Review of Computer Engineering Research
2022 Vol. 9, No. 4, pp. 239-249.
ISSN(e): 2410-9142
ISSN(p): 2412-4281
DOI: 10.18488/76.v9i4.3169
© 2022 Conscientia Beam. All Rights Reserved.

MULTIMODAL BIOMETRIC TEMPLATE TRANSFORMATION APPROACH USING A LIST RANKING ALGORITHM

Ashoka Rajan R[1+]
Pon Bharathi A[2]
Sarika A S[3]
Vedha Vinodha D[4]

[1]*SCOPE, Vellore Institute of Technology, Chennai, India.*
[1]*Email: ashok.tiruchendur@gmail.com*
[2,3]*ECE, Amrita College of Engineering and Technology, India.*
[2]*Email: bharathpon@gmail.com*
[3]*Email: sarikathr99@gmail.com*
[4]*ECE, JCT College of Engineering and Technology, India.*
[4]*Email: dvedha1975@gmail.com*

(+ Corresponding author)

Article History
Received: 1 April 2022
Revised: 16 September 2022
Accepted: 4 October 2022
Published: 14 October 2022

Keywords
Biometric Security
Database Security
Multi-biometrics
Multimodal biometrics
Parallel algorithm
Physiological biometrics
Sine model XOR
Template security
Template transformation.

ABSTRACT

User authentication has become vital with the advancement in technologies that comes with an increased threat to security. Biometrics is typically used to secure the data of individuals based on their unique features, such as fingerprints, retinas, and hand geometry. Template transformation is a technique in which the original feature vectors are transformed into modified feature vectors. When these templates are transformed and stored, it becomes difficult for imposters to hack the system. Existing systems store and secure these templates based on key generation. When the key information is compromised, the system can be easily hacked. Hence, in the proposed system, the templates are transformed using a modified list ranking algorithm and then stored for verification. Also, in order to improve security, instead of using a single biometric, the proposed system obtains biometric data from left fingerprints, right fingerprints and palm prints and fuses them into a single feature vector set. Thus, even when the repository is attacked, it would be very difficult to break into the system. The proposed system provides a 2.9 % equal error rate compared with existing systems.

Contribution/Originality: This research predominantly focuses on improving the security of biometric template databases without affecting the conventional matching performance of biometric recognition systems. To increase the security of template database, this research applies a novel parallel list ranking algorithm over multimodal biometrics instead of single biometrics

1. INTRODUCTION

It is crucial to install security systems in critical areas. They are becoming increasingly popular among people and businesses in society due to situations such as identity theft and other vulnerabilities. A security system also plays an important role in crime-related applications during investigations and other processes. A security system is a method by which critical information or critical devices are automatically secured. Initially, security breaches were not at an acceptable level, hence the importance of security systems was realized. The use of password-based authentication was the earliest security measure adopted to protect systems and information. A password is a set of characters used to confirm the identity of the user. There are many disadvantages to using this type of security system, such as storing user passwords. Systems are also secured using personal identification numbers (PINs), which is a numerical password. PINs usually contain 8-12 digits and are generally associated with credit and debit cards, thus most of the issues are related to the unprivileged access to users' accounts through personal identification numbers.

It is clear that the earliest security methods are not strong enough to protect the most critical assets. When biometric technology came into existence, which is more easily accessible than ever before, it resulted in enhanced security and greater convenience to securely protect systems. Biometrics is an automated pattern recognition system that records physiological or behavioral characteristics and offers the highest level of security. Biometrics cannot be stolen or forgotten. It is consistent and secure since biometrics cannot be reengineered and therefore a reliable way of protecting critical assets by eliminating the need to remember passwords or PINs. And when biometrics is used as a part of a smart card, a strong level of security for any confidential data can be provided. The earliest biometric system was a uni-biometric system (single biometric system). These systems are often affected by problems such as noisy data, non-universality, and lack of individuality.

Multimodal biometric systems are capable of using more than one physiological or behavioral characteristic for enrollment, verification, and identification. Using a single biometric system, the security of credentials was not accurate, so in order to improve security multimodal biometrics are used, which eliminate the issue of non-universality. Also, it is extremely difficult to identify and attack multiple biometric characteristics of a user.

Multi-biometric systems also address the problem of noisy data. When the raw data from a biometric is polluted by noise, the data from another biometric trait can be used to verify the identity of the user. A multi-biometric system is designed as a fault tolerant system by continuing to process, even when data from certain sources are unreliable because of hardware or software issues. The existing methods explained below protect these biometric templates.

