Generation of Cancellable and Irrevocable Fingerprint Biometric Templates Using Quadrant Shift Modulation Transformation

T. Jennifer
Department of Computer Applications, SRM Institute of Science and Technology, Trichy, India
pradeep.jenni@gmail.com

K. Kanagalakshmi
Department of Computer Applications, SRM Institute of Science and Technology, Trichy, India
kkanagalakshmi@gmail.com (corresponding author)

Received: 11 May 2025 | Revised: 25 July 2025 and 12 August 2025 | Accepted: 14 August 2025

 DOI: https://doi.org/10.48084/etasr.12072

ABSTRACT

Cancellable biometrics support multiplicity by allowing the generation of multiple secure templates from the same biometric data. In recent years, biometric technologies have advanced beyond conventional identification and authentication techniques, making template protection an increasingly critical requirement. Because biometric data are unique to each individual, it is essential to preserve and cross-reference original features across applications. However, once compromised, biometric data cannot be recovered, highlighting the need for secure, revocable representations. In this study, we present Quadrant Shift Modulation (QSM), a patented technique designed to achieve both cancelability and irrevocability of biometric traits. Biometric authentication remains a reliable and user-friendly method of personal identification, yet protecting stored biometric data from malicious attacks remains challenging. The proposed QSM algorithm focuses on creating and protecting fingerprint templates by employing quadrant shift and quadrant swap operations to generate cancellable templates. Experimental evaluation using the Fingerprint Verification Competition 2004 (FVC2004) dataset demonstrates that the QSM system achieves 97.79% accuracy, an average Genuine Acceptance Rate (GAR) of 92.25%, and a False Rejection Rate (FRR) of 7.75%, confirming its effectiveness.

Keywords-biometrics; fingerprint; bit-shifting; cancellable template; minutiae points;transformation;Q-shift; Q-swap

I. INTRODUCTION

Cancellable biometrics offer a strategic way to ensure diversity, security, and privacy in biometric systems. As biometric authentication becomes more prevalent in modern identity verification, replacing traditional methods like passwords, PINs, and physical tokens, concerns about the permanence and traceability of biometric data have intensified [1]. Since biometric traits are unique and irreplaceable, any compromise poses a permanent security risk. To address these issues, we propose a novel technique called Quadrant Shift Modulation (QSM), which generates biometric templates that are both cancellable and irreversible. This method aims to prevent the recovery of original biometric data while enabling the reissuance of new templates if the existing ones are compromised.

Unlike conventional authentication systems that are prone to theft and misuse, biometric systems utilize distinct physiological or behavioral characteristics to enhance security [2]. Fingerprints, due to their uniqueness and permanence, are widely used across sectors, including commercial applications (e.g., smartphones, banking), governmental applications (e.g., passports, national IDs), and forensic applications. However, despite their reliability, biometrics pose privacy risks, such as unauthorized tracking and non-revocability. Cancellable biometrics mitigate these risks by applying non-invertible, repeatable transformations to biometric data, supporting key goals such as diversity, reusability, non-invertibility, and high recognition accuracy [3]. In this work, we focus on fingerprint template protection using the QSM method, which ensures secure, private, and robust authentication.

II. RELATED WORK

Biometric template protection has become a critical area of research, as it aims to generate cancellable and irreversible templates while maintaining high recognition accuracy. One such technique, known as Shift-Phase Transformation (SPT), addresses biometric security threats by creating irreversible and cancellable fingerprint templates, with its correctness, security, and efficiency confirmed by experimental data [4]. Authors in

[5] proposed a secure fingerprint system that extracts binary features from ridges and minutiae to enable integration with cryptosystems and Hamming distance matching, with accuracy and robustness further improved by including core and delta points.

The Optimal Iterative Solubility (OIS) algorithm, specifically designed to generate the coefficient matrix required in template protection, has been employed in fingerprint template protection techniques. Enrollment and authentication are the two main stages of such systems, with the OIS algorithm, minutiae points, and a Secure Point Base (SPB) framework used to extract an identification vector during the enrollment process [6].

The cancellable biometric model based on Snake and Ladder (SNL) offers a new approach for secure fingerprint authentication. Authors in [7] utilized the principle of multi-source fusion to improve template diversity and security by creating a virtual identity. Authors in [8] proposed a fingerprint template protection method based on the CiKX transform and Tanimoto similarity measure, which enhances template security and diversity by generating robust and unique representations of biometric data.

