Journal of Medical Systems (2019) 43: 112
https://doi.org/10.1007/s10916-019-1220-x

IMAGE & SIGNAL PROCESSING

A Novel Technique for Multi Biometric Cryptosystem Using Fuzzy Vault

V. Sujitha [1] · D. Chitra [1]

Received: 23 December 2018 / Accepted: 21 February 2019 / Published online: 21 March 2019

Abstract
Biometric authentication is the process of recognizing a person by means of his\her psychological or behavioral traits. One of the most important issues faced by the biometric system developer is to protect the template obtained from the biometric of a person. Unimodal biometric system has some drawbacks such as noisy data, interclass variations and spoof attack. Multimodal biometric system has been developed to address the boundaries of unimodal biometric system and increase the security of template. In this paper, template security analysis of multimodal biometric system based of fingerprint and palmprint is proposed and implemented. Fuzzy vault scheme is employed to protect both the fingerprint and palmprint template. At enrollment, image processing techniques such as image enhancement, segmentation and bottom-hat filtering are applied on both the biometric to improve the quality and subsequently the most important features are extracted. Extracted features are concatenated. Combined features along with secret key are utilized to generate the database in the vault. During authentication, query images are sent as an input with the stored template to recover the key. Experimental results are shown that the proposed multi biometrics system performs well than the other methods considered for comparison.

Keywords Brute-force attack · Fingerprint · Multimodal biometric system · Palmprint and security analysis

Introduction

In the modern era, internet has emerged as one of most important and commonly used technology for sharing or exchanging information. An accurate authentication plays a main job in secure communication. Generally, knowledge-based and token-based security methods are utilized for authentication. But, these methods suffer from some limitations such as passwords may be easily guessed by unauthorized user and smartcards may be lost or stolen by attackers [1]. To overcome the limitations of traditional security systems, biometric based authentication system has been developed. Biometric system is the branch of science that identifies the person based on his or her psychological or behavioral characteristics such as fingerprint, palmprint, palm vein, face, iris, gait, writing style and voice. Unlike smart cards and passwords-based security systems, biometric system cannot be guessed, forgotten, forged and misplaced [2, 3].

Unimodal biometric system verifies the person based on single biometric source of information. Such systems have some troubles such as noisy information, non-universality, spoof attack and inter class variations which reduce the performance of the system and security [4]. To address these issues and increase the security, multi modal biometric systems have been introduced. Multi biometric uses two or more modalities of same person to increase the security and overall efficiency of the system. Based on the performance, the multi biometric system is categorized into many groups such as sensor, matching score, and feature and decision level fusion [5]. This paper focuses on feature-level fusion. The key idea behind feature-level fusion is that combining the extracted feature points of multi biometric algorithms into a single feature points, after preprocessing and feature extraction is done.

Protection of template is one of main problem in biometric authentication system. Biometric protection methods can be

This article is part of the Topical Collection on *Image & Signal Processing*

✉ V. Sujitha
sujithavpacet@gmail.com

D. Chitra
chitrapacet@gmail.com

[1] Department of CSE, P. A. College of Engineering and Technology, Pollachi, Tamilnadu, India

typed into biometric cryptosystem and feature transformation method. The obtained biometric feature sets are manipulated employing transformation in the feature transformation method. In this approach, only the modified templates are stored in the data base and matching is done in the transform domain [6]. To ensure high security, biometric cryptosystem uses the merits of both cryptography and biometrics. Key generation and key release approaches are widely used methods to combine biometrics with cryptography. Examples of bio cryptosystems consist of fuzzy vault [7] and commitment [8], source coding [9] and fuzzy extractor [10].

Fingerprint is the ridges and valley of finger and shown in Fig. 1. Fingerprint recognition is most frequently used form of biometrics to classify the individual due to its acceptance, feasibility and reliability [2]. Palmprint recognition has demonstrated to be one of the most stable and unique biometrics and widely used method because of its performance, high acceptance rate, uniqueness and low cost. Palm print consist three major features which include three flexion creases or principal lines, secondary creases or wrinkles and ridges. Figure 2 illustrates the features of palm print. By fusing important features of fingerprint and palmprint such as minutiae and principal lines, it is possible to construct a multi biometric system with high security [2].

In this paper, presents a novel approach for protecting multibiometric template of a person in multimodal scheme. The proposed technique consists of three major process (i) Preprocess and extract the feature points from palm print and fingerprint (ii) Perform the feature-level fusion to get a single feature set and (iii) construct the fuzzy vault to secure multi biometric template. Further to this, the performance of the proposed multi biometric system is examined against brute force and correlation attack.

Contribution and outline of the paper as follows: In Section 2 describes the related works. In Section 2 presents the implementation work of proposed vault locking and unlocking algorithms. The simulation results are demonstrated in section 4. In section 5, give main conclusions from the proposed scheme and followed by relevant references.

