Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 8, pp. 2915–2931
DOI : 10.47974/JDMSC-2437

Secure vein biometrics authentication based on multimodal artificial template and cryptographic salts

Sarika Khandelwal [#]
Department of Computer Science and Engineering
G H Raisoni College of Engineering
Nagpur 440016
Maharashtra
India

Khyati Rami [†]
SAL Institute of Technology and Engineering Research
Gujarat Technological University
Ahmedabad 380060
Gujarat
India

Harsha Vyawahare [§]
Department of Computer Science and Engineering
Sipna College of Engineering & Technology
Amravati 444701
Maharashtra
India

Alok Singh Gahlot [‡]
Department of Computer Science and Engineering
MBM University
Jodhpur 342011
Rajasthan
India

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

[#] *E-mail:* **sarikakhandelwal@gmail.com**
[†] *E-mail:* **drkhyatirami@gmail.com**
[§] *E-mail:* **harsha.vyawahare@gmail.com**
[‡] *E-mail:* **aloksg@gmail.com**

© Taru Publications

Ruchi Vyas [@]
Department of Computer Science and Engineering
Geetanjali Institute of Technical Studies
Udaipur 313022
Rajasthan
India

Gaurav Kumawat *
Department of Data Science and Engineering
Manipal University Jaipur
Jaipur
Rajasthan
India

Abstract

Hidden biometrics, due to their resistance to duplication and hacking, offer superior security. This work utilizes vein biometrics for their hidden nature, specifically combining palm and finger vein data to enhance security. One key challenge in biometric systems is protecting the stored template, which cannot be revoked or reissued once compromised. We propose a method that merges two vein templates using user-specific scaling and rotation, creating an artificial, irreversible template. Even if the template is stolen, altering the user's secret information regenerates a different template, protecting the original data. Personal Image Identification (PII) adds another user-specific layer of security. The approach employs salt cryptography to ensure simplicity and irreversibility, without storing the original template. Compared to existing methods, our technique offers equivalent accuracy with higher resistance to attacks and lower computational complexity.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Artificial multimodal yemplate, Cryptographic salts, PII (Personal image identification).*

1. Introduction

Personal identification involves a unique set of attributes possessed by individuals. Biometric identification, using traits such as fingerprints, iris, vein patterns, or voice, offers greater security. Unimodal biometrics rely on a single trait. Multimodal combines multiple features, improving accuracy, reliability, and resistance to spoofing. Multimodal systems can use various sensors or fuse different biometric modalities at multiple

[@] *E-mail:* **ruchivyas85@gmail.com**
* *E-mail:* **gaurav.kumawat@jaipur.manipal.edu (Corresponding Author)**

levels. Techniques such as cross fold of random indexes [2], rank level fusion [3], and random distance method [4][23] are commonly used. Hidden biometrics, like vein patterns, are more secure because they are not easily visible or duplicated. This research uses vein biometrics due to their hidden nature, uniqueness, stability, and ability to confirm a living individual [5]. These patterns can be captured using low-resolution NIR images, making the system cost-effective. However, growing biometric use has increased risks, as unprotected templates can be reconstructed and misused [6]. According to ISO/IEC 24745 [7], biometric templates must ensure irreversibility and unlikability. Biometric data, being limited, must be recoverable while maintaining accuracy and efficient storage [8]. The proposed multitier framework ensures irreversibility, recoverability, and minimal storage requirements. Results demonstrate its superiority over existing approaches. The following sections detail related work, challenges, the proposed method, and its evaluation.

