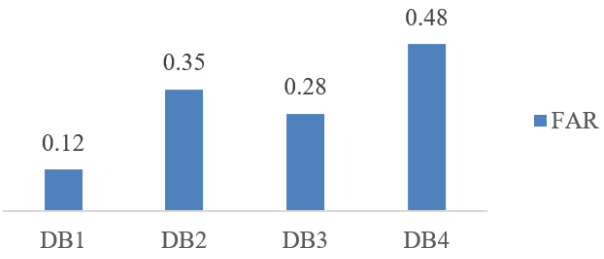


Fig. 3. FAR of proposed TBTT method on FVC2004 datasets.

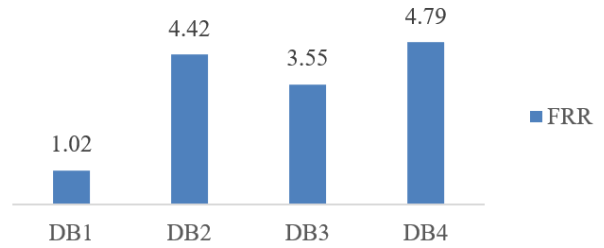


Fig. 4. FRR of proposed TBTT method on FVC2004 datasets.

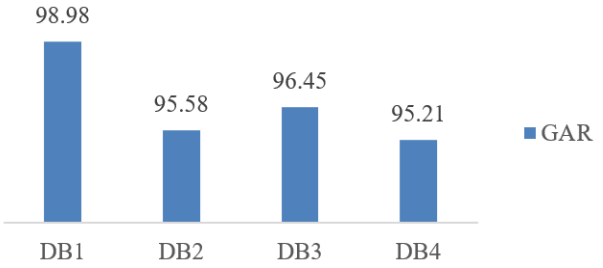


Fig. 5. GAR of proposed TBTT method on FVC2004 datasets.

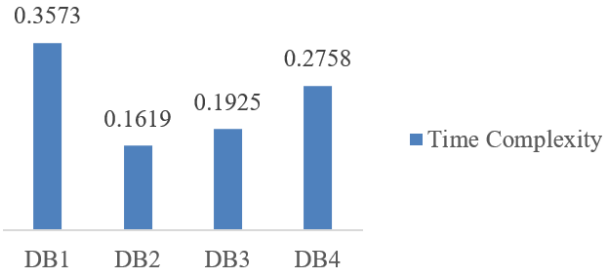


Fig. 6. Time complexity of proposed TBTT method on FVC2004 datasets.

The correlation ratio measures the similarity between the original and transformed images. A lower correlation ratio indicates a higher degree of transformation applied to the fingerprint. Table V and Figure 7 present the correlation ratios of the fingerprints.

TABLE V. CORRELATION RATIOS BETWEEN ORIGINAL AND TRANSFORMED FINGERPRINTS

FVC2004 dataset	File name (.tif)	Correlation ratio
DB1	101_1	0.0605
	101_2	0.0519
	101_3	0.0391
	101_4	0.0318
DB2	102_5	0.0476
	104_6	0.0627
	105_7	0.0365
DB3	103_8	0.0441
	104_1	0.0661
	104_2	0.0532
DB4	102_1	0.0423
	102_2	0.0597
	102_3	0.0494

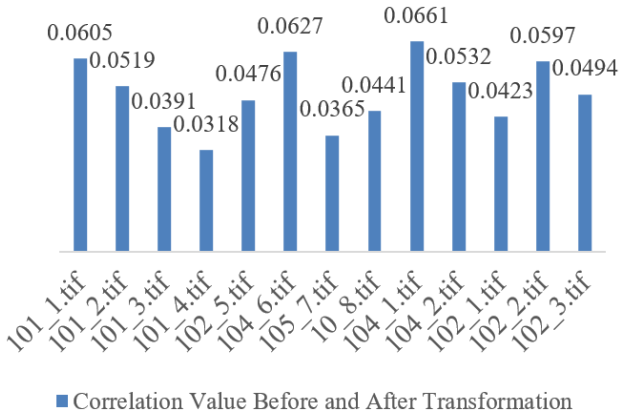


Fig. 7. Correlation ratios between original and transformed fingerprints.

B. Visual Results

This section presents the visual results of the images processed by the proposed TBTT method, highlighting each major step of the transformation pipeline. Figure 8 presents sample median-filtered fingerprint images. Figure 9 displays the specially masked ROIs, clearly isolating the relevant fingerprint area from the background. Figure 10 illustrates the plotted minutiae (bifurcations) within the masked ROIs, emphasizing the key features used for matching. Figure 11 shows the scrambled minutiae points generated by the proposed TBTT method.

(a) (b) (c)

Fig. 8. Median-filtered fingerprint images: (a), (b), (c) sample images.