Despite these advances, stored fingerprint templates remain vulnerable to attacks such as replay, reconstruction, and cross-matching [9]. Although many template protection techniques are currently in use, they have not achieved complete defense against such attacks. More reliable and irreversible transformation techniques are required, as studies have demonstrated that original fingerprint patterns can be reverse-engineered from stored templates with sufficient supplementary information [10].

Biometric attributes are preferable to previous systems because they are permanent and distinct, but they can also cause long-term harm if data are released. Therefore, contemporary biometric systems require enhancement using advanced template protection methods such as visual cryptography, homomorphic encryption, hybrid models, biometric cryptosystems, and cancellable biometrics, while maintaining cost efficiency and usability. Authors in [11] also emphasize safeguarding user privacy and address issues with raw biometric data by proposing methods such as Bloom filter-based template protection. Furthermore, a weighted feature-level fusion technique is suggested to enhance privacy and recognition accuracy.

Authors in [12] propose a fast and reliable minutiae extraction method that operates directly on binary fingerprint images using run-length coding, eliminating the need for thinning. Authors in [13] enhance adaptive fingerprint image processing through contextual filtering with automatically adjusted parameters, improving preprocessing, global and local analysis, and matched filtering.

III. PREPROCESSING TECHNIQUES

Each stage of the preprocessing procedure follows a specific strategy to achieve its objectives [14]. This strategy involves four main steps, described below: image preprocessing, image augmentation/noise removal, ridge extraction, and the definition of a Region of Interest (ROI). Subsequently, Feature of Interest (FOI) detection enables the generation of biometric templates that are both cancellable and irrevocable using QSM.

- Image preprocessing: This step aims to improve the visibility of ridge patterns in fingerprint images, which may be blurry or low-contrast, as shown in Figure 1 [15]. Techniques such as histogram equalization are applied to adjust contrast, spreading the pixel intensity range so that ridge patterns become clearer. These enhancements ensure sufficient image quality for subsequent processing stages, such as feature extraction.

- Image augmentation / noise removal: Noise can arise from low image quality, scanning errors, or environmental conditions. To eliminate unwanted artifacts that could affect fingerprint properties, noise removal is applied [16]. Median filtering replaces each pixel with the median of its neighbors, effectively removing "salt-and-pepper" noise, whereas Gaussian filtering preserves ridge sharpness and reduces high-frequency noise (Figure 2).

- Ridge extraction and thinning: Finger placement on the scanner can introduce distortions. Orientation field estimation, typically using gradient-based or frequency-based techniques, adjusts the fingerprint image to ensure precise alignment [17]. Ridge thinning reduces the ridge width to a single pixel, preserving essential ridge structure while enabling accurate feature extraction [18] (Figure 3).

- ROI detection: The ROI focuses computation on the most relevant portions of a fingerprint image, which is particularly important in systems with limited processing power or when handling large datasets [19]. By concentrating on the ROI, unnecessary areas are excluded, leading to faster processing and improved algorithmic efficiency. In fingerprint recognition systems, the ROI typically corresponds to the central portion of the fingerprint, excluding peripheral regions where image quality often degrades due to distortion, noise, or incomplete ridge patterns (Figure 4). A practical method for defining the ROI involves dividing the fingerprint image into four equal quadrants and selecting the quadrant that contains the core fingerprint characteristics, such as minutiae points and ridge patterns [20]. This approach ensures the ROI is centered, square-shaped, and strictly within the fingerprint boundaries, excluding irrelevant or distorted areas.

FOIs refer to bifurcations and ridge endings, which are critical for accurate fingerprint recognition and matching. Using a square-shaped ROI derived from quadrant division makes FOI detection more focused and efficient (Figure 5). Dividing the image into quadrants isolates the central region of the fingerprint, where core features are concentrated. By examining the ridge flow within this region, the system can precisely detect where ridges split or terminate, identifying the minutiae points essential for recognition. This quadrant-based method streamlines the detection process, enhances reliability, and improves the overall accuracy and performance of the fingerprint recognition system [21-25].

Finally, a homomorphic encryption mechanism is applied to the image after preprocessing to protect sensitive information [26].

Fig. 1. Original fingerprint image.

Fig. 2. Fingerprint image after noise removal.