2. Techniques for protecting biometric templates

Biometric template protection scheme should sustain characteristics like diversity, recoverability, security, and performance [9]. Two general categories to classify template protection schemes that have been proposed in the literature are: Hardware based Protection and software-based template protection [24]. Commercial products called privarisPlusID [10] uses hardware-based protection. Software based template protection involves storage of biometric samples in converted form by using some transformation function and some keys [26]. Software protection is further classified into feature transformation and biometric cryptosystem. Figure 1 shows the classification of different template protection schemes

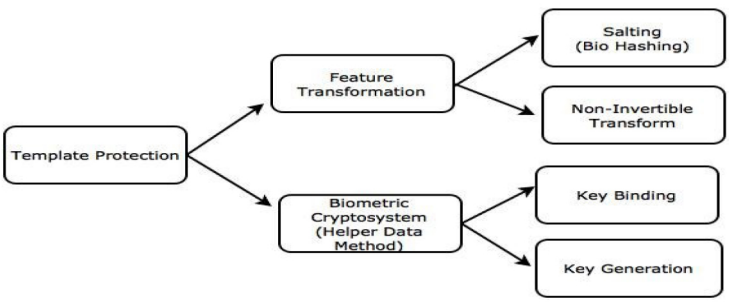


Figure 1

Classification of different template protection schemes

available in literature [1]. Our approach is using non-invertible transformation to store the template. The final stored template is irreversible.

3. Proposed Algorithm

We propose an efficient template protection method addressing key limitations.

Phase 1: Securely merge finger and dorsal hand vein images into a multimodal artificial template.

Phase 2: Encrypt the template using a salt-based cryptographic method to enhance security.

The phase I template generation procedures and phase II template security will be covered in this section. Let us now discuss the proposed personal image identification method to add a personal security layer for template creation and security.

A. *Personal Image Identification: Personal* **Image Identification (PII)** is a user-specific mechanism where individuals select three images from a pool during registration, adding a personalized second layer of security [11]. The image order is based on the user's password, ensuring a unique PII arrangement per user. This selection is used to generate a cryptographic salt, enhancing biometric template protection. Figures 2 and 3 illustrate the image selection interface and PII variation with user ID. The proposed system uses this salt as a security token in a two-phase process detailed in the next section.

B. *Template Preprocessing:* To process vein images, the Region of Interest (ROI) is extracted after normalizing them to 50×50 pixels using bi-cubic interpolation. The grayscale image is converted to binary, and the largest square is selected as the ROI. Image quality is enhanced through intra-region smoothing via diffusion, while inter-region smoothing is suppressed. Sauvola segmentation [12] differentiates vessel from non-vessel regions (Figure 4), and a thinning algorithm is used to extract the vein skeleton.

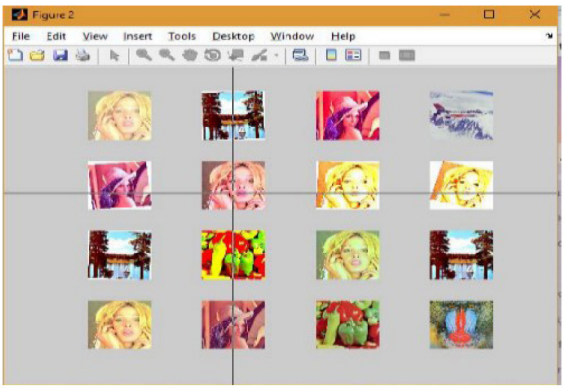


Figure 2

Snapshot of sample PII image selection window.

Figure 3

Snapshot of the changed arrangement of PII images when the subject ID differs

C. *Phase I (Artificial Multimodal Vein Template Generation):* A multimodal vein template is formed by irreversibly merging palm and finger vein images. The process uses a secret key and a pseudo-random number generator to apply a random rotation and scaling to one of the templates before merging [25]. This ensures the original features cannot be separated or traced back, enhancing security. As shown in Figure 5, the merged template makes it visually impossible to distinguish individual vein curves. This technique, referred to as hidden cryptography, securely combines original templates without transforming them individually. The result is an irreversible,

user-dependent, and highly secure artificial template. Although irreversible, some visual vein features may still remain. To further secure the data, the merged template is encrypted in the second phase using a salt-based cryptographic method. The full process is illustrated in Figures 4 and 6.

The output of this phase is a merged artificial multimodal template which is irreversible to retrieve the exact original input templates. The creation of this irreversible multimodal template by merging finger and palm vein curves is demonstrated in figure 5. It also demonstrates that the template is scaled and rotated at a certain angle which is again user dependent. A complete flow diagram for the creation of an artificial template is given in figure 4. It is essential to encrypt this artificial template. Even if it is irreversible to get the exact original templates but after encryption, it will become theoretically impractical to extract any information from the stored templates. Hence to add another layer of protection, this artificial template is then passed to the second phase where a saltcrypted template is created as explained below.