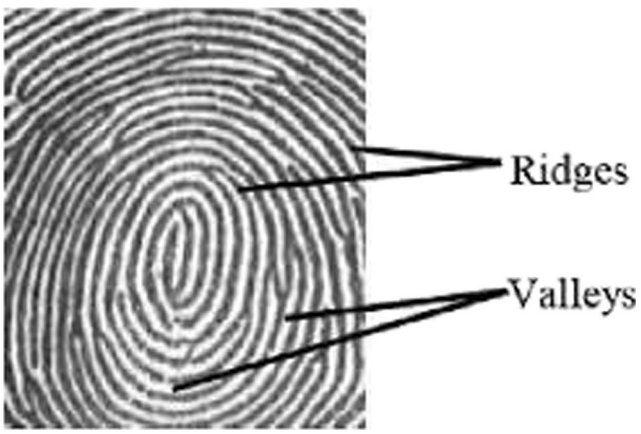


Fig. 1 Fingerprint image

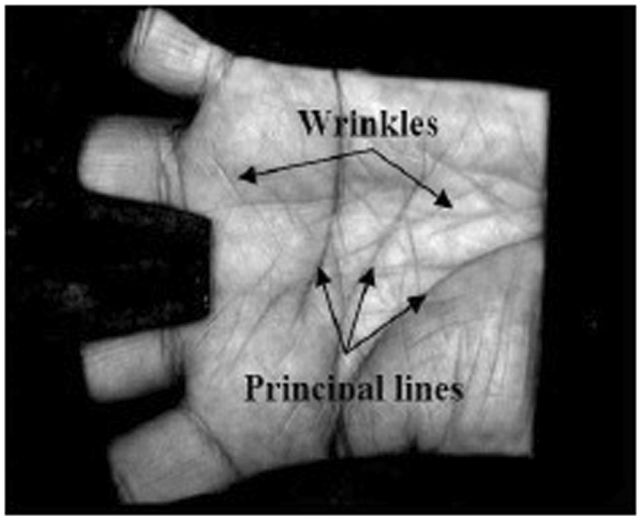


Fig. 2 Palmprint image

Background

Numerous template protection methods including fuzzy vault [7] and [11], fuzzy commitment [8], source coding [9] and fuzzy extractor [10] introduced in biometrics. Among these methods, fuzzy vault developed by Jules et al. [7] provides higher security for biometric template. Fuzzy vault method is secure in the sense it does not disclose information regarding minutiae while it uses one-way hash function for encryption and it has capacity to handle intra-class dissimilarities in biometric data [12]. Brindha et al. [2] have presented a fuzzy vault based multimodal template security method for fingerprint and palmprint. Enrolled fingerprint and palm print images were preprocessed using some image processing methods such as binarization, thinning, minutiae extraction and Region of Interest (ROI) extraction. After preprocessing, features of both the images were extracted. Then the features are concatenated and projected on the polynomial. Chaff points were added with the feature vectors. Features along with the secret key are merger and it's utilized to generate the vault. At the time of verification, query features are comparing with the database in the vault to recover the key.

In 2008, Karthick Nanda Kumar et al. explained the fusion of multi biometrics and minentropy estimates to calculate the protection of the fuzzy vault [13]. In 2012, Nagar et al. [6] proposed a template protection scheme employing fuzzy vault and fuzzy commitment. Fuse the multibiometric features using feature level fusion method. The proposed scheme consists of three stages. At stage one, features of multi biometrics are converted into binary string. In stage two, features were

combined and in third stage securely sketching. Results are shown that the multi biometrics scheme outperforms than single biometric scheme. Vinothkanna et al. [14] have developed a multi biometric system using fingerprint and ear images. Initially, both the biometric images are filtered by adaptive median filter to remove noise. Then minutiae points were extracted from fingerprint image. Active Appearance Model (AAM) is applied on the preprocessed ear image for extracting the features. Two features are grouped and chaff points were included. Fuzzy vault is constructed by combining secret key with the grouped feature points. During verification, individuals are identified by comparison made between the query features with vault [7].

Fuzzy based approach is utilized for securing biometric template by the authors Selwal et al. [15]. In this method, features of fingerprint and hand geometry are combined to reduce the spoof attacks on biometric systems. Simulation results are promising since biometric templates are protected during feature fusion process. The performance of the multi biometric system is improved with equal error rate of 3.3% and increased Genuine Acceptance Rate (GAR) of 97.3%. The goal of this work is to generate the fuzzy vault employing combined features of fingerprint and palmprint.

Proposed multimodal biometric fuzzy vault

Multimodal biometric system provides higher security and improved performance then the unimodal biometric system. It overcomes the limitations of single biometric system. Fuzzy vault based multimodal biometric systems are more secure. In this paper, fuzzy vault scheme is employed to protect both biometric templates such as fingerprint and palmprint.

