Cluster Computing (2019) 22:S12817–S12825
https://doi.org/10.1007/s10586-018-1762-6

Security analysis of prealigned fingerprint template using fuzzy vault scheme

D. Chitra[1] · V. Sujitha[1]

Received: 8 November 2017 / Revised: 3 January 2018 / Accepted: 6 January 2018 / Published online: 20 January 2018

Abstract

Biometric systems accumulate information from biometric elements of an individual and used to exceptionally confirm the person with the physical and behavioral properties of the biometric characteristic. Biometrics and cryptography systems have been identified as the two main components of digital security system. Cryptography is combined with biometric to achieve high security. In this paper, fingerprint template protection is proposed which is based on fuzzy vault scheme. Initially, enrolled fingerprint images are preprocessed using some image processing techniques and preprocessed images are prealigned automatically using directed reference point. All the minutiae points are extracted and extracted minutiae features along with secret key are used to produce the fuzzy vault. Query features are given as an input with the stored template to recover the corresponding key. The proposed method is validated on FVC 2002 database. Simulation results prove that the proposed method can achieve high genuine acceptance rate with improved security.

Keywords Biometrics · Bio cryptosystems · Brute force attack · Correlation attack · Fingerprint · Fuzzy vault

1 Introduction

Biometrics is the exploration of measuring human uniqueness with the end goal of authenticating or identifying the character of a substance. Biometrics concerns with identifying people by their physiological characteristics such as fingerprint, iris, retina, palm print, hand geometry and face or some behavioral aspects such as voice, signature and gesture. Biometric technology needs huge volume of biometric data for template creation which causes some serious issues like leakage of privacy. The template security is considering important feature because stolen images are reused by hackers. To address the various security problems, integration between biometrics and cryptography has led to the development of new technology called as bio crypto systems or bio crypto technology [1]. In a biometric cryptosystems, protected template is constructed from the input biometric template and stored into the system database as an alternative of the original image. In lack of the genuine user's biometric data, it must be computationally very hard to recreate the original pattern from the template.

Different types of bio crypto technology have been proposed namely fuzzy extractor [2], fuzzy vault scheme [3] and fuzzy commitment [4–6]. Among these bio crypto technologies, the fuzzy vault system is one of the most important technologies and provides high security for template protection. Since fuzzy vault scheme is introduced, many characteristics have been employed to develop bio crypto systems using fuzzy vault system such as fingerprint [7,8], palm print [1], face [9] and iris [10]. Fingerprint recognition is one of most commonly used biometrics to identify the person more than 100 years due to its consistency over time, acceptance, feasibility and reliability. Fingerprint is a pattern of valleys and ridges [11,12]. Fingerprint matching algorithms are classified into three groups namely minutiae based matching, non-minutiae based matching and correlation based matching. Minutiae based matching uses extracted local minutiae features for comparison. Non-minutiae matching uses shape, orientation and frequency of fingerprint in order to perform matching. Correlation based matching calculates the pixel wise correlation [8,13–17]. Minutiae features of fingerprint are shown in Fig. 1.

✉ V. Sujitha
sujithavpacet@gmail.com

D. Chitra
chitrapacet@gmail.com

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

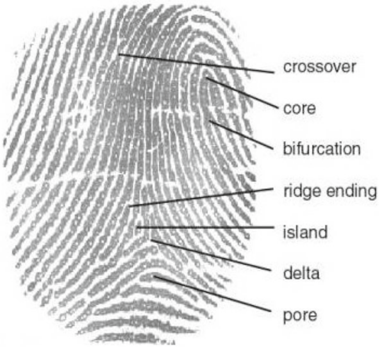


Fig. 1 Minutiae features of fingerprint

Fuzzy vault scheme [3] is a key binding approach and can compensate for intra class variation in the data. Fuzzy vault scheme saves the data only transformed version of biometric template for protection. The challenging task in fuzzy vault is the alignment of query with the stored biometric template. For this reason, absolute pre-alignment is adopted based on directed reference point proposed in [18]. It accurately aligns both query and template minutiae. Furthermore, performance of proposed bio crypto system is tested against brute force attack and correlation attacks to prove its security. Empirical findings showed that the proposed system resistant against brute force attack and correlation attack.

This paper is ordered as follows: Sect. 2 gives brief overview of related work. Proposed minutiae based fuzzy vault system is explained in Sect. 3. Section 4 demonstrates the simulation results. Conclusion of this work is presented in Sect. 5 followed by relevant references.

2 Background

Many techniques have been developed for the implementation of biometric cryptosystem based on fuzzy vault. Juels and Sudan [11] in 2002, proposed the fuzzy vault scheme that is used to protect biometric templates using polynomial construction method. It is a better method for storing fingerprint minutiae templates protected as a part of a security application [3]. As there are other biometric cryptosystems ([2,14], and [18]) being considered for securing fingerprint templates, but the fuzzy vault scheme is one of the most excellent scheme for template protection compared to other.