A. *Phase II: Production of Saltcrypted Template*

In this phase, the artificial multimodal template is encrypted using a salt derived from Personal Image Identification (PII). The steps are as follows:

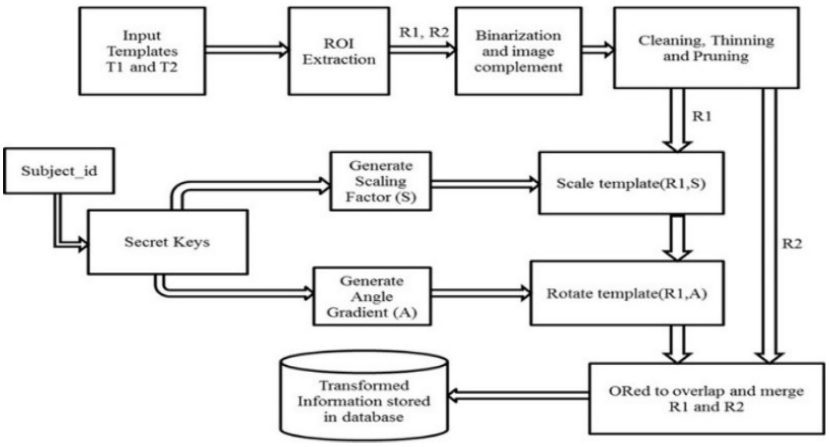


Figure 4

Flow diagram for creation of merged artificial multimodal template.

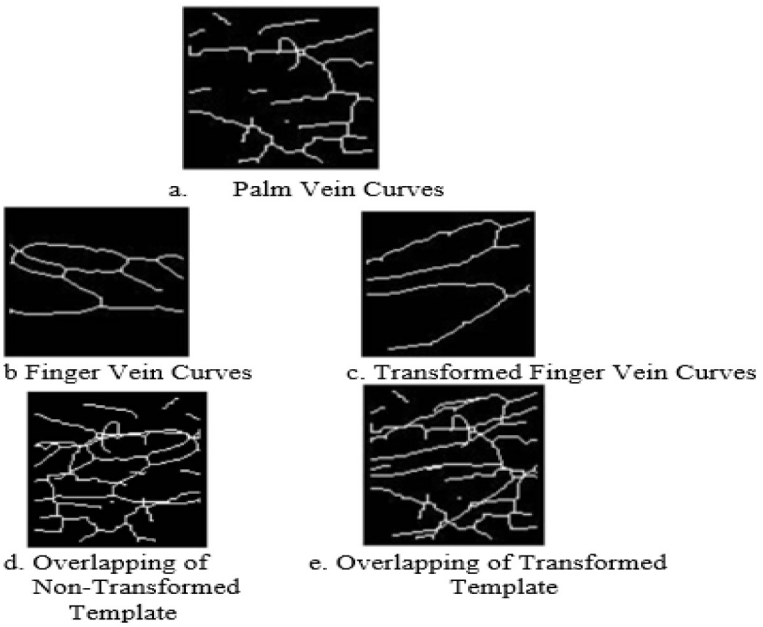


Figure 5

Formation of irreversibly Transformed Template

Salt Cryptographic Algorithm:

1. Input the artificial template f1.
2. User provides a Subject ID and password.
3. User selects 3 personal images based on password-guided arrangement.
4. A PII seed is generated using the sum of digits in the User ID and pixel data from selected images.
5. The PN generator uses this seed to generate a salt.
6. The template f1 is XORed with the salt to create the salted template f2.
7. The password is embedded into f2 using a bit replacement method guided by the PII-based insertion sequence.
8. The final salted and embedded template is stored; no original templates are retained.