Many systems have been proposed that take advantage of multi-biometrics. Juels and Sudan [1] proposed the fuzzy vault scheme, which makes use of a polynomial to conceal biometric data, and the identification of users is based on the reconstruction of a polynomial using a Reed–Solomon error-correcting code (ECC). Nagar, et al. [2] proposed a model which uses feature-level fusion to secure many templates of a user as a single entity. The implementation is done using the fuzzy vault and fuzzy commitment techniques. However, the limitation of the fuzzy vault technique is, that it is difficult to generate chaff that is indistinguishable from genuine points, and in fuzzy commitment, there is a lack of perfect codes for desired code lengths.

Nandakumar and Jain [3] proposed a fuzzy vault scheme that creates a template by fusing fingerprint and iris features from a set of chaff points. Gyaourova and Ross [4] proposed a scheme indexing biometric databases. In this scheme, fixed-length codes are generated. By computing similarity scores between a query image and a set of images in the repository, an index score is obtained. It may not achieve state-of-the-art indexing performance for some biometric modalities, but it can be easily ported for use on multimodal databases. Pioneering work in fingerprint biometrics was done by Tomko, et al. [5], however, usability and security issues were quickly discovered and they worked to ensure that these issues were resolved. Li, et al. [6] proposed a method to add security to fingerprint-based multi-biometric cryptosystems using a method known as decision-level fusion. Hash functions are used in the construction of templates to protect each single unique biometric trait. Since hash functions are used, the hash function should be time efficient, and a bad hash function might become vulnerability and an easy target. Othman and Ross [7] proposed a fingerprint security method by combining spiral and continuous components from two fingerprints. This method provides virtual identities and is used to generate a cancellable fingerprint template. This method provides a new identity for authentication. Enhancement of the performance of mixed fingerprints, and also by exploring other algorithms for alignment, selecting and mixing the different pairs must be improved.

Nagar, et al. [8] proposed a new technique for securing individual templates by storing only the boundary sketch generated from the same fingerprint template using biometric cryptosystems. Li and Kot [9] stated that fingerprint data is binary and contains private user information without causing any obvious abnormalities. During the authentication phase, the hidden data is extracted from the stored template to verify the authenticity of the query fingerprint. In this scheme, no boundary pixel is used in the data embedding to improve the performance of the fingerprint identification. However, when an online database is compromised by an imposter, it is not possible to obtain the original user templates, thus the privacy of users is enhanced using this scheme. Cao and Jain [10] proposed a system based on reconstruction techniques for securing fingerprint templates, improving the template interoperability, and improving fingerprint synthesis. In this method, the reconstruction technique uses prior knowledge of the structure of the fingerprint ridge to improve the reconstruction of the original fingerprint image. However, an investigation must be carried out to check the accuracy of the reconstructed fingerprints. Uz, et al. [11] proposed a technique that combines several biometric feature sets into a super template set using hierarchical matching. The hierarchical matching algorithm enables higher quality minutiae because of the higher level hierarchy. Dodis, et al. [12] defined three metric spaces for classifying biometrics. Most of the biometric features fall under the Hamming metric and the set difference metric because most of the features can be represented as either a bit string or as a feature set. The third metric is the edit metric.

Li, et al. [6] pointed out some limitations in using entropy-based security systems and proposed a better security system that combines the information-theoretical approach with the system of computational security. The construction of a fingerprint-based multi-biometric system is fused with levels of decisions. Hash functions are also used along with the construction of decisions to increase the protection of each biometric trait. Golic and Baltatu [13] justify that the average min-entropy does not identify the statistical independence of a random variable. The system introduces the conditional Shannon entropy. Both the conditional Shannon entropy and the average min-entropy calculate the security from the information-theoretical perspective, which will be reflected as the probability rather than the biometric templates' actual values. Yang, et al. [14] developed a Delaunay quadrangle that works when the Delaunay triangle suffers. This system is used to deal with non-linear local structural change which cannot be handled by the triangular approach. Alignment-free features extracted are less sensitive to the triangular approach and are applied directly only to template protection. Fang, et al. [15] developed a cascaded method within the sketch of a secure framework. The main advantage of the proposed approach is that biometric feature data can easily be combined with a multi-biometric cryptosystem. The benefit is that it allows the use of templates which are heterogeneous in nature.

Liu, et al. [16] proposed a two-layer security method which combines fingerprint modality with an electrocardiogram (ECG) of a biometric user. In this method, fusion happens at feature and decision levels using a convolution neural network and a support vector machine. One of the important vulnerability issues in biometric recognition systems is an attack via record multiplicity. To protect the template database from such attacks, Tran, et al. [17] designed a dual-level security method which works well even when the images are of poor quality. A rotation invariant alignment-free biometric hashing technique was proposed by Wang and Abdullahi [18]. To improve the hash generation process, Fourier-Mellin transform and fractal coding techniques are combined in this approach.