(a) (b) (c)

Fig. 9. Masked ROIs for fingerprint images: (a), (b), (c) sample images.

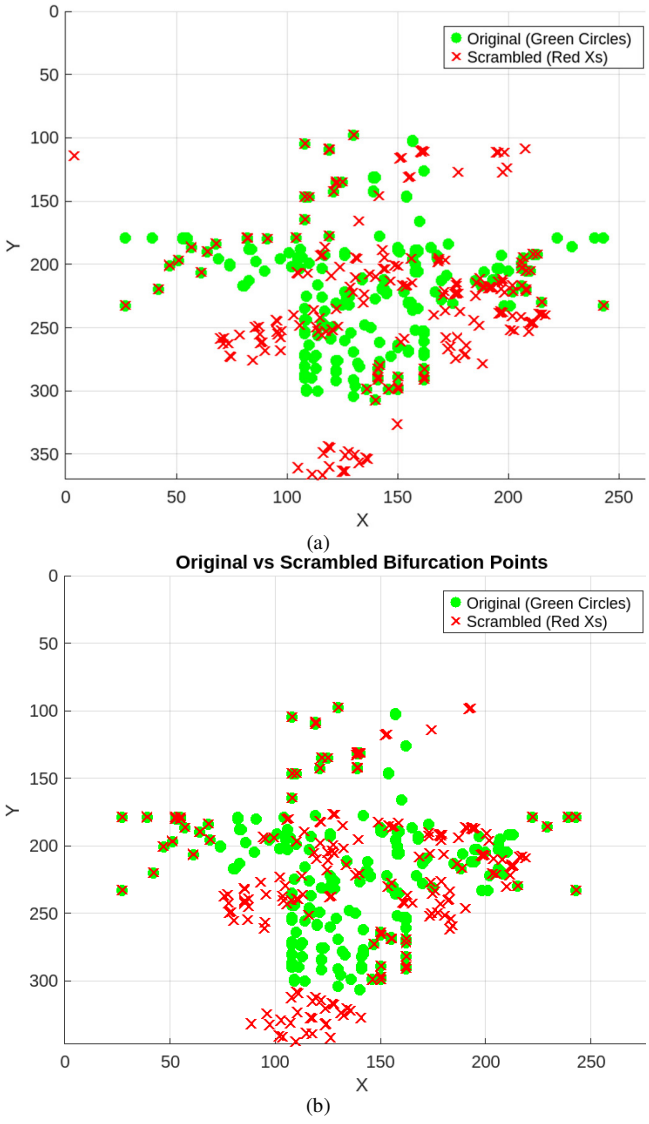
(a) (b) (c)

Fig. 10. Plotted minutiae (bifurcation points) in the masked ROIs: (a), (b), (c) sample images.

(a) (b) (c)

Fig. 11. Scrambled minutiae points based on the proposed TBTT method: (a), (b), (c) sample images.

Finally, Figure 12 presents the minutiae positions before and after applying the proposed TBTT method, emphasizing how local details are preserved.



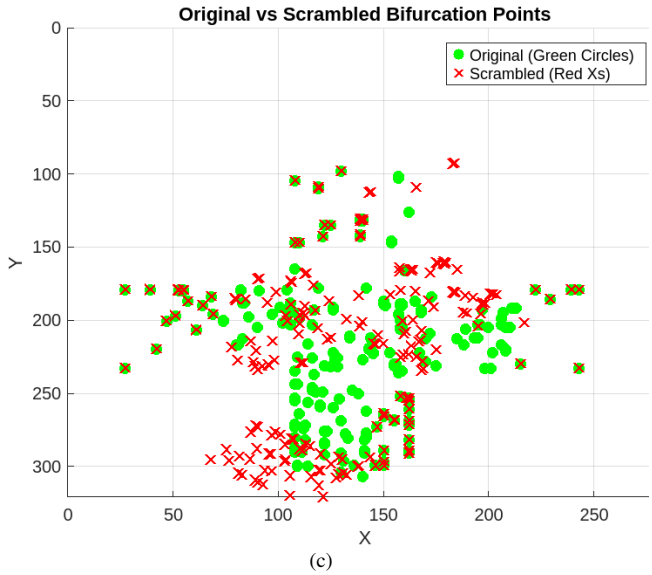


Fig. 12. Original and transformed minutiae points showing the effect of TBTT transformation: (a), (b), (c) sample images.

IV. CONCLUSION

This work demonstrates that the Tetrahedron-based Transformation Technique (TBTT) is a robust and effective approach for protecting fingerprint templates. The technique ensures strong non-invertibility and resilience against reverse engineering by applying irreversible geometric transformations that segment the minutiae template into triangular regions and rotate them independently.