Registration Phase (Figure 6):

1. Input templates T1 and T2; secret key; Subject ID.

2. A=Artf_template_creation(T1, T2, secret_key)
3. C=Salt_cryptography(A, secret_key, subject_id)
4. Store C with respect to the subject_id in the database

Query Phase

1. Input query templates T1and T2; secret key; Subject ID.
2. Generate A and encrypted query template C as above.
3. Compare C with stored templates.
4. If correlation > threshold → Match found.
5. Else → No match.

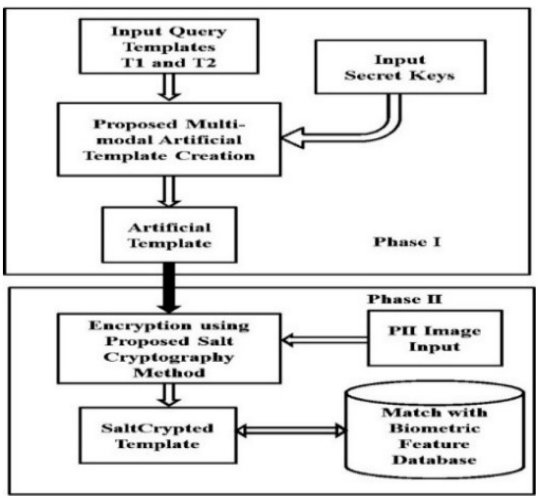


Figure 6

Registration Process of Proposed architecture.

4. Result and Discussions

The proposed algorithm is implemented in MATLAB. Palm vein images are sourced from NCUT's database [13], and finger vein images from Wuhan University's FVD [14]. A total of 960 unique artificial templates were generated—810 (85%) for training and 150 (15%) for testing.During training, templates are evaluated for true positives and false negatives. Figures 7–10 illustrate key steps: user ID and password registration (Fig. 7), PII image selection (Fig. 8), and palm and finger vein image selection (Figs. 9–10). PII selection is user-specific and guides salt

Figure 7

ID and key registration window

Figure 8

Snapshot pf sample PII image selection window

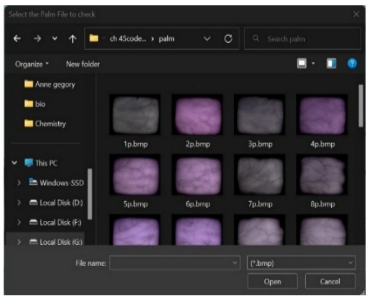


Figure 9

Snapshot of the window pane to select palm vein image from dataset.

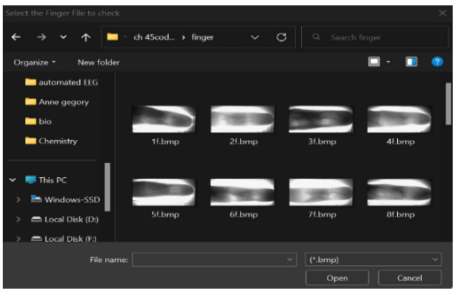


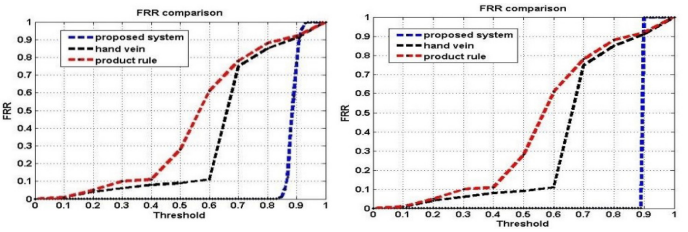
Figure 10

Snapshot of the window pane to select finger vein image from dataset

generation for encryption. Post-training, random test images are matched against stored templates. System performance is evaluated using standard metrics like False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR measures how often an unauthorized user is incorrectly accepted.