The remainder of the paper is organized as follows: Section 2 introduces the proposed multi-biometric template transformation approach with the modified list ranking algorithm; Section 3 details the results and explains the computational security for the list ranking algorithm; and Section 4 contains the conclusions and suggestions for future studies.

2. PROPOSED SYSTEM

Figure 1 shows the multi-biometric architecture that uses three inputs from the user and transforms them in such a way that it is different from the original template. During enrollment, the ridge ending features and bifurcation features are extracted from left fingerprint, right fingerprint and palm prints. The three inputs are first preprocessed by enhancing the images using binarization techniques, thinning operation and minutiae extraction.

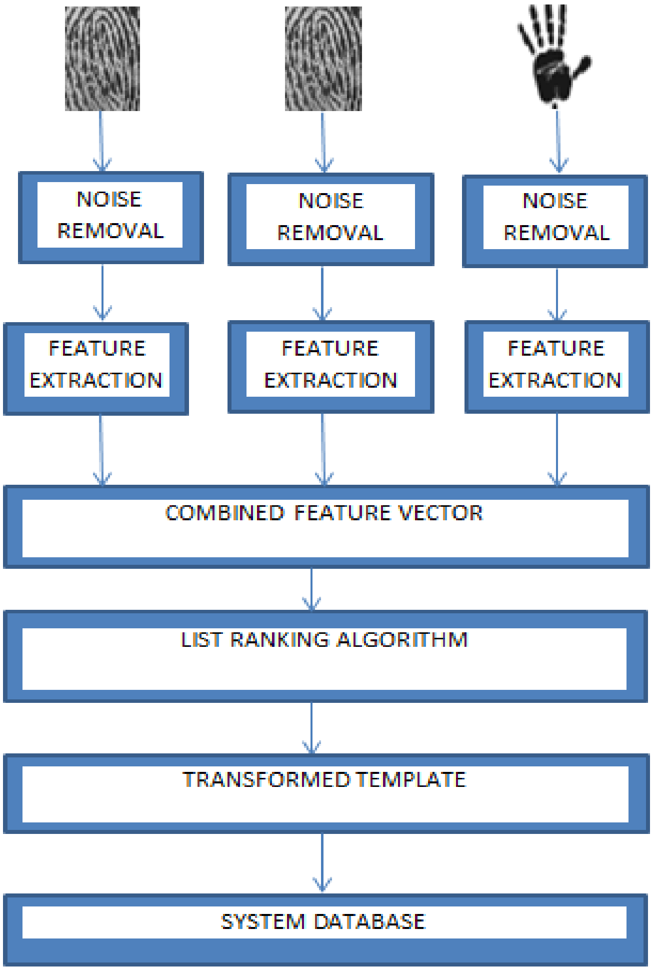
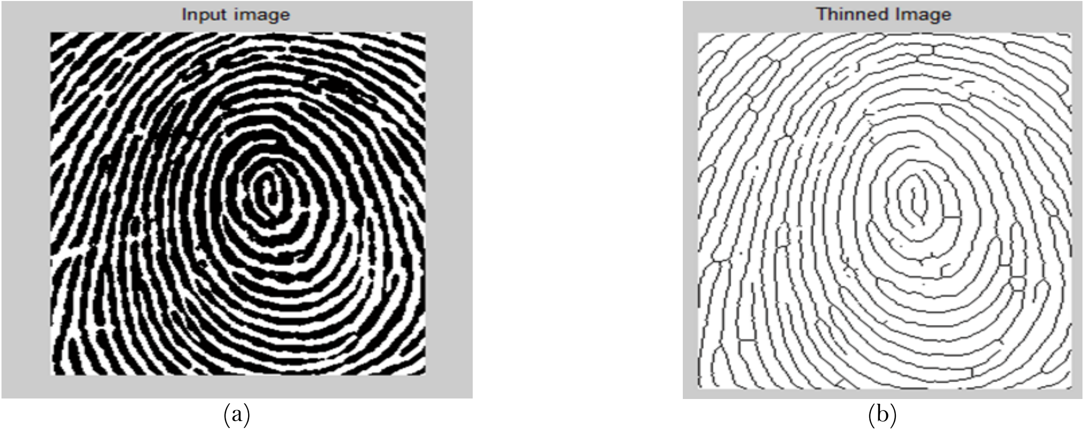


Figure 1. Architecture diagram.