Multimodal biometric system recognizes a person based on multiple sources of information. It utilizes a combination of different recognition methods. Their efficiency is better than the unimodal biometric systems. This paper uses fuzzy vault scheme for securing the multi biometric template. The proposed system includes the fused feature vectors from fingerprint and palmprint. Figure 3 shows the framework of the proposed multimodal biometric fuzzy vault. It is based on two biometrics namely palmprint and fingerprint. In this work, two different feature techniques are used to extract the feature vectors from the biometrics. The feature vectors are combined by using proper technique. Then, fused feature vectors are used to generate vault and finally stored in the database.

In the proposed system, the biometric feature vectors are represented using Galois field GF (2^{16}). The series issue of the proposed multimodal biometric fuzzy vault is the fusion of feature vectors from different biometrics (fingerprint and palmprint) into a single feature vector set.

Fingerprint minutiae extraction

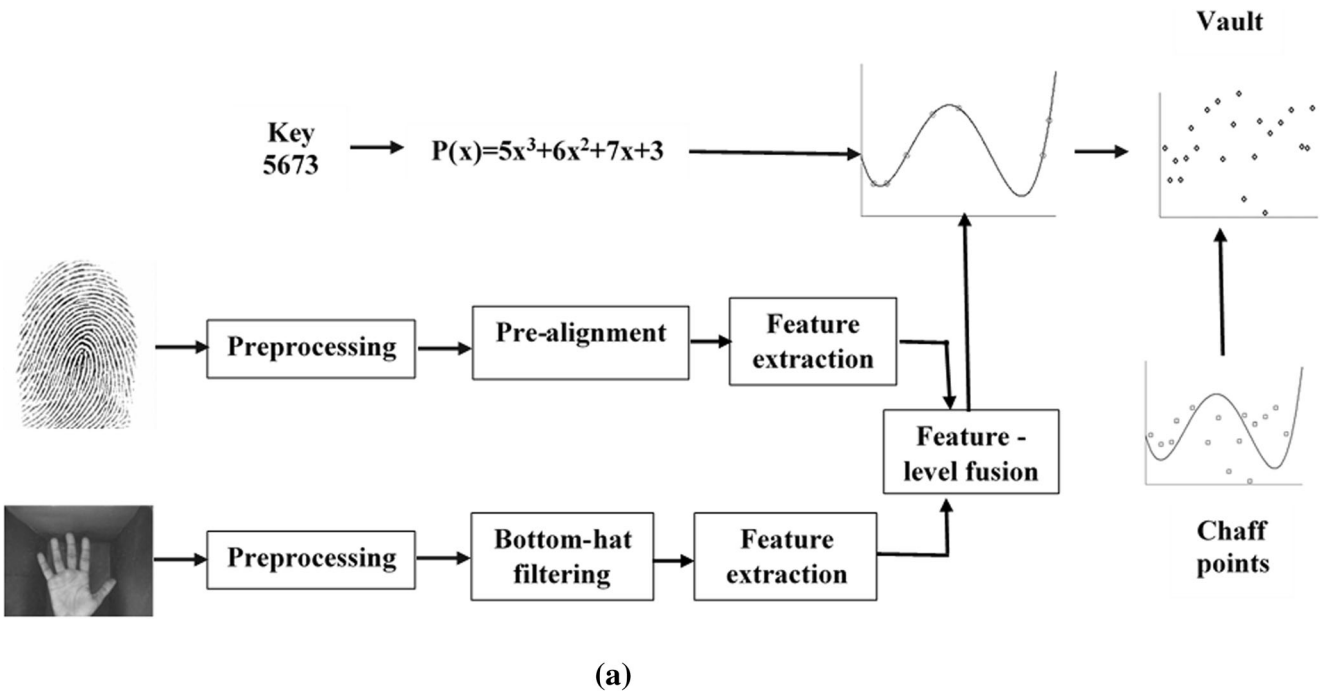
Proposed multi biometric system follows the technique proposed by Bhowmik, et al. [16] for minutiae extraction. Initially, fingerprint images are enrolled and preprocessed by some image pre-processing methods which include histogram equalization; binarization and segmentation in order enhance the image quality and guarantee the reliability [17]. Figure 4 illustrates the preprocessing of fingerprint image. Minutiae points are extracting using crossing number (CN). The location and orientation of the selected minutiae points are pre-aligned and quantized using the technique proposed by Tam et al. [18]. In this method, reference point is found among direction. The reference point is employed as origins and direction represents the axis. Only the most important feature vectors are chosen for vault generation. It is selected based on the quality.

During verification, the query feature vectors are employed to remove the chaff points. A simple decision maker is applied to determine correspondence between vault points and query feature vectors. Query having a matching point in the vault can unlock the vault.