FAR is defined as: FAR = False Accepted Attempts / Total Attempts FRR is defined as: FRR = False Rejected Attempts / Total Attempts

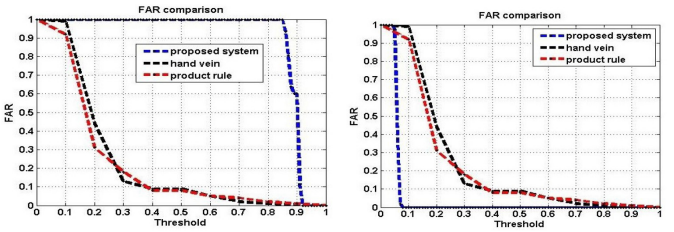
We evaluated both worst-case and best-case scenarios. In the worst case, all users share the same secret keys and PII images. In the best case, users have unique IDs, passwords, and randomly selected PII images and vein patterns. We tested the system using 150 unseen templates to assess resistance to false acceptances. Correlation among templates with different keys and PII is negative, resulting in negligible FAR and FRR. In practice, both FAR and FRR were observed to be zero. Figures 11a and 11b show



(a) (b)

Figure 11

FRR comparison of proposed method for a) Worst case b) Best case



(a) (b)

Figure 12

FAR comparisons of proposed method for a) Worst case b) Best case

FRR vs. correlation threshold for worst and best cases. Figures 12a and 12b show FAR comparisons. Our FAR plot outperforms prior work [15].

B. *EER and ROC Curves*

Figures 13a and 13b show the FAR and FRR vs. threshold plots for the worst and best cases, respectively. Figure 13 c provides a zoomed-in view of Figure 13b. The intersection point represents the Equal Error Rate (EER) on the y-axis and the optimal matching threshold on the x-axis. Though the worst-case EER is relatively high (~0.6), such a scenario is unlikely.

The Receiver Operating Characteristic (ROC) curve, shown in Figure 14, plots FAR against FRR. The point where the curve intersects the 45° line gives the EER, confirming values seen in Figures 13a and 13b. As shown, the worst-case EER is 0.42, while in the best case, our method achieves a very low EER of 0.001.

C. *Advantages of Proposed method*

At each phase, the algorithm has proven the different security as explained below.

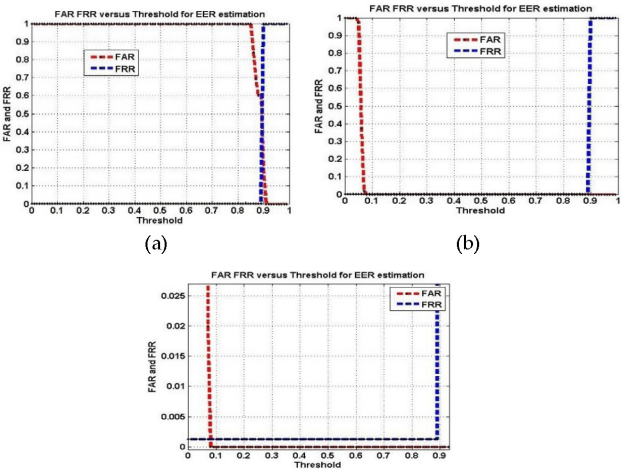


Figure 13

EER Estimation of proposed system for

a) Worst Case b) Best Case c) Enlarged view of Figure 13 (b)

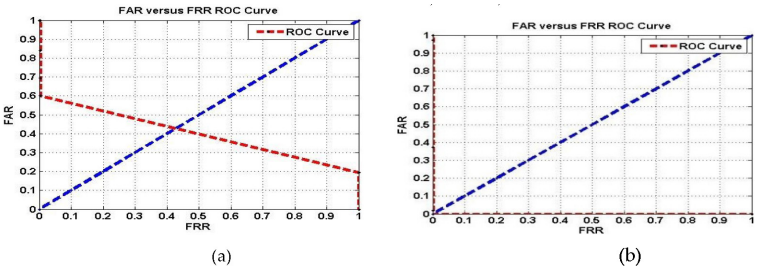


Figure 14

ROC curve a) Worst case b) Best Case

1) Irreversible Property: The saltcrypted artificial template is a random binary sequence, making it impossible to extract any information about the original or artificial templates, ensuring complete security.
2) No Visual Information: The stored template has no visual clues about the original or merged templates (Figure 15), enhancing privacy.
3) Lesser storage requirement: Finger images (130KB) and palm templates (2.25MB) are compressed to just 2.5KB per subject, demonstrating the algorithm's space efficiency and suitability for embedded devices.