In 2011, Hanoon [19] used histogram equalization followed by vector quantization to improve the quality of fingerprint image and shown better result in terms of efficiency. Bhowmik et al. [12] presented a method for fingerprint enhancement. The authors used discrete fourier transform (DFT) and histogram equalization techniques to increase the contrast of images. DFT method showed some improvement by cascading above mentioned enhancement techniques. Barnouti [20] combined histogram equalization with the compression methods in order to enhance the contrast of the image. Compression method showed increased recognition rate when applying histogram equalization technique during enrollment process.

Uludag et al. [21] used helper data to improve the fuzzy vault system performance. In this method, biometric template is stored after changing to other set of coordinates. Results showed that the helper data does not leak information about the protected fingerprints and increased security. In 2007, Nandakumar et al. [7] enhanced the performance of fuzzy vault using minutiae matcher. They used high curvature points as a helper data to align the query minutia with the stored template. Nagar et al. [22] presented method for securing fingerprint template based on fuzzy vault with minutiae descriptors. The authors used local ridge frequency and ridge orientation information along with minutiae position to improve the security.

Tams et al. [8] proposed minutiae based fuzzy vault scheme for template protection. In this method, absolute pre-alignment is employed to align the query with stored template. This alignment method does not leak any minutiae information and provides high security. Proposed method focus on the opportunity in implementing Pre-aligned minutiae based finger print template matching via fuzzy vault cryptosystem.

3 Fingerprint pre-alignment fuzzy vault cryptosystem

This section describes the functioning of the proposed minutiae based fuzzy vault system. Initially, the enrolled fingerprint image is preprocessed before extraction of features to reduce noise. All the minutiae points are extracted based on connected components after segmentation and thinning process. Core and delta points are identified and orientation fields are found using those core and delta points. The preprocessed fingerprint image is pre-aligned based on directed reference points and minutes are quantized. Euclidean distance is calculated and based on that value false minutiae points are removed.

Fuzzy vault is constructive for securing point-set based biometric features like fingerprint minutiae. The fuzzy vault system is a cryptographic method with a key to encode a polynomial function and the vault are generated for the enrolled pre-aligned fingerprint image. Additional chaff points are added randomly with extracted minutes to enhance the security of the template. Figure 2 demonstrates the framework of proposed fuzzy vault system. This system consists of five essential process namely preprocessing, prealignment and minutiae extraction, fuzzy vault and verification.

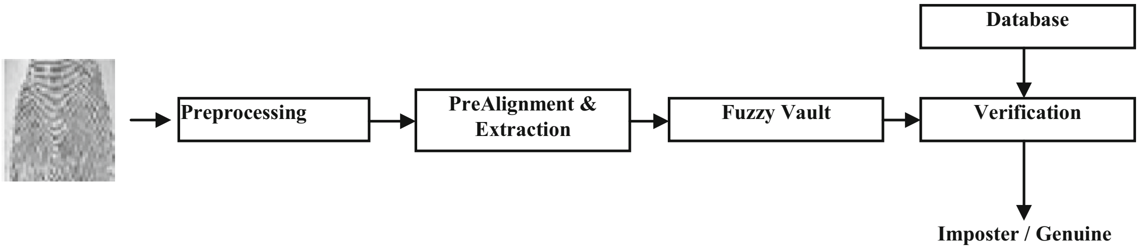


Fig. 2 Framework for proposed system

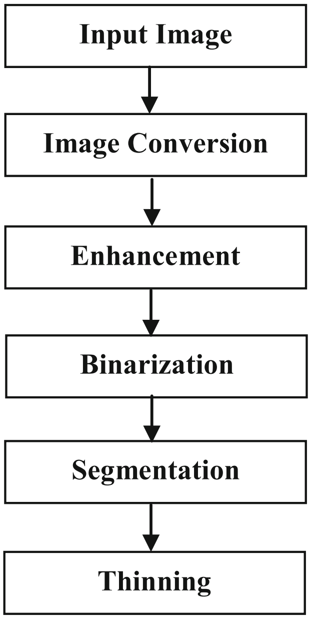


Fig. 3 Preprocessing

3.1 Preprocessing

Fuzzy vault system for fingerprint recognition proposed in this paper based on the core, ridges and bifurcations of the input image. Initially, each fingerprint was pre-processed individually regulate to improve the quality of an image and guarantee the reliability [23]. The various steps used for preprocessing an image are depicted in Fig. 3.