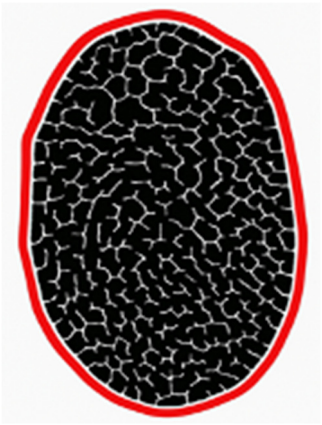

Fig. 3. Fingerprint image after ridge extraction.

Fig. 4. ROI selection in the fingerprint image.

Fig. 5. Minutiae marking within the ROI.

IV. MATERIALS AND METHODS

Biometric data are highly sensitive and cannot always be kept entirely confidential, making robust protection essential. Biometric template protection methods aim to secure these data against unauthorized access and misuse. With growing reliance on biometric systems, ensuring data privacy has become a critical area of research [22].

A. Materials

The Fingerprint Verification Competition 2002 and 2004 (FVC2002 and FVC2004) datasets were utilized to assess the QSM algorithm's performance for fingerprint template protection. These databases contain 80 fingerprint images collected using a standardized setup during the April 2004 competition. This are widely used benchmark dataset that help assess the accuracy and robustness of fingerprint recognition and protection methods in biometric security research [27].

B. Proposed Method: Quadrant Shift Modulation

The block diagram of the proposed method is shown in Figure 6. The QSM algorithm is a reliable and efficient technique for ensuring the irrevocability and cancelability of fingerprint templates. A key feature of this biometric method is cancelability, which enables the reuse of biometric traits rather than the creation of new ones. This prevents unauthorized access by allowing the rapid regeneration of a new template using the same biometric information. Irrevocability reduces security risks and protects user data from potential leakage by ensuring that the recorded fingerprint template cannot be reversed or reconstructed.

The proposed QSM algorithm effectively addresses the challenges of biometric template protection by employing the Quadrant Shift (QSh) and Quadrant Swap (QSw) techniques. These methods provide a highly secure and performance-driven solution for enhancing the protection of fingerprint templates. QSh involves shifting the fingerprint data within specific quadrants, disrupting the spatial arrangement of biometric features while maintaining their inherent structure. This adds an additional layer of security, making it more difficult for unauthorized parties to extract sensitive information. QSw further strengthens the protection by swapping the quadrants of the fingerprint template, further obfuscating the original data.

This technique guarantees that even in the event that an attacker manages to access the template, reconstructing the original fingerprint is practically impossible. Together, these techniques make the QSM algorithm highly effective in safeguarding biometric data, offering a balance between security and performance while preserving the integrity and uniqueness of the biometric template.

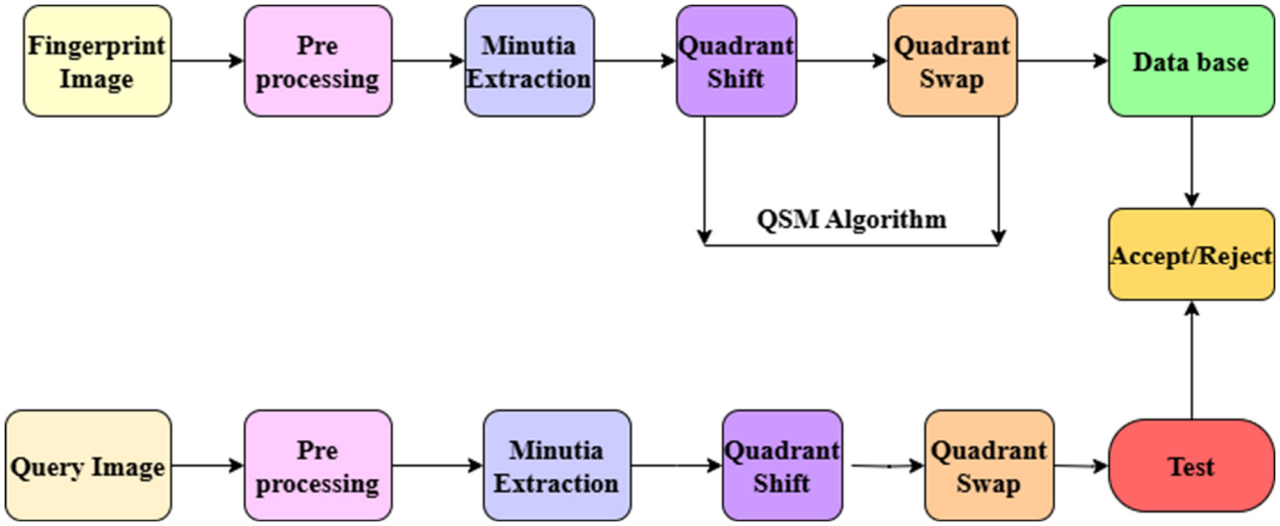

Fig. 6. Block diagram of the QSM algorithm.