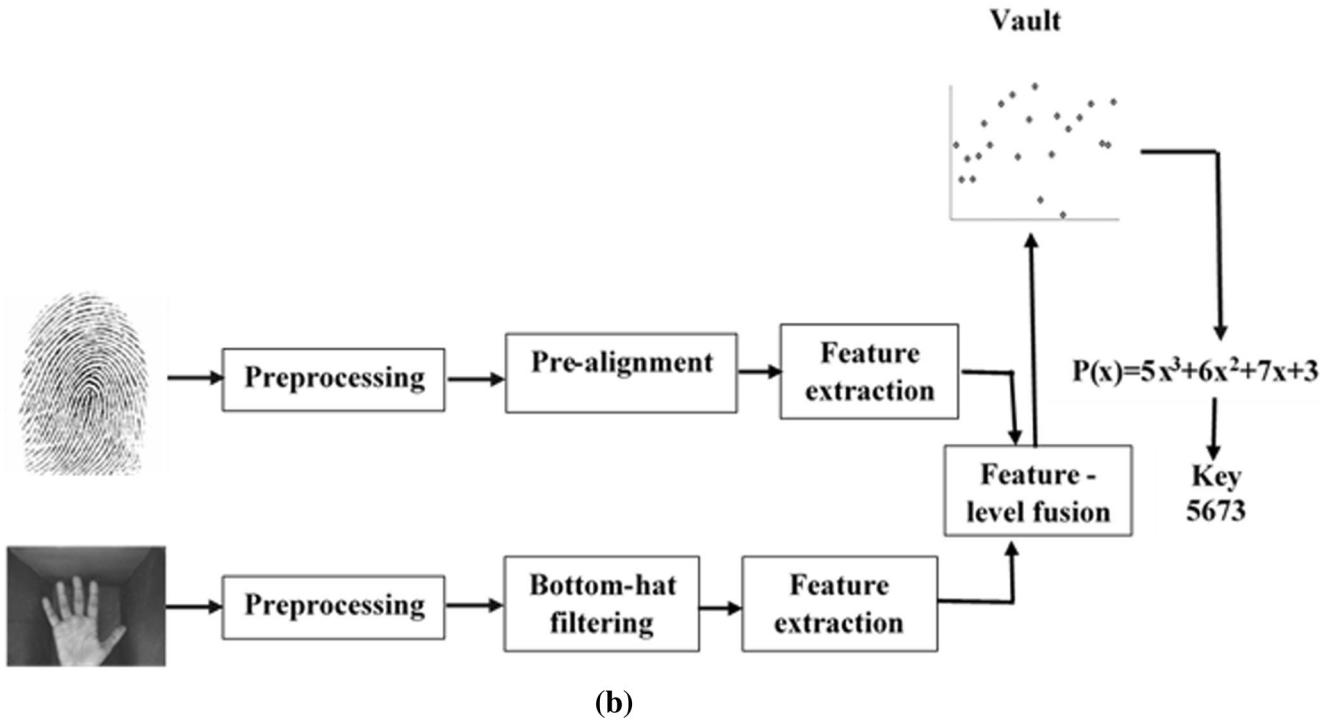
Palmprint feature extraction

Palmprint based biometric identification system has been used recently due to its uniqueness, permanence and high acceptance rate. The important merit of palmprint based recognition system is the accessibility of more space and contains more information than other traits such as fingerprint, iris etc. In palmprint recognition, feature extraction is the crucial step. Proposed technique uses principal line as features. Principal lines are attained from a low resolution palm images and then the direction and location are extracted from that line. Those values are used to identify an individual uniquely.

Various techniques have been developed for extracting principal line which includes prewitt, canny and sobel [19]. But, these pre-defined edge detectors produce in addition insignificant principal lines. To solve this problem, the proposed technique constructs the palmprint cryptosystem in three phases. In the first phase, image processing methods such as binarization, noise filtering and morphological operation are applied to improve the image quality. In the second phase, palmprint alignment and Region of Interest (ROI) extraction are performed by detecting reference point between fingers, reference line construction and normalization. In the third step, bottom-hat filtering method presented in [20] is adopted to extract the most important feature vectors and is depicted in Fig. 5. In bottom-hat filtering method, Four Average Filter (AVF) along four directions such as AVF_0, AVF_{45}, AVF_{90} and AVF_{135} are formed. They convolved with the preprocessed ROI to produce filtered image along 4 directions. AVF masks employed in this paper are shown in Fig. 6.