3.1.1 Image enhancement

Different types of fingerprint scanners are available in the market. Most of fingerprint scanners return 3D (color) images. For the implementation of the proposed system, the 3D images should be converted into 2D or gray scale images [23,24]. Let the 3D image represented by three components namely Red, green and blue, the gray scale conversion of a pixel is calculated using Eq. (1),

$$\mathrm{I} = \frac{\mathrm{Red} + \mathrm{Green} + \mathrm{Blue}}{3} \tag{1}$$

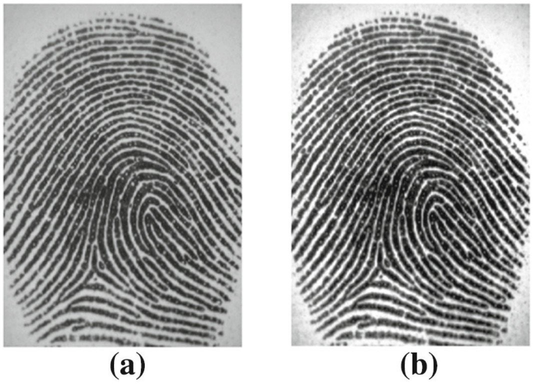


Fig. 4 **a** Original input image, **b** enhanced image

Histogram equalization techniques are employed to enhance the quality of the image. Generally, histogram equalization is used to improve the contrast of the input image by modifying pixel intensity value. Figure 4a and b shows the input image before and after histogram equalization and enhanced image.

3.1.2 Binarization

Binarization is the method of transforming gray scale image into binary image. There are many techniques are found in the literature [18,24,25] and [17] for image Binarization. Binarization process helps to improve the contrast between valleys and ridges in an image. In this work, Otsu thresholding is applied on the enhanced image to convert it into binary image. Figure 5a and b shows the input image and its binary version.

$$I_B[i,j] = \begin{cases} 1 & if\ X_{i,j} > t_{i,j} \\ 0 & if\ X_{i,j} < t_{i,j} \end{cases} \tag{2}$$

3.1.3 Segmentation

Segmentation is the process of eliminating unwanted edges of the fingerprint image. The objective of segmentation is to

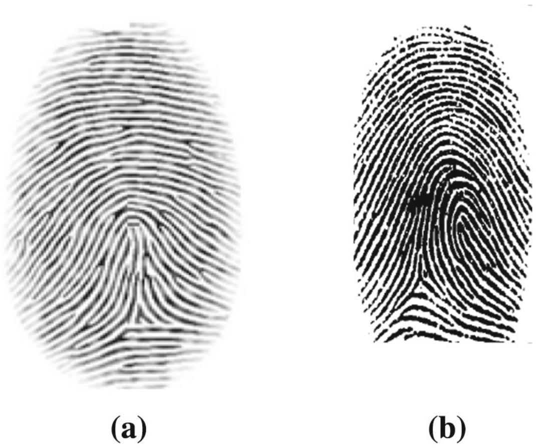


Fig. 5 **a** Original input image, **b** binarized image

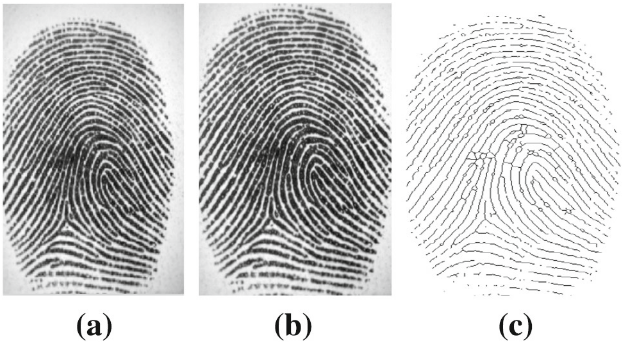


Fig. 6 **a** Input image, **b** segmented image, **c** thinned image

extract the region of interest (ROI). In this work, block direction estimation and some morphological operations proposed by Ravikumar et al. [11], Singh et al. [26], and Farah et al. [23] are employed to extract the ROI. Segmented results are shown in Fig. 6b.

3.1.4 Thinning

In thinning, the morphological operation of thinning is done to extract the fingerprint features and to eliminate the unnecessary noise. Figure 6c shows the thinning image.

3.2 Extraction and pre alignment

To extract the minutiae features from the preprocessed fingerprint image, crossing number (CN) method is used shown in Table 1. It is the popular and commonly used method. CN off a pixel in a binary image is the half the sum of the variation between pairs of neighboring pixels in the 8-neighborhood. The value of CN for pixel P is calculated using Eq. (3). Extracted Minutiae points are shown in Fig. 7a.