C. *Quadrant Shift*

The fingerprint image is typically divided into four equal sections by splitting the image both horizontally and vertically. Each quadrant represents a distinct portion of the fingerprint, often containing critical features such as ridges and minutiae points [19]. This division allows focused processing of individual sections, making it easier to analyze specific features and enhance template security.

The QSh technique introduces a sophisticated layer of security by applying differential bit-shifting operations to the four quadrants of a fingerprint image, based on their odd or even positional designation [23]. Odd-numbered quadrants ($Q1$ and $Q3$) undergo right shifts, whereas even-numbered quadrants ($Q2$ and $Q4$) undergo left shifts. This differential shifting disrupts the spatial arrangement of the fingerprint, dispersing critical information across the image and increasing resistance to unauthorized access. The transformation can be summarized as follows:

- $Q1$–Right shift for odd quadrants:

  For $(x, y) \in Q_1$: $P_{new}(x, y) = \left\lfloor \frac{P(x,y)}{2^n} \right\rfloor$ (1)

  Here, $P(x, y)$ is the original pixel value at position (x, y), 2^n represents the bit-shifting factor, where n is the number of bits to shift. For example, $n = 1$ performs a division by 2, $n = 2$ performs a division by 4, and so forth. The result $P_{new}(x, y)$ is the transformed pixel value.

- $Q2$ – Left shift for even quadrants:

  For $(x, y) \in Q_2$: $P_{new}(x, y) = (P(x, y) \ll n) \bmod 2^b$ (2)

  Here, $P(x, y)$ is the original pixel value at (x, y). The operator $\ll n$ denotes a left bitwise shift by n positions. The modulus $\bmod 2^b$ ensures the pixel intensity remains within the valid range $[0, 2^b - 1]$, where b is the image's bit depth. The resulting $P_{new}(x, y)$ is the final pixel value after transformation.

- $Q3$ – Right shift for odd quadrants:

  For $(x, y) \in Q_3$: $P_{new}(x, y) = \left\lfloor \frac{P(x,y)}{2^n} \right\rfloor$ (3)

  This operation mirrors $Q1$ and is applied to Quadrant 3 pixels.

- $Q4$ – Left shift for even quadrants:

  For $(x, y) \in Q_4$: $P_{new}(x, y) = (P(x, y) \ll n) \bmod 2^b$ (4)

  This operation mirrors $Q2$ and is applied to Quadrant 4 pixels.

By drastically changing the fingerprint's representation, this transformation obfuscates the biometric data and makes it much more difficult for attackers to reverse-engineer its properties or recreate the original template. The differential disperses critical information across different areas of the image. As a result, even if parts of the template are exposed, the remaining sections are rendered unusable and cannot be easily pieced together. This method ensures that unauthorized users cannot easily extract identifiable features from any single quadrant, adding a robust layer of security to the fingerprint data. Ultimately, the QSh technique provides a powerful means of safeguarding biometric information, ensuring that any compromised portion of the template does not lead to the exposure of the entire fingerprint.

D. Quadrant Swap

After performing the QSh operation, the next critical transformation step is QSw. This step further obscures the spatial structure of the fingerprint data, making the template non-invertible and resistant to reverse engineering.

The primary goal of quadrant swapping is to enhance template security by ensuring non-invertibility and diversity. Since the spatial layout of minutiae and ridge patterns plays a crucial role in biometric identification, altering their global positions without modifying their internal structures provides effective protection against template reconstruction attacks [28].