A. Thinning

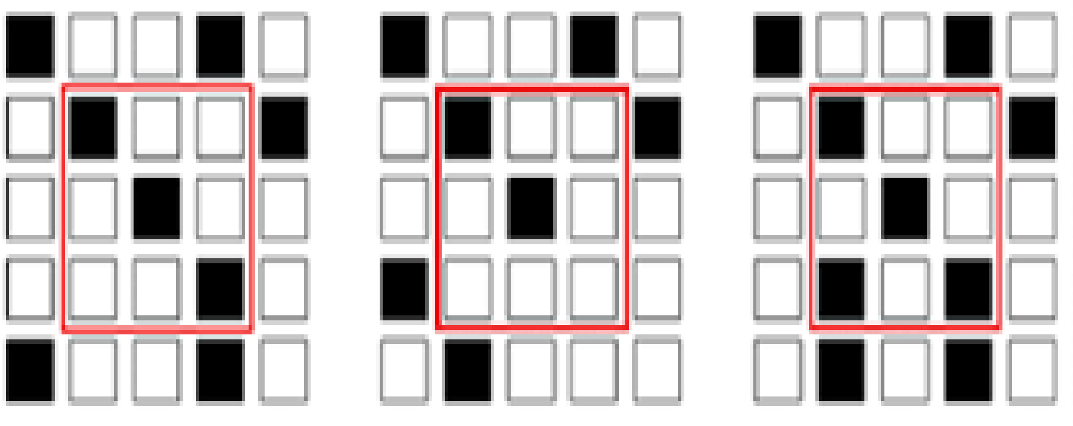
Thinning is an operation in which the original biometrics obtained from the scanners are processed and the noise is removed to provide a clearer image for feature extraction. Figure 2(a) shows the original fingerprint image and Figure 2(b) shows the thinned image after removing the noise from the fingerprint.



Figures 2(a). Original image. **(b)** Thinned image.

B. *Minutiae Extraction*

The thinned image is used for data retrieval. There are many features that can be obtained, such as ridge end, bifurcation and the core point. The proposed system extracts the ridge points and the bifurcations based on the crossing number concepts (CN). The thinned image is treated as a matrix. For each pixel, the crossing number is calculated from the neighboring pixels. If the crossing number is 2, then it is treated as ridges and if the crossing number is 4, it is treated as bifurcations. The crossing numbers are manipulated as shown in Figure 3.



CN = 2 CN = 1 CN = 3

Figure 3. Crossing numbers.

C. *Feature Vector Generation*

Here, the right fingerprint's feature vector acts as plain text, Key 1 is the left fingerprint's feature vectors and the palm print is Key 2. Key 1 and Key 2 are processed using the linear equation $ax + bx^2 + c$, and the output is XORed with plaintext, as shown in Figure 4.

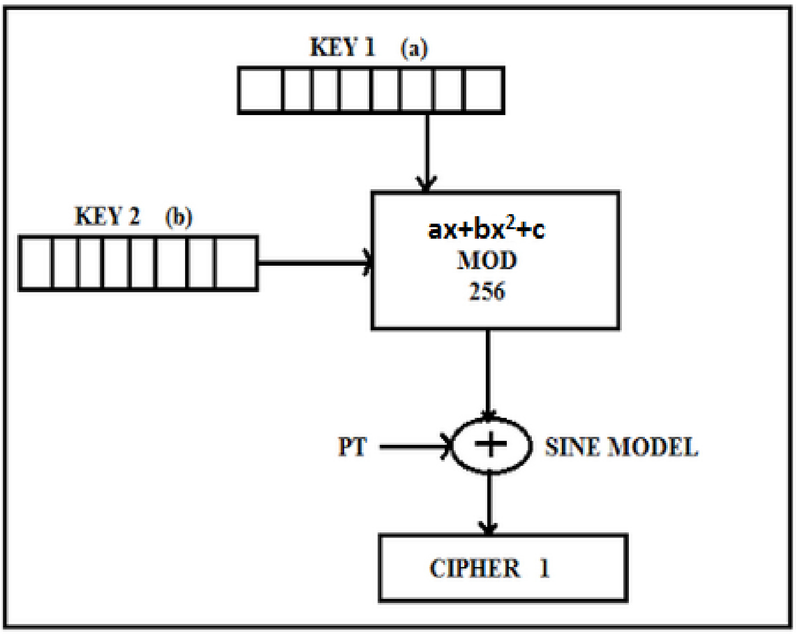


Figure 4. Node operation of list ranking.