(a)



(b)

Fig. 3 Block diagram of proposed multi biometric system **a** Vault encoding **b** Vault decoding

Filtering operation can be expressed as:

$$F_0(x,y) = (I_0(x,y)*AVF_0) \quad (1)$$

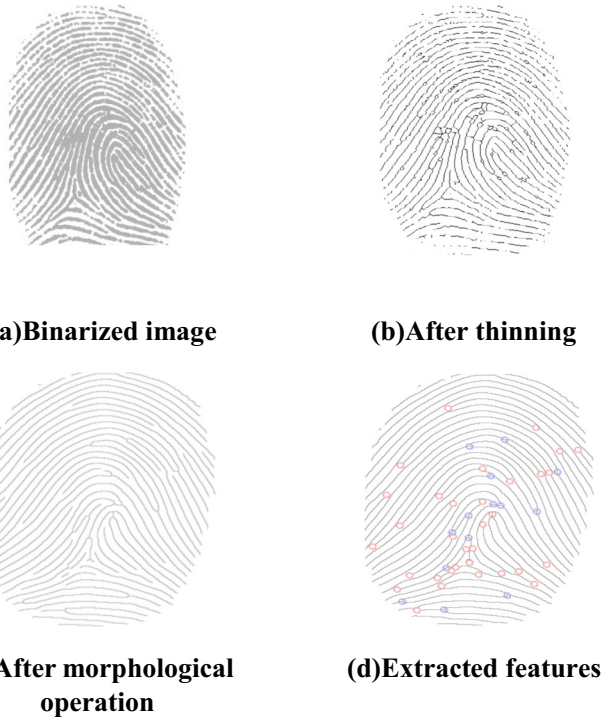
$$F_{45}(x,y) = (I_{45}(x,y)*AVF_{45}) \quad (2)$$

$$F_{90}(x,y) = (I_{90}(x,y)*AVF_{90}) \quad (3)$$

$$F_{135}(x,y) = (I_{135}(x,y)*AVF_{135}) \quad (4)$$

Where, F is the filtered image and I denotes the preprocessed image. Bottom-hat filtering is the method of subtracting the image from the closing of it. It is performed by dilation followed by erosion process and given below.

$$I_D'(x,y) = \max_{p,q}\left(I\left(x-p,y-q^{p,q} + S(p,q)\right)\right) \quad (5)$$



(a)Binarized image (b)After thinning

(c)After morphological operation (d)Extracted features

Fig. 4 Fingerprint preprocessing

$$I'_E(x,y) = \max_{p,q}\left(I\left(x+p,y+q^{p,q}-S(p,q)\right)\right) \quad (6)$$

The main advantage of morphological operation used in bottom-hat filtering method is that it improves the quality of an image and highlights the details. Filtered images are fused to produce a single image by calculating mean of four filtered image. Cleaning operation is performed to highlight principal lines and represented in Eq. (7)

$$I'(x,y) = \begin{cases} 0 & I(x,y) \geq km \\ I(x,y) & otherwise \end{cases} \quad (7)$$

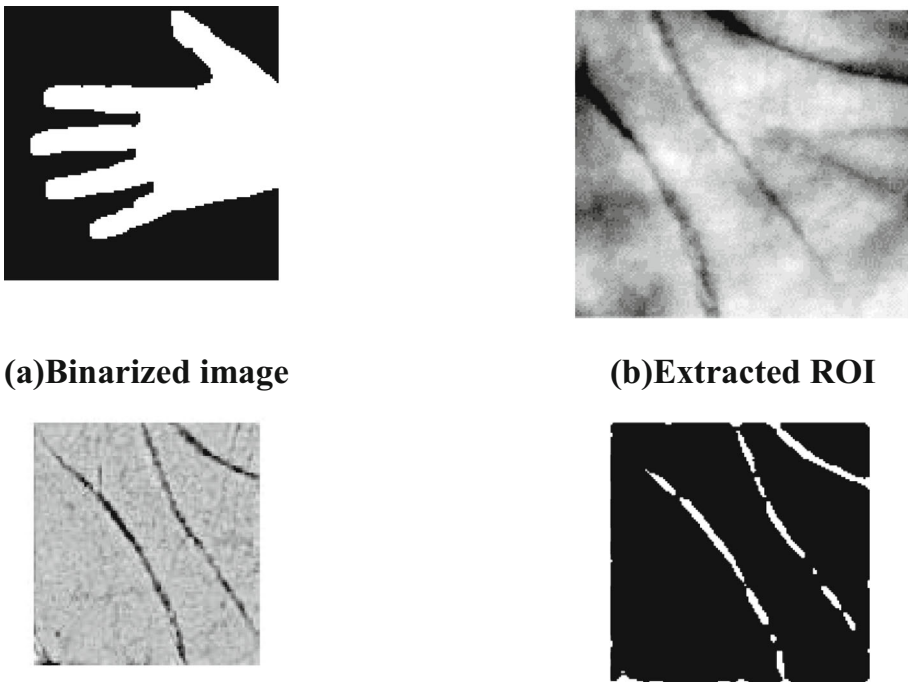
Where, m indicates the mean and k denotes the scaling value. Sufficient principal lines are extracted at last. The obtained palmprint feature points are concatenated with fingerprint features and utilized for fuzzy vault construction.

In this paper, for each user, 4 images are used as input for all images feature extraction process is performed. The most important feature vectors are selected based on their quality. The common points from all the images are determined to get the feature vectors. The features extracted from both the palmprint and fingerprints are concatenated. Along with this feature vectors, some randomly generated chaff or dummy points are added.