Additionally, the QSw operation is non-linear and key-dependent, meaning that different swapping sequences can be generated using predefined keys or random seeds. This property enables cancelability, as a compromised template can be revoked and replaced by generating a new swapping pattern without requiring new biometric data. Thus, QSw acts as a powerful post-processing step that complements bit-level transformations and provides a strong foundation for biometric template protection schemes. The transformation can be expressed as follows for the swap pattern $Q_1 \leftrightarrow Q_2, Q_3 \leftrightarrow Q_4$:

$$P_{swap}(x,y) = \begin{cases} P_{Q2}(x,y), & \text{if}(x,y) \in Q_1 \\ P_{Q1}(x,y), & \text{if}(x,y) \in Q_2 \\ P_{Q4}(x,y), & \text{if}(x,y) \in Q_3 \\ P_{Q3}(x,y), & \text{if}(x,y) \in Q_4 \end{cases} \quad (5)$$

where $P_{Qi}(x,y)$ is the pixel from the respective quadrant before the swap, and $P_{swap}(x,y)$ is the pixel value after swapping.

V. PERFORMANCE EVALUATION OF THE PROPOSED METHOD

This section presents the results obtained using the QSM algorithm. The algorithm was implemented in MATLAB, and its performance was assessed using standard fingerprint datasets. Figures 7, 8, and 9 illustrate the outputs of key steps in the proposed QSM model: the original fingerprint image, the selected ROI, and the minutiae-marked image, respectively.

Fig. 7. Original fingerprint image.

Fig. 8. Square-shaped ROI on the fingerprint image.

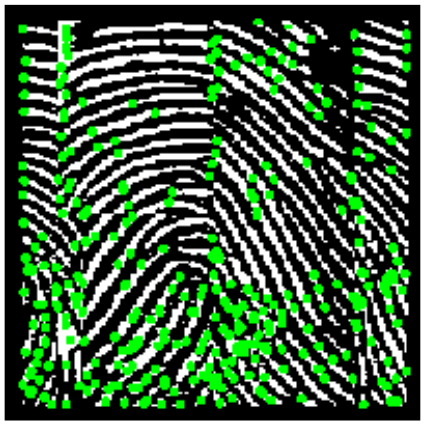

Fig. 9. Minutiae-marked image within the ROI.

A. Performance Metrics

The effectiveness of the QSM algorithm is evaluated using several commonly used biometric metrics: Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), and Genuine Acceptance Rate (GAR). Table I summarizes these metrics for the tested datasets.

TABLE I. PERFORMANCE METRICS OF THE QSM METHOD ON THE FVC2004 DATASET

Dataset (FVC2004)	Time (s)	FRR	GAR	Accuracy (%)
DB1	0.0009	0.07	0.91	95.98
DB2	0.0006	0.09	0.95	95.25
DB3	0.0006	0.07	0.93	95.75
DB4	0.0005	0.08	0.90	97.79

Accuracy reflects the overall reliability of the system and is calculated as the ratio of correctly classified instances (both genuine and impostor) to the total number of attempts. Higher accuracy indicates better discrimination between authorized and unauthorized users. Figure 10 shows the accuracy of the QSM algorithm across the tested dataset.

(GAR) measures how effectively the system verifies legitimate users. A high GAR indicates that genuine users are correctly recognized without unnecessary rejections.

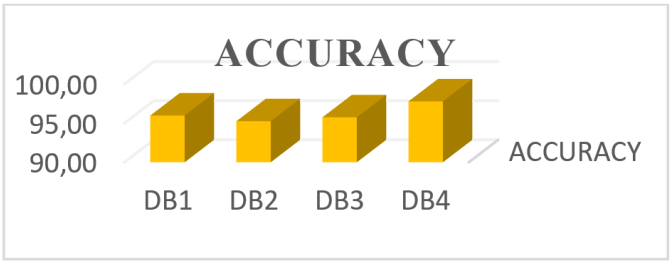

Fig. 10. Accuracy of the QSM method on the FVC2004 dataset.

B. Comparative Analysis

The performance of the proposed QSM algorithm is compared with existing methods from the FVC2002 dataset, including OIS [6], SNL [7], and CikX [8]. Table II presents the comparative results in terms of FAR, FRR, GAR, and accuracy.