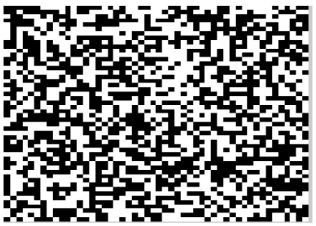


Figure 15

Sample saltcrypted template to ensure there is no visual information about the original template.

4) Better Attack Complexity: Detecting the correct overlapped pattern is computationally expensive (2MxN = 22,500 combinations), making information theft nearly impossible, as no original data exists in the stored template.
5) We tested template similarity across different subjects and passwords, showing low similarity even in worst-case scenarios, enhancing security.

a) Similarity of templates of different subjects: We tested template similarity for both the worst case (same secret keys and PII images) and the best case (unique IDs, passwords, random PII images, and vein patterns). The generated saltcrypted artificial templates were expected to have low similarity. The correlation between templates was calculated, and the results are shown in Figure 16.The average correlation for our dataset is 0.62, indicating low similarity. Figure 16a shows the correlation for the worst case, and Figure 16b shows the best case, where most of the image is black, indicating minimal

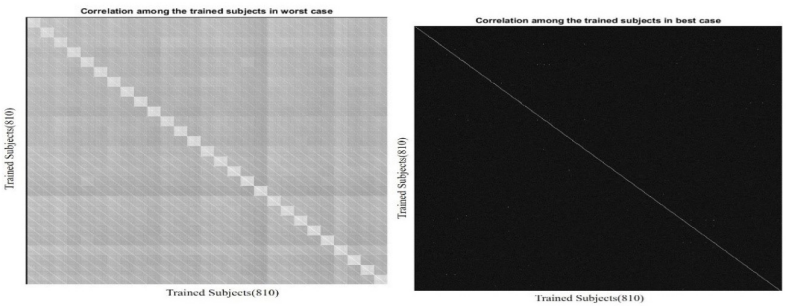


Figure 16

Correlation among various stored saltcrypted templates of different individual's in a) worst case, b) Best case

correlation. This demonstrates the method's ability to distinguish between a large numbers of subjects.

b) Similarity among Registered and Unregistered Templates: Figure 17a and 17b show the correlation between templates of unregistered and registered subjects for the worst and best cases, respectively. In the worst case, the average similarity is 0.71, which is still relatively low. In the best case, the average correlation is negative, indicating no similarity between the templates.

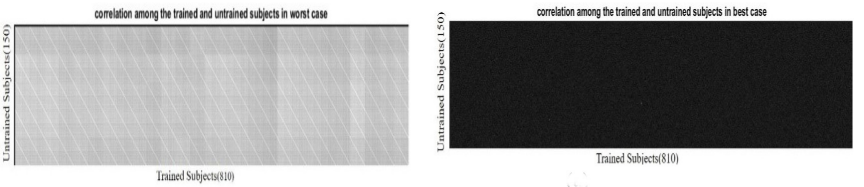


Figure 17

Correlation among the templates of registered and unregistered subject's in (a) Worst case, (b) Best Case.

c) Similarity of Templates of Same Person with Different Passwords :We tested cases where the same user inputs different passwords—useful if a password is compromised. By changing passwords for two registered users, we generated new templates (Figure 18). Both showed correlation below 0.5, confirming that different passwords produce distinct saltcrypted templates from the same original input—an important security feature.

d) Different IDs but Selected PII Images and the Password is Same: Figure 18 shows templates for the same subject with identical secrets

Figure 18

Saltcrypted templates for same individual but different passwords

Figure 19

Saltcrypted templates for same individual with same PII image selection and secret info but different ids input.

and PII images but different user IDs. The resulting templates are clearly different, highlighting the impact of user ID on template generation.

Different PII Images Selected when the Password is same :Now we test the strength provided by PII images-based cryptography as shown in figure 19. We test for same subject with same password, but this time select different PII images. Due to this the resultant templates are completely different as shown in figure 20.