Table 1 Cross numbering method

P1	P2	P3
P8	P	P4
P7	P6	P5

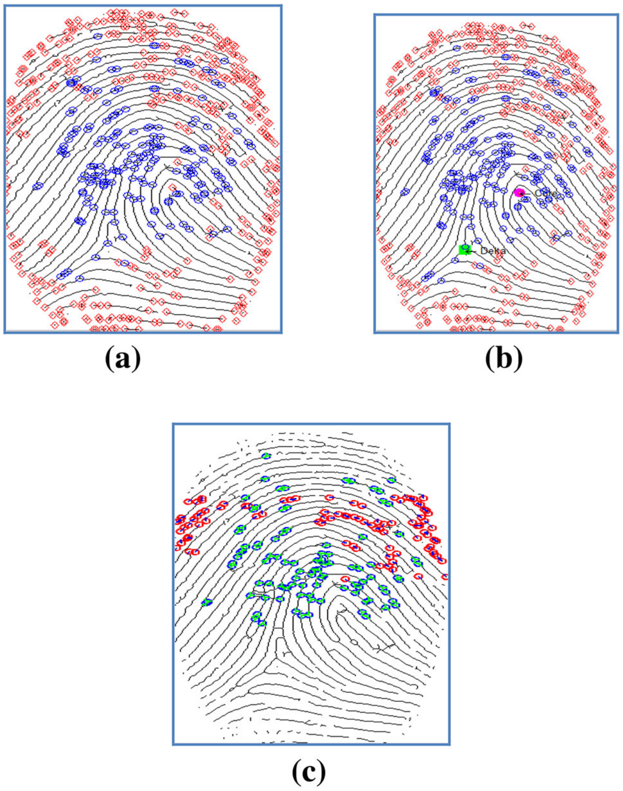


Fig. 7 **a** Minutiae extraction, **b** core and delta points, **c** minutiae points after false removal

Table 2 Crossing number properties

CN	Property
0	Isolated point
1	Ridge
2	Ridge point continues
3	Bifurcation
4	Crossing point

$$CN\left(P\right)=\frac{1}{2}\sum\nolimits_{j=1}^{8}\left|P_j-P_{j-1}\right|. \tag{3}$$

Table 2 lists the properties of CN. A ridge pixel with a CN of one represents the ridge ending and CN of three corresponds to bifurcation.

Extracted minutiae are represented by 3-tuple (x, y, θ), where x denotes the row index, y represents the column index and θ indicate the orientation angle of minutiae. The algorithm described in [8] adopted for minutiae alignment and

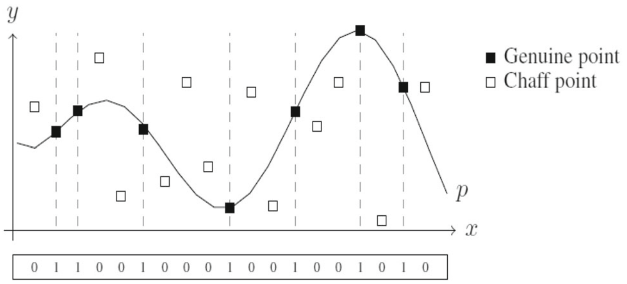


Fig. 8 Vault construction

quantization. Pre Alignment is performed based on (x, y, θ) value described in [8]. In this alignment method, reference point is constituted with direction. The reference point is used as system's origin and direction defines the axis. Core and delta points are identified (shown in Fig. 7b) and based on core and delta points orientation field are estimated. False minutiae's are detected and removed using Euclidean distance shown in Fig. 7c. Translation and rotation should be performed after estimation of orientation field. After pre alignment quantization is performed with pre aligned fingerprint [8].

3.3 Fuzzy vault system

Fuzzy vault is functional for securing point-set based biometric features such as fingerprint minutiae. The major important of the fuzzy vault system is to secure critical data with the fingerprint data. In this proposed work, develop the fuzzy fingerprint vault, (i.e.) fingerprint authentication using fuzzy vault scheme to secure fingerprint templates. Fuzzy vault has been worked with unordered sets (common in biometric templates, including fingerprint minutiae data), it is a promising candidate designed for crypto-biometric systems.

The major advantages of the fuzzy vault system is discussed as follows,

Fuzzy vault is secure in the sense that it cannot leak data about fingerprint characteristics information because it makes use of one-way hash function for encryption. It is capability to hold intra-class variations in biometric data. Different cryptography, it may permit a match to occur if the difference among the query biometric data and the template is small. The fuzzy vault scheme stores only a transformed version of the template, which makes it applicable to several modalities besides fingerprints.

Fuzzy vault constructions is shown in Fig. 8.

The proposed minutiae based fuzzy vault system uses Galois field (F = GF (2^{16})) for constructing fuzzy vault. Proposed minutiae based fuzzy vault system has three parameters such as M, C and S. M represents the number of minutiae extracted. C denotes the chaff points that are merged with the genuine points for constructing the vault. Security of fuzzy vault scheme is depending on the number of chaff points. As more number of chaff points added with the genuine points, vault security increases and vice versa. S represents the degree of polynomial. Fuzzy vault encoding and decoding (shown in Fig. 9) of fingerprint image is explained in the following,

1. Let the secret key $S = \{s\}_{i=1}^{n-1}$s used to find the polynomial P with order n.
2. x and y coordinates of minutiae are used to construct the vault (v = x/y)
3. Genuine points (G) and chaff points (C) are generated
4. Evaluate the polynomial P at all points in the selected minutiae in order to obtain P(v).