In order to improve the robustness, instead of the usual XOR, a sine XOR model is used, as shown in Figure 5. The numbers are represented as bits {A1, A2, A3, A4, A5, A6, A7, A8}. Then the sine model XOR is performed on these bits. For example, Input: 10(00001010), 28(00011100)

Output: 140

There are some cases where modulus must be performed to bring the features within the 0–255 range. Normally, the XOR returns true if both the inputs are different, otherwise the XOR will return output as false. Figure 5 depicts the bit representations of the pixel values extracted from the feature vectors. The list ranking algorithm uses the sine XOR model, where an XOR operation is performed on the inputs in the format of a sine wave type with the inputs of 2^N. The sine model will end when the sine wave crosses the value of N = 8. The output from the sine XOR model is taken and fed into the list ranking algorithm. These XORed vectors are then combined with Key 2, which is the palm print, using the linear equation $ax + bx^2 + c$.

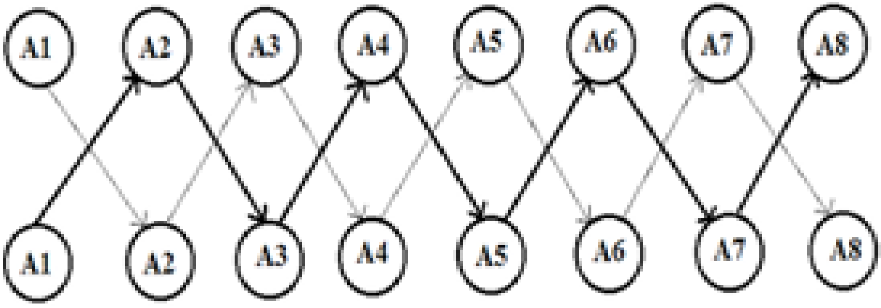


Figure 5. Sine XOR model

D. *Modified List Ranking Algorithm*

In the list ranking algorithm, each node will operate on all three inputs. The algorithm takes the right fingerprint input as plaintext, the left fingerprint acts Key 1, and the palm print acts as Key 2. The plaintext right fingerprint is taken in 8-bit node form and adds the 2^N (N values starts from 0) nodes combination in the first step. Then the left fingerprint and palm print are taken and the list ranking algorithm is repeated. Again, there will be 8-bit values for all three inputs (left, right and palm). The output from this stage is sent to the sine model operation. These ciphers act as an input for the algorithm. In the first step, adjacent ciphers are XORed using the sine model operation. Thus, the numbers are XORed from the current node in a logarithmic sequence such that the current node is + 2^N, where N is the iteration count. For instance, if N = 1, then this would XOR the first and third node values, then the second and fourth, and so on. This process continues until there are one or two nodes left. Figure 6 presents the complete process of the list ranking algorithm.