Encoding and decoding of fuzzy vault

The proposed multi biometric system includes the fusion of features from palm and finger images. Initially, both images (enrolled fingerprint and palmprint) are preprocessed using different techniques. The steps followed during preprocessing of fingerprint are image enhancement, binarization, segmentation, prealignment, quantization and minutiae extraction. Palmprint image is preprocesses using binarization, morphological operation, reference point detection, line extraction,

Fig. 5 Palmprint preprocessing



(a)Binarized image (b)Extracted ROI

(c)After Bottom-hat filtering (d)Extracted features

Fig. 6 Average filters

$$AV_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad AV_{45} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$AV_{90} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \quad AV_{135} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

ROI extraction, bottom-hat filtering and feature extraction. The feature vectors are represented as an element in GF (2^{16}). The important features are extracted from both palmprint and fingerprint are combined and projected on the polynomial. Security of proposed multimodal biometric system depends on the number of dummy points. The security of fuzzy vault increased by using more number of dummy points included with genuine points. Dummy points make the hacker to acquire more time to concession the vault but consume extra computation time. Unlocking is reverse process of vault locking. It is used to recover the secret key.

Fuzzy vault locking and unlocking algorithm

This sub section describes the functioning of proposed multimodal biometric system. Proposed algorithms for fuzzy vault encoding and decoding is explained in Tables 1 and 2 respectively.

Experimental results and discussion

This section discusses the performance of the proposed multi biometric system in terms of GAR and FRR. Efficiency of the system is also analyzed under correlation and brute force attack.

Performance evaluation

The proposed fuzzy based multi biometric template protection technique is implemented in MATLAB. The number of genuine vectors in the multimodal fuzzy vault is between 25 and 40. The merits of including chaff points with the genuine

Table 1 Fuzzy vault locking algorithm

Step1: Fusion

Let F = {f_1,f_2,f_3……f_m} and P = {p_1,p_2,p_3…..p_n} represent two feature points (f ϵ R^m and P ϵ R^n) obtained from fingerprint and palmprint respectively. Extracted feature vectors are subsequently combined to get single feature vector set.

$$FV = F + P$$

Dimension of FV is k, k = (m + n)

$$FV = \{f_1, f_2, f_3, \cdots f_m, p_1, p_2, p_3, \cdots p_n\}$$

Where FVϵ R^{m+n}

Step 2: Polynomial generation

Secret key $SK = \{K\}_{i=0}^{n-1}$ is employed to produce the polynomial P with order n.

Step 3: Genuine points generation

Project the feature vector FV using polynomial P to make genuine points G

$$G = [(f_1, P(f_1)), (f_2, P(f_2)), \cdots (f_m, P(f_m)), (p_1, P(p_1)), (p_2, P(p_2)), \cdots (p_n, P(p_n))]$$

Step 4: Chaff or dummy points generation

Generate some chaff points, C randomly

$$C = [(x_1, y_1), (x_2, y_2), (x_3, y_3), \cdots (x_p, y_q)]$$

Step5: Vault construction

Construct the FV by integrating generated genuine points with the dummy(chaffs) points

$$Vault = G \cup C$$

Table 2 Fuzzy vault unlocking algorithm

Step 1: Extraction of feature vectors
Query feature vectors are calculated in the same way used in vault locking.
Step 2: Comparison
Compare query feature vectors with the stored fuzzy vault
Step 3: Matching
Compute the Euclidean distance.
Step 4: Extraction of polynomial
Genuine points are filtered out based minimum distance between vault and query feature vector set.
Step 5: Decoding
Apply Reed Solomon (RS) decoder on the polynomial to extract secret key.

vectors are to increase the security of template. The dummy points merged in this proposed technique is 10 times more in number than that of genuine vector so, total number of points used for constructing the vault is 715. Performance of the proposed multimodal biometric fuzzy vault is evaluation by computing some commonly used statistical measure such as GAR and FRR. Table 3 lists the parameters employed for implementation.

This paper has developed a framework for protecting multiple biometric template of a person using fuzzy vault. The proposed technique can protect multiple biometric template of a person by first fusing features of both (fingerprint and palmprint) biometric and then applying fuzzy vault scheme. Proposed technique provides template security at two levels (i) Fusion of two feature vector and generates single feature vector set and (ii) Use of fuzzy vault scheme makes it very hard to get the original information from the stored database. Concatenation of two biometric feature vectors not only improves the performance of individua biometric system but also to generate single vault (data base) for both the biometrics.

The performance of the proposed multimodal biometric fuzzy vault is summarized in Table 4. The GAR of the proposed technique is 95% at a FAR is 0.05 and degree of polynomial is 8. Fuzzy vault based multi biometric system that uses same technique for extracting features from both palmprint and fingerprint is approximately 87.8% (FNMR) at FMR of 12.2%. Thus, there is some improvement in the GAR of the proposed technique due to the application of different technique for extracting features.