$$\begin{aligned} \mathrm{FV} &= \mathrm{GUC} \qquad (4)\\ \mathrm{G} &= [(\mathrm{v}_1, \mathrm{P}(\mathrm{v}_1)), (\mathrm{v}_2, \mathrm{P}(\mathrm{v}_2)), \ldots.(\mathrm{v}_\mathrm{m}, \mathrm{P}(\mathrm{v}_\mathrm{m}))]\\ \mathrm{C} &= [(\mathrm{r}_1, \mathrm{s}_1), (\mathrm{r}_2, \mathrm{s}_2), \ldots.(\mathrm{r}_\mathrm{l}, \mathrm{s}_\mathrm{l})]\\ &\quad \mathrm{r}_\mathrm{k} \cdot \mathrm{v}_\mathrm{j} \text{ and } \mathrm{s}_\mathrm{k} \cdot \mathrm{P}(\mathrm{v}_\mathrm{j})\ [\mathrm{k} = 1, 2, \ldots \mathrm{l}, \mathrm{j} = 1, 2, \ldots.\mathrm{m}] \end{aligned}$$

where, v denotes the genuine points, P (v) represents the projection of genuine point, r is the chaff point, m is the number of genuine points, l is the number of chaff points and s is the dummy value.

3.3.1 Vault decoding

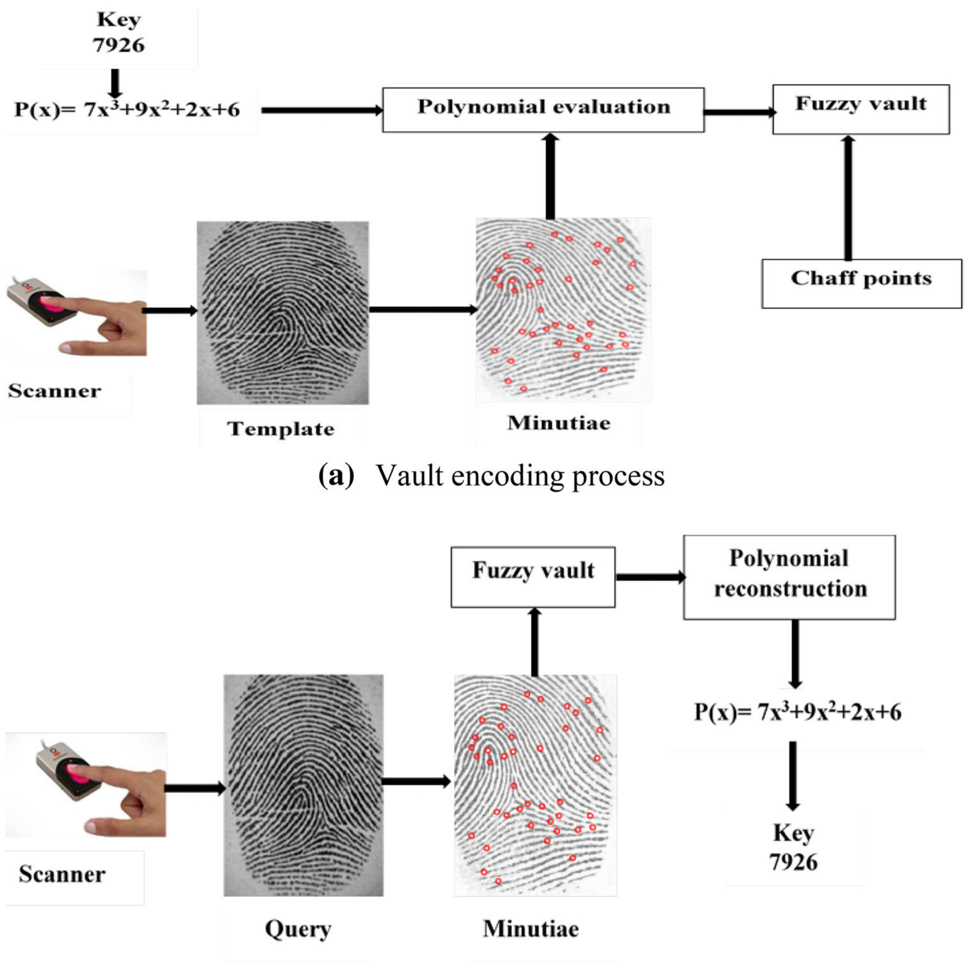
Vault decoding process is used to reconstruct the polynomial and recover the secret key S.

1. Query minutiae points are compared with the stored fuzzy vault.
2. Genuine points are separated and polynomial is reconstructed
3. Coefficients are mapped to obtain the secret key S.