Figure 20

Saltcrypted templates for same individual but different PII image selection

D. *Performance Comparison with Previous Works*

Table 1 compares previous methods using various modalities and algorithms along with their FAR, FRR, and EER. The proposed method clearly outperforms them.

Table 1

Comparison of FAR, FRR and EER Among Various Multimodal Feature Level Fusion and Proposed Method

S. No.	Modality	Algorithm	EER%	FAR%	FRR%	Ref.
1	Finger vein and finger print	Weighted sum rule	0.78	NA	NA	[16]
2	Face and voice	Score level fusion	25.70	NA	NA	[17]
3	Face and voice	Feature level fusion	2.14	NA	NA	[17]
4	Dorsal hand vein, palm vein and finger vein	Maximum likelihood	0.04	0.04	0.05	[15]
5	Palm-dorsa vein	Multi resolution analysis and combination	3.75	3.5	1.5	[18]

Contd...

6	Hand vein and knuckle shape	Matching vein triangulation and shape features	1.14	1.14	1.14	[19]
7	Hand vein and palm print images	Weighted SUM rule	4.7	NA	NA	[20]
8	Hand geometry, palm and finger textures, dorsal hand vein	Simple Sum rule	0.01	0.01	0.01	[21]
9	Hand vein	ICA1	5.4	NA	NA	[22]
10	Finger and palm vein	Proposed algorithm	0.1	0.1	0.1	Proposed

6. Conclusion and Future work

We proposed a multilevel security algorithm for artificial multimodal vein templates using PII-based salt cryptography. Key steps and algorithms were detailed, with implementation in MATLAB. The system ensures strong security at each level, with irreversible final templates containing no visible original data. The average matching time is 0.6 seconds, with 100% TP and TN rates, and zero FP and FN. Each stored template requires just 2.5 KB, making it ideal for low-resource devices. Biometric templates are prone to attacks, and their compromise can lead to identity theft. Our method generates irreversible multimodal vein templates, further secured through cryptographic salts and enhanced with improved PII. Results confirm strong protection and efficient storage, making it suitable for real-time use. Future work may integrate block chain for added security.

References

[1] U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain, "Biometric cryptosystems: Issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960 (2004), doi: 10.1109/JPROC.2004.827372.

[2] L. Leng, A. B. J. Teoh, L. Leng, M. Li, L. Leng, M. Li, and M. K. Khan, "Orientation range for transposition according to the correlation analysis of 2DPALMHash Code," in *Proc. Int. Symp. Biometrics and Security Technologies (ISBAST)*, pp. 230–234 (2013), doi: 10.1109/ISBAST.2013.40.

[3] P. P. Paul and M. Gavrilova, "Rank level fusion of multimodal cancelable biometrics," in *Proc. IEEE 13th Int. Conf. Cognitive Informatics and*

Cognitive Computing (ICCI-CC), pp. 80–87 (2014), doi: 10.1109/ICCI-CC.2014.6921445.

[4] H. Kaur and P. Khanna, "Random distance method for generating unimodal and multimodal cancelable biometric features," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 709–719 (2019).

[5] Z. Liu and S. Song, "An embedded real-time finger-vein recognition system for mobile devices," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 2, pp. 522–527 (2012).

[6] J. Galbally, R. Cappelli, A. Lumini, G. Gonzalez-de-Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia, and D. Maio, "An evaluation of direct attacks using fake fingers generated from ISO templates," *Pattern Recognition Letters*, vol. 31, no. 8, pp. 725–732 (2010).

[7] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1406–1420 (2018).

[8] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryption," *Pattern Recognition*, vol. 67, pp. 149–163 (2017).

[9] D. Maltoni, J. Feng, A. K. Jain, and D. Maio, *Handbook of Fingerprint Recognition*, Springer International Publishing (2022). [Online]. Available: http://www.siscocorp.com/docs/Privaris_plusID.pdf

[10] S. S. Khandelwal and P. C. Gupta, "Multitier biometric template security using cryptographic salts and personal image identification," *ELCVIA Electronic Letters on Computer Vision and Image Analysis*, vol. 13, no. 3 (2014).