TABLE II. PERFORMANCE COMPARISON OF QSM WITH EXISTING METHODS

Method	FAR (%)	FRR (%)	GAR (%)	Accuracy (%)
OIS	7.0	3.0	96.4	96.0
SNL	5.4	3.5	94.56	91.33
CikX	8.7	8.0	95.6	95.0
QSM	7.1	7.7	96.41	96.19

VI. CONCLUSION

A novel algorithm, Quadrant Shift Modulation (QSM), was developed to ensure the security of fingerprint template protection. The fingerprint template protection process consists of two main steps: enrolment and authentication. During enrolment, the input fingerprint image is pre-processed, and minutiae features are extracted. The QSM technique is then applied to secure these features and generate a protected template.

During authentication, the same preprocessing and feature extraction procedures are applied to the query fingerprint image. The protected template stored in the database is then compared with the features obtained from the query image, and the system decides whether to grant or deny access based on this comparison.

Experimental results show that the QSM algorithm achieves robust performance, with a low False Acceptance Rate (FAR) of 7.1%, False Rejection Rate (FRR) of 7.7%, a Genuine Acceptance Rate (GAR) of 96.41%, and high accuracy: 96.19% on the FVC2002 dataset and 97.79 % on the FVC2004 dataset.

REFERENCES

[1] K. Saeed, "Biometrics Principles and Important Concerns," in *Biometrics and Kansei Engineering*, K. Saeed and T. Nagashima, Eds. New York, NY, USA: Springer, 2012, pp. 3–20, https://doi.org/10.1007/978-1-4614-5608-7_1.

[2] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Commun. ACM*, vol. 43, no. 2, pp. 90–98, Feb. 2000, https://doi.org/10.1145/328236.328110.

[3] B. V. K. V. Kumar, M. Savvides, C. Xie, K. Venkataramani, J. Thornton, and A. Mahalanobis, "Biometric verification with correlation filters," *Applied Optics*, vol. 43, no. 2, pp. 391–402, Jan. 2004, https://doi.org/10.1364/AO.43.000391.

[4] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable Biometrics: A review," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, Sep. 2015, https://doi.org/10.1109/MSP.2015.2434151.

[5] A. Nagar, S. Rane, and A. Vetro, "Alignment and bit extraction for secure fingerprint biometrics," in *Media Forensics and Security II*, San Jose, CA, USA, 2010, pp. 223–236, https://doi.org/10.1117/12.839130.

[6] K. Kanagalakshmi and J. K. Antony, "A cancellable and irrevocable approach for fingerprint template protection using optimal iterative solubility algorithm and secure point base," *Biomedical Engineering: Applications, Basis and Communications*, vol. 35, no. 1, Feb. 2023, Art. no. 2250049, https://doi.org/10.4015/S1016237222500491.

[7] J. K. Antony and K. Kanagalakshmi, "Fingerprint template protection using SNL approach-based pattern transformation," *International Journal of Biometrics*, vol. 15, no. 5, pp. 623–643, Sep. 2023, https://doi.org/10.1504/IJBM.2023.133198.

[8] K. Kanagalakshmi and J. K. Antony, "An effective approach for fingerprint template protection based on CiKX transform and Tanimoto similarity measure," *International Journal of Information and Computer Security*, vol. 26, no. 4, pp. 291–315, Jun. 2025, https://doi.org/10.1504/IJICS.2025.146544.

[9] A. Sarkar and B. K. Singh, "A review on performance,security and various biometric template protection schemes for biometric authentication systems," *Multimedia Tools and Applications*, vol. 79, no. 37, pp. 27721–27776, Oct. 2020, https://doi.org/10.1007/s11042-020-09197-7.

[10] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review," *Symmetry*, vol. 11, no. 2, Feb. 2019, Art. no. 141, https://doi.org/10.3390/sym11020141.

[11] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch, "Multi-biometric template protection based on bloom filters," *Information Fusion*, vol. 42, pp. 37–50, Jul. 2018, https://doi.org/10.1016/j.inffus.2017.10.003.

[12] J.-H. Shin, H.-Y. Hwang, and S.-I. Chien, "Minutiae Extraction from Fingerprint Images Using Run-Length Code," in *Foundations of Intelligent Systems: 14th International Symposium*, Maebashi City, Japan, 2003, pp. 577–584, https://doi.org/10.1007/978-3-540-39592-8_81.

[13] J. S. Bartunek, M. Nilsson, B. Sallberg, and I. Claesson, "Adaptive Fingerprint Image Enhancement With Emphasis on Preprocessing of Data," *IEEE Transactions on Image Processing*, vol. 22, no. 2, pp. 644–656, Feb. 2013, https://doi.org/10.1109/TIP.2012.2220373.