The proposed TBTT was evaluated on the Fingerprint Verification Competition 2004 (FVC2004) datasets DB1–DB4, with average accuracies of 98.86%, 95.23%, 96.17%, and 94.73%, respectively. Furthermore, the algorithm demonstrates minimal recognition response time of 0.24 ms, along with low False Acceptance Rate (FAR) and False Rejection Rate (FRR).

The TBTT method also significantly improves efficiency, as each protected template requires only 4 KB of storage compared to 300 KB for storing full fingerprint images, resulting in substantial storage savings. Overall, the TBTT method provides a cancelable, compact, and computationally efficient solution for fingerprint template protection.

REFERENCES

[1] A. Hayat, S. S. Ali, A. K. Bhateja, and N. Werghi, "FinTem: A secure and non-invertible technique for fingerprint template protection," *Computers & Security*, vol. 142, Jul. 2024, Art. no. 103876, https://doi.org/10.1016/j.cose.2024.103876.

[2] V. S. Baghel, S. S. Ali, and S. Prakash, "A non-invertible transformation based technique to protect a fingerprint template," *IET Image Processing*, vol. 17, no. 13, pp. 3645–3659, Nov. 2023, https://doi.org/10.1049/ipr2.12130.

[3] F. A. Hossam Eldein Mohamed and W. El-Shafai, "Cancelable biometric authentication system based on hyperchaotic technique and fibonacci Q-Matrix," *Multimedia Tools and Applications*, vol. 83, no. 23, pp. 63755–63793, Jul. 2024, https://doi.org/10.1007/s11042-023-17855-9.

[4] A. Khan and H. Farooq, "Principal Component Analysis-Linear Discriminant Analysis Feature Extractor for Pattern Recognition." arXiv, Apr. 05, 2012, https://doi.org/10.48550/arXiv.1204.1177.

[5] N. K. Sreeja, "A hierarchical heterogeneous ant colony optimization based fingerprint recognition system," *Intelligent Systems with Applications*, vol. 17, Feb. 2023, Art. no. 200180, https://doi.org/10.1016/j.iswa.2023.200180.

[6] A. A. Momani and L. T. Kóczy, "A robust fingerprint identification approach using a fuzzy system and novel rotation method," *Pattern Recognition*, vol. 159, Mar. 2025, Art. no. 111134, https://doi.org/10.1016/j.patcog.2024.111134.

[7] J. J. Engelsma, K. Cao, and A. K. Jain, "Learning a Fixed-Length Fingerprint Representation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 43, no. 6, pp. 1981–1997, Jun. 2021, https://doi.org/10.1109/TPAMI.2019.2961349.

[8] A. A. Alzhrani, M. Balfaqih, F. Alsenani, M. Alharthi, A. Alshehri, and Z. Balfagih, "Design and Implementation of an IoT-Integrated Smart Locker System utilizing Facial Recognition Technology," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 16000–16010, Aug. 2024, https://doi.org/10.48084/etasr.7737.

[9] M. H. Algarni, "Fingerprint Sequencing: An Authentication Mechanism that Integrates Fingerprints and a Knowledge-based Methodology to Promote Security and Usability," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 14233–14239, Jun. 2024, https://doi.org/10.48084/etasr.7250.

[10] P. Rakheja, "An asymmetric double fingerprint template encryption using twin decomposition technique in hybrid transform domain," *Multimedia Tools and Applications*, vol. 84, no. 9, pp. 6687–6709, Mar. 2025, https://doi.org/10.1007/s11042-024-19100-3.

[11] M. S. Khan, H. Li, Y. Sun, and C. Zhao, "Cancelable fingerprint template protection based on random quantization and improved bloom filter," *Multimedia Tools and Applications*, vol. 84, no. 17, pp. 17547–17579, May 2025, https://doi.org/10.1007/s11042-024-19692-w.

[12] W. El-Shafai, A. El-Mesady, and F. M. Kamal, "Enhancing biometric authentication security through the novel integration of graph theory encryption and chaotic logistic mapping," *Multimedia Tools and Applications*, vol. 84, no. 16, pp. 16909–16943, May 2025, https://doi.org/10.1007/s11042-024-19693-9.

[13] A. H. A. El-aziem, A. Abdelhafeez, and T. H. M. Soliman, "A Proposed Cancelable Biometrical Recognition System (CBRS) Based on Developed Hénon Chaotic-Map," *Wireless Personal Communications*, Jan. 2024, https://doi.org/10.1007/s11277-023-10823-4.

[14] C. Liu, Z. Zhi, W. Zhao, and Z. He, "Research on Fingerprint Image Differential Privacy Protection Publishing Method Based on Wavelet Transform and Singular Value Decomposition Technology," *IEEE Access*, vol. 12, pp. 28417–28436, 2024, https://doi.org/10.1109/ACCESS.2024.3367996.

[15] "FVC2004: the Third International Fingerprint Verification Competition." University of Bologna. http://bias.csr.unibo.it/fvc2004/.