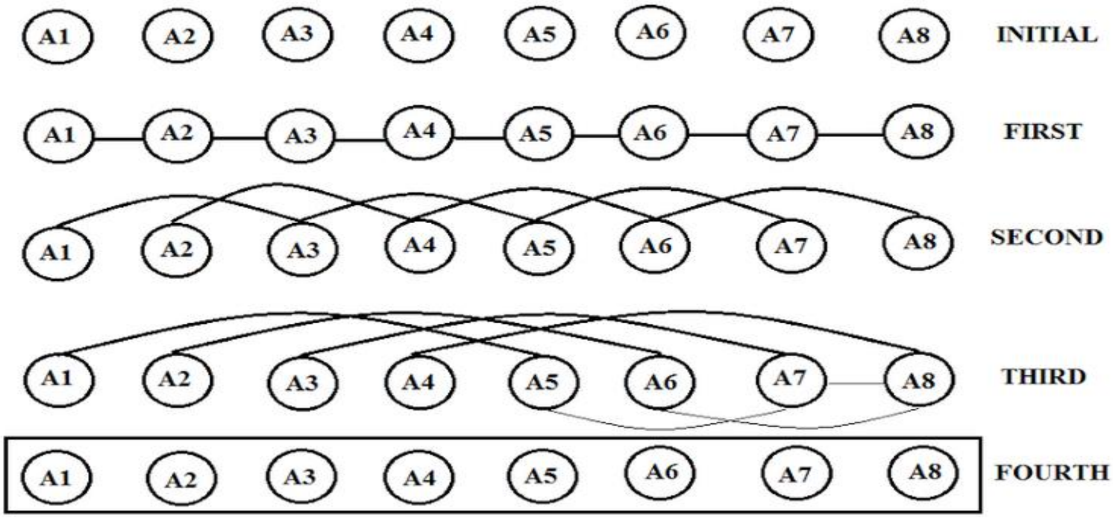


Figure 6. Modified list ranking algorithm.

```
Algorithm:    List ranking algorithm.
Input:        Left print, right print, palm print.
Plaintext:    Left print.
Key 1:        Right print.
Key 2:        Palm print.
Output:       Cipher 1(integer).
1   for i to n
2   $res = left[i]$ base 3
3   $res1 = palm[i]$ base 3
4   $result = res(x^2) + res(x) + palm[i]$
5   for i to n
Convert the left[i] to binary, say rem.
Convert the palm[i] to binary, say rem1.
6   set k to 0
7   for $i = 0$ to 6
if (i%2==0)
result [k++] = rem[i] ^ rem1[i+1]
Otherwise,
result [k++] = rem1[i] ^ rem[i+1]
result [k++] = rem1[i] ^ rem[0]
8 Repeat the same for the loop and complete a sine XOR model
9 Convert the resultant binary number to an integer, say res2
10 $res2 = res2 \bmod 256$
11 node [i] = res2
12 This resultant array of ciphers is then fed into the algorithm (list ranking).
```

E. *Storing in Databases*

The resultant three features are combined using horizontal concatenation and the order of concatenation is preserved. The final resultant is loaded into the database for the verification process.

F. *Scoring and Verification*

During the verification process, the query biometrics (left fingerprint, right fingerprint, palm print) are obtained and the features are generated as discussed above and the final transformed template is treated as the query. This query is indexed with the stored templates for calculating the score percent. The similarity score is the cumulative score of the number of points matched. The score is computed between the query feature vector and all the feature vectors in the database. For a genuine user, the similarity score will be a peak value clearly stating the authenticity of the query user.

Table 1. EER performance between the existing and proposed methods.

Method	2002	2002	2002	2004	2006	2006
	DB1	DB2	DB3	DB2	DB2	DB3
Equal Error Rate						
Liu, et al. [16]	6	6.2	6.35	6.57	7.01	7.23
Wang and Abdullahi [18]	4.73	4.92	5.21	5.56	5.78	6.32
Tran and Hu [17]	4.3	4.4	4.9	5.012	5.7	5.8
Proposed system	2.9	4.2	4.01	4.8	4.7	5.2

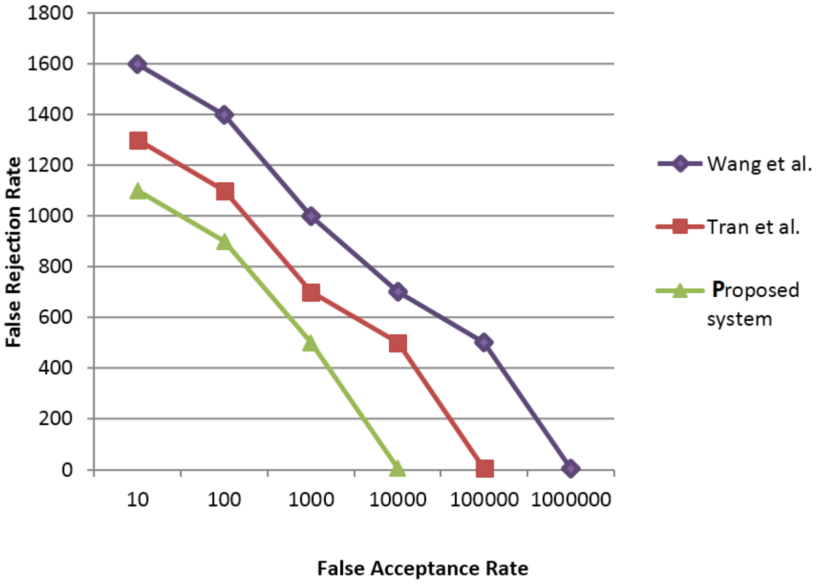


Figure 7. Comparison between the existing system and the proposed system.

Using two different protocols, 1VS1 and Fingerprint Verification Competition (FVC), fingerprint data from different datasets are used in multi-biometric systems. The earlier database consists of poor-quality data, which are collected using low-quality scanners that extract false minutiae points. In recent years, data were collected using high-quality scanners that help in extracting only the genuine points. As a result, the error rate is very much reduced, as shown in Figure 7.

To show the accuracy level achieved, variation in the performance is determined. The performance is improved to a certain extent in the proposed project compared to the existing system, as shown below in Figure 8.

An equal error rate (EER) comparison is made between the accuracy achieved by various existing systems across the different FVC databases in Table 1. In a security system, the false acceptance rate (FAR) and false rejection rate (FRR) will be directly proportional. If the FRR is too high, there is a high chance that genuine users will be rejected, hence the EER percentage should be moderate for a security system. The proposed system was tested using various datasets, and an EER of 4.3% was found, as shown in Figure 9.