Table 5 evaluates the performance of the current technique with the other methods in terms of GAR. From the Table 5, it can be shown that the proposed technique outperforms than other methods considered for comparison from the literature.

Table 3 Simulation parameters for proposed multi biometric technique

Parameter	Fingerprint	Palmprint	Multimodal
Number of genuine vectors, G	40	25	65
Number of chaff points, C	400	250	650
Total points, T	440	275	712
Degree of polynomial, k	8–12	8–12	8–12

Table 4 Performance of the proposed technique

Degree of Polynomial, k	GAR (%)	FAR (%)
8	95	0.05
9	93	0.34
10	90	0.03
11	88	0.02
12	83	0.01

Brute-force attack

Nandakumar et al. [21] and [22] analyzed the security of multibiometric vault in terms of security bits. Security analysis of the proposed technique is carried out by evaluating min-entropy of template. Table 6 gives the security of proposed technique under brute force attack. According to Nandakumar et al. [22] and [9], the min- entropy of proposed fuzzy vault can be expressed as:

$$H_\infty = -log_2\left(\frac{\binom{G}{k+1}}{\binom{T}{k+1}}\right) \tag{8}$$

Where,

G Number of genuine points
C Number of chaff points
k Degree of polynomial
T Total number of points (T = G + C)

From the Table 6, noticed that the degree of the polynomial is considered mainly to enhance the security. Polynomial with higher degree needs lot of computational attempt to decode the vault and reconstruct the key and the polynomial with minor degree can be simply decoded by the attackers.

Table 5 Performance comparison

Methods	GAR (%)
Brindha et al. [2]	88
Nagar et al. [6]	87
Vinothkanna et al. [14]	85
Proposed	95

Table 6 Security analysis of the proposed technique

Degree of polynomial	Total combinations tried to decode the vault	Number of combinations required	Total evaluations	Security bits
8	3.6921×10^{48}	3.1967×10^{10}	1.1549×10^{38}	127
9	2.5677×10^{50}	1.7901×10^{11}	1.4355×10^{39}	130
10	1.6236×10^{52}	8.9506×10^{11}	1.8139×10^{40}	133
11	9.3898×10^{53}	4.0278×10^{12}	2.3312×10^{41}	137
12	5.0054×10^{55}	1.6421×10^{13}	3.0481×10^{42}	140

Table 7 Security comparison

Method	k	Total combinations tried to decode the vault	Number of combinations required	Total evaluations	Correlation attack
Brindha et al. [2]	10	1.1357×10^{27}	1.4307×10^{10}	7.9380×10^{16}	Not considered
Meenakshi et al. [23]	10	2.3848×10^{23}	3.4270×10^{11}	6.9587×10^{11}	Not considered
Proposed	10	1.6236×10^{52}	8.9506×10^{11}	1.8139×10^{40}	Removed

Table 7 compares the security analysis of proposed technique with the existing other methods. From the Table 7, it is inferred that the proposed technique can provide higher security than other methods.

Correlation-attack

Correlation attack assumes that some attacker intercepts multiple enrollments which are created using the same person biometric data [2, 24]. The fuzzy vault may be constructed by two different ways: (i) fuzzy vault generated by same genuine vectors with different key and (ii) minutiae points are same and chaff points are different. Let the attacker interrupts two vaults securing the set of minutiae {n} and {n'}. A hacker can found translation and rotation values of {n'} minutiae. i.e. {T(n')}. If distance (n, T(n')) < = Threshold (Th),transformed features of (n') correlate with (n). Let V includes of vault pairs that belong to {n} with distance (n, T(n')) < = Th. RS decoder used by the hacker to decode the vault when the matching pairs of (n, n') are smalller than non-matching pairs. Suppose {n} and {n'} are equal in size, for each genuine and chaff points of {n} there exist a both those points of {n'}. Minutiae points are quantized with the help of method described in [18] to oppose the correlation attack. This quantization process conforms that the current method resistance against correlation attack.

Conclusion

This paper provides a new technique for protecting multiple biometric sources of a person as a single entity. The goal of the proposed technique is to enhance the security of multi biometric template employing fuzzy vault scheme. During enrollment, the fingerprint and palmprint biometric images are preprocessed using image processing methods in order to improve the quality of an image and make it suitable for other process that is feature extraction and fusion. Subsequently, the most important points are extracted from fingerprint and palmprint and concatenated to have single feature vector set. Secret key and fused points are used to generate the vault. We have also confirmed that the proposed technique provides higher security compare to single bio traits. Proposed method provides better GAR and to oppose brute force attack, correlation attacks. In future, may include wavelet transform to improve the performance and also include some other biometric traits to increase security.