3.4 Verification

The vault can be reconstructed and the secret key can be regained only when there is adequate contest between the query image and the enrolled input image. The vault decoding is performed during verification and extracts the minutiae points from the query fingerprint template Q. The points form an unordered set B. Compute the polynomial projections; P(X), for the elements of set B. Compare the points of the input sets in the vault and the query template. If the sets overlap substantially then the vault is unlocked and the key (S^*) is retrieved by the user. Finally, matching between is processed with the query image and stored image based on key value ($S^* = S$). If $S = S^*$ means the query and input image is same and input is genuine otherwise imposter.

Fig. 9 Framework of fuzzy vault system. **a** vault encoding, **b** vault decoding process



(a) Vault encoding process

(b) Vault decoding process

4 Simulation results and discussions

This section presents the simulation parameters are used for implementation. It also analyses the brute force attack and correlation attack to prove the security of the proposed system.

In biometrics system there are several numbers of attacks are presented. But in the attacks against secure template majorly reduces the security of biometric system.

Some of the template based attacks are brute force, known key attack, substitution attack, correlation attack, decidability attack, doppelganger attack and hill climbing attack. Among these attacks brute force and correlation attacks are mostly occurred in all templates. So in this work brute force attack and correlation attack are detected prove the security of the proposed system

- Brute force-attacker tries each likely bit combination till they estimate the correct original feature data or key.
- Correlation attack-from a cryptanalysis point of view, a good stream cipher should be resistant against a known-plaintext attack. In a known-plaintext attack the cryptanalyst is given a plaintext and the corresponding cipher text, and the task is to determine a key K. For a synchronous stream cipher, this is equivalent to the problem of finding the key K that produces a given key stream $z_1, z_2, \ldots, z_N$.

Table 3 Simulation parameters used for implementation

Number of genuine points, G	40
Number of chaff points, C	400
Total points, T	440
Degree of polynomial, k	8–12

4.1 Performance evaluation

The performance of the proposed fingerprint fuzzy vault system has been tested on FVC2002-DB2 [27] for varying k = 8… 10. Matlab is used for implementation of fingerprint authentication. Table 3 lists the simulation parameters used

Table 4 Performance of minutiae based fuzzy vault system

Degree	GAR (%)	FAR (%)
8	89	0.72
9	84	0.51
10	83	0.04
11	78	0.01
12	75	0.01

Table 5 Performance comparison

Method	GAR (%)	Brute force attack	Correlation attack
Nandakumar et al. [7]	86	Weak brute force security	Present
Li et al. [28]	92	No	Present
Tam et al. [8]	79	No	No
Proposed	82	No	No

for implementation. The goal of adding chaff points with the genuine data is to improve the security of template. The chaff points added is 10 times more in number than that of the genuine points. Performance of proposed fuzzy vault method is evaluated using genuine acceptance rate (GAR) and false acceptance rate (FAR). Only two impressions of each person used for implementation, one for enrollment and other for query. Table 4 shows the GAR and FAR of the proposed method.

Table 5 compares the performance of the proposed minutiae based fuzzy vault with the existing methods presented in [7,8] and [28]. From the Tables 4 and 5, it is observed that the proposed system performed well compared to existing methods.

4.2 Brute force attack

The security analysis of minutiae based fuzzy vault system is shown in Table 6. It is observed from the table that the security of fuzzy vault depends on the degree of polynomial. Polynomial degree with smaller degree can be can be reconstructed easily by the attacker. Performance of the proposed fuzzy vault is compared with the existing method [29,30]. Table 6 represents the comparison of proposed minutiae based fuzzy vault with the existing method at degree of polynomial 8. From both the table, it is evident that the proposed minutiae based fuzzy vault proves better than the other methods considered for comparison from the existing methods available in the literature (Table 7).

Polynomial with higher degree provides high security. It is difficult to reconstruct the polynomial. Fuzzy vault with k degree, for brute force, the attacker has to try (T, k + 1) combinations of k + 1 element each. Number of combinations are needed to decode the fuzzy vault is (G, k + 1) therefore, for an attacker to decode the vault by brute force attack, it takes C (T, k + 1)/C (G, k + 1) evaluations. Experimental results shown in that the fuzzy vaults offer the potential to provide high security for the biometric template. Performance of the proposed fuzzy vault is compared with the existing method [8,30].

4.2.1 Correlation attack

Correlation attack is a type of attack via record multiplicity [30]. In correlation attack the attacker interrupts at least minimum two vaults belong to one person. The vaults may be generated by two different ways: (i) fuzzy vault created using same genuine points with different secret key (ii) same minutiae points with different chaff points. Let the attacker intercepts two vaults protecting two set of minutiae {n} and {n'}. The aim of an attacker is to find the 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 consists of fuzzy vault pairs that belong to {n} with distance(n, T(n'))<= Th. The attacker can use RS decoder to crack the vault when the matching pairs of (n, n') are lesser than non-matching pairs. Suppose {n} and {n'} are equal in size, for each genuine and chaff points of {n} there exist a genuine and chaff points of {n'}. To resist the correlation attack, minutiae features are quantized using the method described in [8]. This quantization process proves that the proposed system resistance against correlation attack.