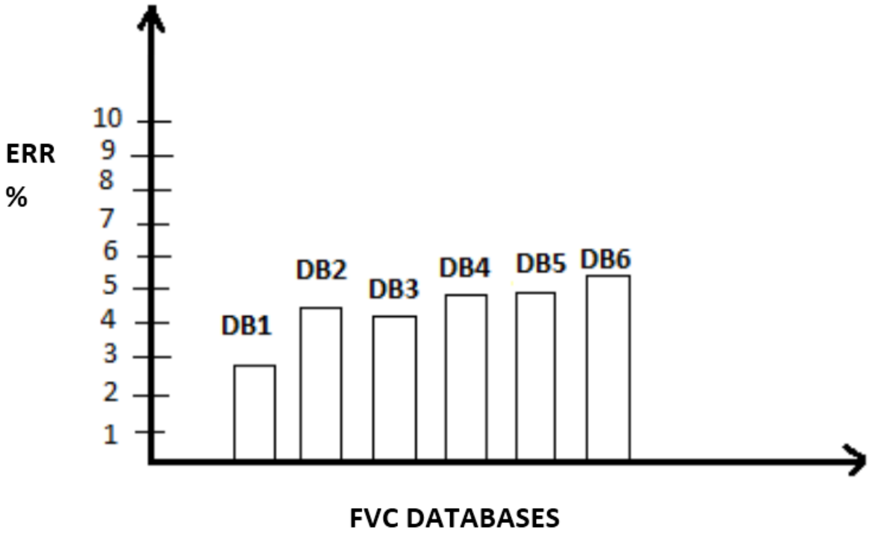


Figure 8. Accuracy achieved across different databases.

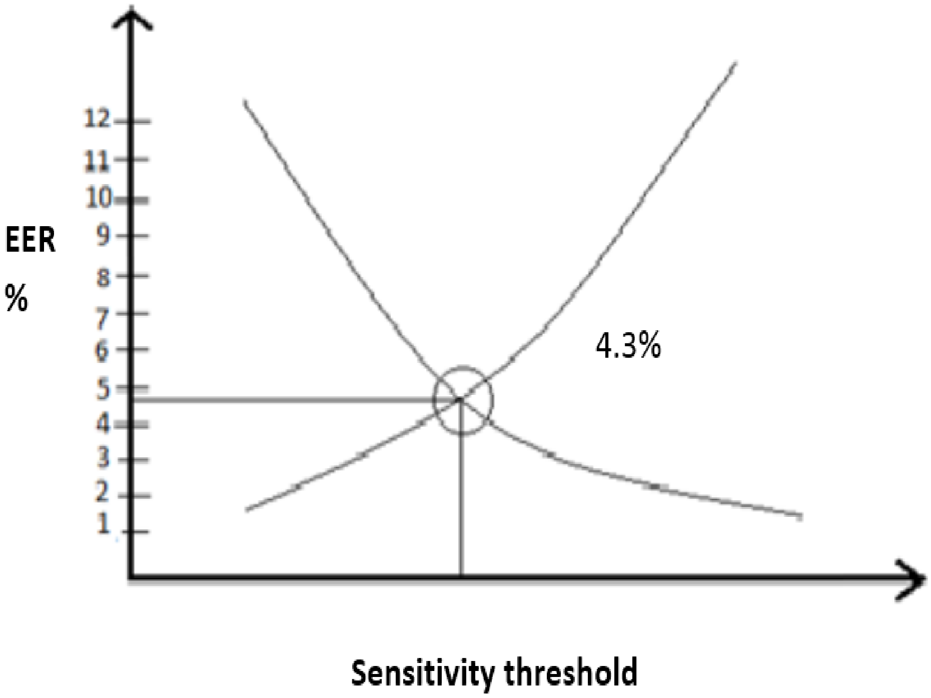


Figure 9. EER of the proposed system.

3. SECURITY ANALYSIS

The proposed system utilizes a parallel algorithm to randomly transform the given input to the transformed template and stores it in the database. The input, i.e., the combined feature vector's length will be between 50 and 500. Let us denote the length as *l* and the number of nodes as *n*. The number of possible transformations that can be performed on the given input ranges from *j* to *k*.

N (number of possible transformations) = $\sum_{i=j}^{k} C_i \wedge C_{i+j}$

C_i = the cipher obtained from the left fingerprint, right fingerprint and palm print.

C_{i+j} = the adjacent cipher of C_i .

N = the number of possible transformations.

The range of *'N'* depends on the *'l'* and is usually 50 to 100 in length and hence the number of transformations will be five or six because $2^5 = 32$ less than 50 and $2^6 = 64$ less than 100. Thus, if the length is *l*, the number of transformations is m for $2^m < l$. Also, every level has a transformation; level 0 has an *l-1* transformation, and level 1 has an *l-2* transformation. Level 2 has an *l-4* transformation, and level 3 has an *l-8* transformation, and this continues until the $2^m <$ l. Hence, this analysis clearly shows that it difficult to crack the security method and perform this *n* operation. Also, since the transformations are in powers of 2, the complexity of the program decreases. In order to improve the genuine acceptance rate (GAR), no minutiae points are eliminated, and the running time complexity will always be square of the length *l* (l^2).