Compliance with ethical standards

Conflicts of interest The authors have no conflict of interests and the paper has not been submitted to any other Journals.

Human and animal rights This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent It is not required as the dataset is taken online databases.

References

1. Fu, B., Yang, S. X., Li, J., and Hu, D., Multibiometric Cryptosystem: Model Structure and Performance Analysis. IEEE Transactions on Information Forensics and Security 4(4):867–882, 2009.
2. Brindha, V. E., and Natarajan, A. M., Multi-Modal Biometric Template Security: Fingerprint and Palmprint Based Fuzzy Vault. Journal of Biometrics & Biostatistics 3(6):1–6, 2012.

3. Sanjekar, J. B., and Patil, P. S., An Overview of Multimodal Biometrics, Signal & Image Processing. An International Journal (SIPIJ) 4(1):57–64, 2013.
4. Mishra, A., Multimodal Biometrics it is: Need for Future System. Int. J. Comput. Appl. 3(4):28–33, 2010.
5. Prakash, S. M., Betty, P., and Sivanarulselvan, K., Fusion of Multimodal Biometrics using Feature and Score Level Fusion. International Journal on Applications in Information and Communication Engineering 2(4):52–56, 2016.
6. Nagar, A., Nandhakumar, K., and Jain, A. K., Multibiometric cryptosystem based on feature level fusion. IEEE Transaction on Information Forensics and Security 7(1):255–268, 2012.
7. Juels, A., and Sudan, M., A fuzzy vault scheme. Des. Codes Crypt. 38(2):237–257, 2006.
8. Juels, A., and Wattenberg, M., A fuzzy commitment scheme. ACM Conference on Computer and Communications Security, New York: ACM, 28–36, 1999.
9. Draper, S., Khisti, A., Martinian, E., Vetro, A., and Yedidia, J. S., Using distributed source coding to secure fingerprint biometrics. IEEE International Conference on Acoustics, Speech and Signal Processing, IN-9582274, 2007.
10. Dodis, Y., Reyzin, L., and Smith, A., Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. Advances in cryptology-Euro crypt, Springer Berlin Heidelberg, 523–540, 2004.
11. Uludag, U., and Jain, A. K., Securing fingerprint template: fuzzy vault with helper data. In: Proceedings of IEEE Workshop on Privacy Research in Vision, pp. 163–169, 2006.
12. Orencik, C., Fuzzy vault scheme for fingerprint verification: implementation, analysis and improvements. Sabanci University, pp. 1–50, 2008.
13. NandaKumar, K., Multibiometric systems: fusion strategies and template security. PhD Thesis, Department of Computer Science and Engineering, Michigan State University, 2008.
14. Vinothkanna, R., and Wahi, A., Fuzzy Vault Fusion Based Multimodal Biometric Human Recognition System with Fingerprint and Ear. J. Theor. Appl. Inf. Technol. 59(2):304–316, 2014.
15. Selwal, A., Gupta, S. K., and Kumar, S., A Scheme for Template Security at Feature Fusion Level in Multimodal Biometric System. Advances in Science and Technology 10(31):23–30, 2016.
16. Bhowmik, P., Bhowmik, K., Azam, M. N., and Rony, M. W., Fingerprint image enhancement and its feature extraction for recognition. Int. J. Sci. Technol. Res. 1(5):117–121, 2012.
17. Tatar, F., and Machhout, M., Improvement of the fingerprint recognition process. Int. J. Bioinform. Biosci. 7(2):1–16, 2017.
18. Tam, B., Mihăilescu, P., and Munk, A., Security considerations in minutiae-based fuzzy vaults. IEEE Trans. Inf. Forensics Secur. 10(5):985–998, 2015.
19. Malik, J., Sainarayanan, G., and Dahiya, R., Personal Authentication using Palmprint with Sobel Code, Canny Edge and Phase Congruency Feature Extraction Method. ICTACT Journal on Image and Video Processing 2(3):357–368, 2012.
20. Bruno, A., Carminetti, P., Gentile, V, La Cascia, M., and Mancino, E., Palmprint principal lines extraction. In the proceedings of the IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications, BIOMS, 2014.
21. Jain, K., Nandakumar, K., and Nagar, A., Biometric template security. EURASIP Journal on Advances in Signal Processing:1–17, 2008.
22. Nandakumar, K., Jain, A. K., and Pankanti, S., Fingerprint based fuzzy vault: implementation and performance. IEEE Trans. Inf. Forensics Secur. 2(4):744–757, 2007.
23. Meenakshia, V. S., and Padmavathi, G., Security analysis of password hardened multimodal biometric fuzzy vault with combined feature points extracted from fingerprint, iris and retina for high security applications. Proc, Computer. Science. 2:195–206, 2010.
24. Kholmatov, A., and Yanikoglu, B., Realization of correlation attack against the fuzzy vault scheme. Proc. SPIE 6819:681900–681907, 2008.