Table 6 Brute force attack

Degree of polynomial	Total combinations tried to decode the vault	Number of combinations required	Total evaluations
8	1.5687×10^{18}	2.7343×10^{8}	5.7371×10^{9}
9	6.7611×10^{19}	8.4766×10^{8}	7.9761×10^{10}
10	2.6430×10^{21}	2.3118×10^{9}	1.1432×10^{12}
11	9.4488×10^{22}	5.5868×10^{9}	1.6912×10^{13}
12	3.1110×10^{24}	1.2033×10^{10}	2.5853×10^{14}

Table 7 Evaluation of proposed system

Method	Brute force attack					Correlation Attack
	Degree of polynomial	No of genuine points	Total combinations tried to decode the vault	Number of combinations required	Total evaluations	Present
Meenakshi et al. [30]	8	30	1.1457×10^{17}	1.4307×10^{7}	8.0079×10^{9}	Not considered
Proposed	8	40	1.5687×10^{18}	2.7343×10^{8}	5.7371×10^{9}	Removed

5 Conclusion and future enhancement

In this paper, prealigned minutiae based fuzzy vault system for finer image is presented. During enrollment, input fingerprint images are preprocessed to improve the quality of an image. Minutiae are extracted using crossing number and using Euclidean distance false minutiae's are removed. Minutiae are pre aligned, quantized to reduce complexity. Fuzzy vault is constructed using quantized minutiae and secret key. In verification, query minutiae are matched with the vault to extract the key. Performance of the proposed system is analyzed using FVC 2002 database. Furthermore, security analyses of the system are also done. Experimental results demonstrate that the proposed minutiae based fuzzy system resistant against brute force attack and correlation attack.

In future work new algorithm is introduced that addresses inconsistency of feature representations, ordering of features, and the need for localization must be systematically investigated for all biometric modalities such as face, iris, etc to achieve security, cancellability, and privacy. Also in future, multibiometric fuzzy vault is implemented to reduce other attacks and it produces high security.

References

1. Liu, H., Sun, D., Xiong, K., Zhengding, Q.: Palm print based multidimensional fuzzy vault scheme. Sci. World J. **2014**, 8 (2014)
2. Arakala, A., Jeffers, J., Horadam, K.J.: Fuzzy Extractors for Minutiae-based Fingerprint Authentication. In: Lee, S.W., Li, S.Z. (eds.) Advances in Biometrics. ICB 2007. Lecture Notes in Computer Science. Springer, Berlin (2007)
3. Juels, A., Sudan, M.: A fuzzy vault scheme. In: Proceedings of the IEEE International Symposium on Information Theory, pp. 408 (2002)
4. Juels, A., Wattenberg, M.: Fuzzy commitment scheme. In: Proceedings of the ACM Conference on Computer and Communications Security (ACMCCS '99), pp. 28–36 (1999)
5. Sapkal, S., Deshmukh, R.: Biometric template protection with fuzzy vault and fuzzy commitment. In: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, ACM, pp. 1–6. https://doi.org/10.1145/2905055.2905118 (2016)
6. Hidano, S., Tetsushi, O., Takahashi, K.: Evaluation of security for biometric guessing attacks in biometric cryptosystem using fuzzy commitment scheme. In: Proceedings of the International Conference of the Biometrics Compendium, Darmstadt, Germany. pp. 1–6 (2012)
7. Nandakumar, K., Jain, A.K., Pankanti, S.: Fingerprint based fuzzy vault: implementation and performance. IEEE Trans. Inf. Forensics Secur. **2**(4), 744–757 (2007)
8. Tam, B., Mihăilescu, P., Munk, A.: Security considerations in minutiae-based fuzzy vaults. IEEE Trans. Inf. Forensics Secur. **10**(5), 985–998 (2015)
9. Wang, Y., Plataniotis, K.N.: Fuzzy vault for face based cryptographic key generation. In: Proceedings of the Biometrics Symposium (BSYM '07), (2007)
10. Lee, Y.J., Park, K.R., Lee, S.J., Bae, K., Kim, J.: A new method for generating an invariant iris private key based on the fuzzy vault system. IEEE Trans. Syst. Man Cybern. B **38**(5), 1302–1313 (2008)
11. Kumar, L.R., Kumar, S.S., Prasad, J.R., et al.: Fingerprint minutia match using bifurcation technique. Int. J. Comput. Sci. Commun. Netw. **2**(4), 478–486 (2012)
12. Bhowmik, P., Bhowmik, K., Azam, M.N., Rony, M.W.: Fingerprint image enhancement and its feature extraction for recognition. Int. J. Sci. Technol. Res. **1**(5), 117–121 (2012)
13. Joshua, A., Kwan, P., Gao, J.: Fingerprint Matching Using a Hybrid Shape and Orientation Descriptor. In: Jucheng, Y. (ed.) State of the Art in Biometrics. InTech, London (2011)
14. Hatano, T., Adachi, T., Shigematsu, S., Morimura, H., Onishi, S., Okazaki, Y., Kyuragi, H.: A fingerprint verification algorithm using the differential matching rate. In: Proceedings of the 16th International Conference on Pattern Recognition (2002)
15. Lindoso, A., Entrena, L., Liu Jimenez, J., San Millan, E.: Correlation-based fingerprint matching with orientation field alignment. In: Proceedings of the International conference on Biometrics, pp. 713–721 (2007)
16. Jain, A.K., Nandakumar, K., Nagar, A.: Biometric template security. EURASIP J. Adv. Signal Process. **2008**, 17 (2008). Article ID579416
17. Chopra, J., Upadhyay, D.P.: Various fingerprint enhancements and matching technique. Int. J. Electron. Commun. Eng. **5**(3), 279–289 (2012)
18. Tams, B.: Absolute fingerprint pre-alignment in minutiae-based cryptosystems. In: Proceedings of the of BIOSIG, pp. 75–86 (2013)
19. Hanoon, M.F.: Contrast fingerprint enhancement based on histogram equalization followed by bit reduction of vector quantization. Int. J. Comput. Sci. Netw. Secur. **11**(5), 116–123 (2011)
20. Barnouti, N.H.: Fingerprint recognition improvement using histogram equalization and compression methods. Int. J. Eng. Res. Gener. Sci. **4**(2), 685–692 (2016)
21. Uludag, U., Jain, A.K.: Securing fingerprint template: fuzzy vault with helper data. In: Proceedings of CVPR Workshop Privacy Research Vision, New York, pp. 163 (2006)
22. Nagar, A., Nandakumar, K., Jain, A.K.: Securing fingerprint template: fuzzy vault with minutiae descriptors. In: Proceedings of the International Conference for Pattern Recognition, Tampa, pp. 1–4 (2008)