[14] F. Zhao and X. Tang, "Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction," *Pattern Recognition*, vol. 40, no. 4, pp. 1270–1281, Apr. 2007, https://doi.org/10.1016/j.patcog.2006.09.008.

[15] Y. Alginahi, "Preprocessing Techniques in Character Recognition," in *Character Recognition*, M. Mori, Ed. London, UK: IntechOpen, 2010, ch. 1, https://doi.org/10.5772/9776.

[16] B. Topçu, M. Kayaoğlu, and U. Uludağ, "Fingerprint phalanx-based score fusion," in *2013 21st Signal Processing and Communications Applications Conference*, Haspolat, Turkey, 2013, pp. 1–4, https://doi.org/10.1109/SIU.2013.6531203.

[17] B. T. Ulery, R. A. Hicklin, M. A. Roberts, and J. Buscaglia, "Interexaminer variation of minutia markup on latent fingerprints," *Forensic Science International*, vol. 264, pp. 89–99, Jul. 2016, https://doi.org/10.1016/j.forsciint.2016.03.014.

[18] L. Jordaan and B. von Solms, "A Biometrics-Based Solution to Combat SIM Swap Fraud," in *Open Research Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2010*, Sofia, Bulgaria, 2010, pp. 70–87, https://doi.org/10.1007/978-3-642-19228-9_7.

[19] P. Gnanasivam and S. Muttan, "An efficient algorithm for fingerprint preprocessing and feature extraction," *Procedia Computer Science*, vol. 2, pp. 133–142, Jan. 2010, https://doi.org/10.1016/j.procs.2010.11.017.

[20] R. Prabhu, X. Yu, Z. Wang, D. Liu, and A. (Andrew) Jiang, "U-Finger: Multi-Scale Dilated Convolutional Network for Fingerprint Image Denoising and Inpainting," in *Inpainting and Denoising Challenges*,

Munich, Germany, 2018, pp. 45–50, https://doi.org/10.1007/978-3-030-25614-2_3.

[21] S. D. Bharkad and M. Kokare, "Performance evaluation of distance metrics: application to fingerprint recognition," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 25, no. 6, pp. 777–806, Sep. 2011, https://doi.org/10.1142/S0218001411009007.

[22] R. de Luis-García, C. Alberola-López, O. Aghzout, and J. Ruiz-Alzola, "Biometric identification systems," *Signal Processing*, vol. 83, no. 12, pp. 2539–2557, Dec. 2003, https://doi.org/10.1016/j.sigpro.2003.08.001.

[23] M. Sivaram, M. U. Ahamed A, D. Yuvaraj, G. Megala, V. Porkodi, and M. Kandasamy, "Retracted: Biometric Security and Performance Metrics: FAR, FER, CER, FRR," in *2019 International Conference on Computational Intelligence and Knowledge Economy*, Dubai, United Arab Emirates, 2019, pp. 770–772, https://doi.org/10.1109/ICCIKE47802.2019.9004275.

[24] Q. Chen, H. Li, S. B. Ariffin, and N. A. B. Mustapa, "A Comprehensive Study on the Homomorphic Encryption for Secure Image Data Processing," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 21783–21790, Apr. 2025, https://doi.org/10.48084/etasr.10007.

[25] S. M. E. Hossain, S. O. F. Khairy, A. Soosaimanickam, and A. M. Raisuddin, "Effective Classifier Identification in Biometric Pattern Recognition," *Engineering, Technology & Applied Science Research*, vol. 14, no. 5, pp. 16604–16608, Oct. 2024, https://doi.org/10.48084/etasr.7424.

[26] W. K. Jummar, A. M. Sagheer, and H. M. Saleh, "Authentication System Based on Fingerprint Using a New Technique for ROI selection," *Babylonian Journal of Artificial Intelligence*, vol. 2024, pp. 102–117, Aug. 2024, https://doi.org/10.58496/BJAI/2024/013.

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

[28] Z. Jin, A. B. Jin Teoh, T. S. Ong, and C. Tee, "Fingerprint template protection with minutiae-based bit-string for security and privacy preserving," *Expert Systems with Applications*, vol. 39, no. 6, pp. 6157–6167, May 2012, https://doi.org/10.1016/j.eswa.2011.11.091.