4. CONCLUSION

In the proposed system, the feature vector of the three biometric traits (left fingerprint, right fingerprint, and palm print) are combined using a modified list ranking algorithm. This prevents hackers from attacking the system because, even if one key is compromised, the remaining two feature vectors must be known to hack the system. Also, the operations are performed on each node and the results are carried to the rest of the nodes to make the system rigid and to protect the system from hackers. From the previous survey carried out on the multi-biometric system, the FAR (false acceptance rate) was comparatively high and the FRR (false rejection rate) made the system inefficient. Therefore, by providing this appropriate solution, the FAR and FRR of this proposed system can be reduced. The proposed system is capable of performing one-way encryption such that, the original templates cannot be obtained by the hacker, meaning that the proposed security of the system is enhanced.

Funding: This study received no specific financial support.
Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study.

REFERENCES

[1] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, pp. 237-257, 2006.Available at: https://doi.org/10.3724/sp.j.1087.2008.01816.

[2] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature-level fusion," *IEEE Iransactions on Information Forensics and Security*, vol. 7, pp. 255-268, 2011.Available at: https://doi.org/10.1109/tifs.2011.2166545.

[3] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in *In 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems. IEEE*, 2008, pp. 1-6.

[4] A. Gyaourova and A. Ross, "Index codes for multibiometric pattern retrieval," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 518-529, 2012.Available at: https://doi.org/10.1109/tifs.2011.2172429.

[5] G. J. Tomko, C. Soutar, and G. J. Schmidt, "Fingerprint controlled public key cryptographic system," United States Patent US 5,832,091, issued November 31998.

[6] C. Li, J. Hu, J. Pieprzyk, and W. Susilo, "A new biocryptosystem-oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 1193-1206, 2015.Available at: https://doi.org/10.1109/tifs.2015.2402593.

[7] A. Othman and A. Ross, "On mixing fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 8, pp. 260-267, 2012.

[8] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature-level fusion," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 255-268, 2012.Available at: https://doi.org/10.1109/tifs.2011.2166545.

[9] S. Li and A. Kot, "Privacy protection of fingerprint database," *IEEE Signal Processing Letters*, vol. 2, pp. 115-118, 2011.Available at: https://doi.org/10.1109/lsp.2010.2097592.

[10] K. Cao and A. K. Jain, "Learning fingerprint reconstruction: From minutiae to image," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 104-117, 2015.Available at: https://doi.org/10.1109/tifs.2014.2363951.

[11] T. Uz, G. Bebis, A. Erol, and S. Prabhakar, "Minutiae-based template synthesis and matching for fingerprint authentication," *Computer Vision and Image Understanding*, vol. 113, pp. 979-992, 2009.Available at: https://doi.org/10.1016/j.cviu.2009.04.002.

[12] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *In International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg*, 2004, pp. 523-540.

[13] J. D. Golic and M. Baltatu, "Entropy analysis and new constructions of biometric key generation systems," *IEEE Transactions on Information Theory*, vol. 54, pp. 2026-2040, 2008.Available at: https://doi.org/10.1109/tit.2008.920211.

[14] W. Yang, J. Hu, and S. Wang, "A Delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement," *IEEE Transactions on Information Forensics and Security*, vol. 9, pp. 1179-1192, 2014.Available at: https://doi.org/10.1109/tifs.2014.2328095.

[15] C. Fang, Q. Li, and E.-C. Chang, "Secure sketch for multiple secrets," in *Int. Conf. Applied Cryptography and Network Security, Nejra, Spain*, 2010.

[16] Y. Liu, M. Hammad, and K. Wang, "Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint," *IEEE Access*, vol. 7, pp. 26527-26542, 2018.

[17] Q. N. Tran and J. Hu, "A multi-filter fingerprint matching framework for cancelable template design," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2926-2940, 2021.Available at: https://doi.org/10.1109/tifs.2021.3069170.

[18] H. Wang and S. M. Abdullahi, "Fractal coding-based robust and alignment-free fingerprint image hashing," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2587-2601, 2020.Available at: https://doi.org/10.1109/tifs.2020.2971142.

Views and opinions expressed in this article are the views and opinions of the author(s), Review of Computer Engineering Research shall not be responsible or answerable for any loss, damage or liability, etc., caused in relation to/arising from the use of the content.