23. Tatar, F., Machhout, M.: Improvement of the fingerprint recognition process. Int. J. Bioinform. Biosci. **7**(2), 1–16 (2017)
24. http://www.biometric-solutions.com/fingerprint-recognition.html
25. Carneiro, R.F.L., Bessa, J.A., de Moraes, J.L., et al.: Techniques of binarization, thinning and feature extraction applied to a fingerprint system. Int. J. Comput. Appl. **103**(10), 1–8 (2014)
26. Singh, R., Shah, U., Gupta, V.: Fingerprint recognition. Student project, Department of Computer Science and Engineering, Indian Institute of Technology, Kanpur, India (2009)
27. Maio, D., Maltoni, D., Cappelli, R., Wayman, J., Jain, A.: FVC2002: second fingerprint verification competition. In: Proceedings of the International Conference on Pattern Recognition, pp. 811–814 (2002)
28. Li, P., Yang, X., Cao, K., Tao, X., Wang, R., Tian, J.: An alignment free fingerprint cryptosystem based on fuzzy vault scheme. J. Netw. Comput. Appl. **33**, 207–220 (2010)
29. Meenakshia, V.S., Padmavathi, G.: Security analysis of password hardened multimodal biometric fuzzy vault. Int. J. Comput. Elect. Autom. Control Inf. Eng. **56**, 312–320 (2009)
30. Meenakshia, V.S., 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. Comput. Sci. **2**, 195–206 (2010)

D. Chitra is working as a Professor and Head in the department of CSE, P. A. College of Engineering and Technology. She received her Doctor of Philosophy from Anna University, Chennai and Master's Degree in Computer Science and Engineering. Her areas of interest include Digital Image Processing, Pattern Recognition, Computer Vision, Data Mining and Grid & Cloud Computing. She has 17 years of experience in teaching and published 70 papers in National and International Conferences and Journals. She is a member of IEEE, ISTE, CSI, IAENG and IRED. She has guided 67 projects in both UG and PG, and currently nine research scholars pursuing Ph.D. She is a reviewer for many Journals and Conferences. She attended 25 national and International seminars/conferences/workshops. She has received awards such as Best Circuit Faculty Award SIAA (ASDF), Shri. P. K. Das Best Faculty Award, Best Faculty Award in Kongu Engineering College and Best Faculty Award in P. A. College of Engineering and Technology. She also organized 21 programmes sponsored by AICTE, Anna University, CSIR, DRDO, ICMR, and INSA.

V. Sujitha is working as an Assistant Professor in department of CSE, P. A. college of Engineering and Technology, Pollachi. She is pursuing her doctorate in Anna University Chennai and obtained her M.E. in Computer and Communication Engineering. She published nearly eight papers in International and national Conferences and Journals. She has Guided eight projects in both under graduate and post graduate students for their project work. She has 7 years of teaching experience and one year of industry experience. She has membership in ISTE, IAENG and ISRD. Her area of interest is Biometrics, Image Processing and Cryptography.