[11] A. Agarwal, S. Maheshwari, and G. Yadav, "Vein biometric security using irreversible curve fitting accounting for minimum storage," in *Proc. Int. Conf. Signal Propagation and Computer Technology (ICSPCT)*, pp. 179–183 (2014).

[12] *Vein Dataset*, Poznan University of Technology. [Online]. Available: http://biometrics.put.poznan.pl/vein-dataset/

[13] *PolyU Finger Vein Database*, Hong Kong Polytechnic University, version 1.0 (2017). [Online]. Available: http://www4.comp.polyu.edu.hk/~csajaykr/fvdatabase.htm

[14] S. Bharathi, R. Sudhakar, and V. E. Balas, "Hand vein-based multimodal biometric recognition," *Acta Polytechnica Hungarica*, vol. 12, no. 6, pp. 213–229 (2015).

[15] R. Raghavendra, K. B. Raja, J. Surbiryala, and C. Busch, "A low-cost multimodal biometric sensor to capture finger vein and fingerprint," in *Proc. IEEE Int. Joint Conf. Biometrics*, pp. 1–7 (2014).

[16] M. I. Gofman, S. Mitra, T.-H. K. Cheng, and N. T. Smith, "Multi-modal biometrics for enhanced mobile device security," *Communications of the ACM*, vol. 59, no. 4, pp. 58–65 (2016).

[17] C.-L. Lin and K.-C. Fan, "Biometric verification using thermal images of palm-dorsa vein patterns," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 2, pp. 199–213 (2004).

[18] A. Kumar and K. V. Prathyusha, "Personal authentication using hand vein triangulation and knuckle shape," *IEEE Transactions on Image Processing*, vol. 18, no. 9, pp. 2127–2136 (2009).

[19] R. Raghavendra, M. Imran, A. Rao, and G. H. Kumar, "Multimodal biometrics: Analysis of hand vein and palm print combination used for person verification," in *Proc. 3rd Int. Conf. Emerging Trends in Engineering and Technology*, pp. 526–530 (2010).

[20] M. A. Ferrer, A. Morales, C. M. Travieso, and J. B. Alonso, "Combining hand biometric traits for personal identification," in *Proc. 43rd Annu. Int. Carnahan Conf. Security Technology*, pp. 155–159 (2009).

[21] A. Yüksel, L. Akarun, and B. Sankur, "Biometric identification through hand vein patterns," in *Proc. Int. Workshop on Emerging Techniques and Challenges for Hand-Based Biometrics*, pp. 1–6 (2010).

[22] G. Kumawat, S. K. Vishwakarma, and P. Chakrabarti, "Cervical cancer prediction using machine learning techniques," in *Proc. Int. Conf. WorldS4*, Singapore: Springer Nature Singapore (2023).

[23] Siswanto and S. M. Al-Maghribi, "Solving the eigenproblems of triangular and diagonal strictly double R-astic matrices over min-plus algebra," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 6, pp. 2237–2245 (2025), doi: 10.47974/JDMSC-2188.

[24] V. R. Bolla, B. Vikas, S. Potluri, Y. Subbarayudu, G. Sucharitha, and N. Narisetty, "The scalable cloud-based reinforcement learning for multimedia data in cognitive neuroscience for secure healthcare analysis," *Journal of Information and Optimization Sciences*, vol. 46, no. 6, pp. 1793–1801 (2025), doi: 10.47974/JIOS-2008.

[25] M. S. Basha, K. R. Prasad, S. K. Mouleeswaran, R. C. Poonia, and S. Sebastian, "Multi-disease detection system with X-ray images using deep learning techniques," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1379–1388 (2024), doi: 10.47974/JIOS-1710.

[26] S. Jain, N. Rajpal, and P. K. Soni, "Multiple sclerosis detection from brain MRI images using least square-SVM," *Journal of Information and Optimization Sciences*, vol. 45, no. 4, pp. 969–980 (2024), doi: 10.47974/JIOS-1620.

Received January, 2025