Polynomial Based Fuzzy Vault Technique for Template Security in Fingerprint Biometrics

Reza Mehmood and Arvind Selwal
Department of Computer Science and Information Technology, Central University of Jammu, India

Abstract: *In recent years the security breaches and fraud transactions are increasing day by day. So there is a necessity for highly secure authentication technologies. The security of an authentication system can be strengthened by using Biometric system rather than the traditional method of authentication like Identity Cards (ID) and password which can be stolen easily. A biometric system works on biometric traits and fingerprint has the maximum share in market for providing biometric authentication as it is reliable, consistent and easy to capture. Although the biometric system is used to provide security to many applications but it is susceptible to different types of assaults too. Among all the modules of the biometric system which needs security, biometric template protection has received great consideration in the past years from the research community due to sensitivity of the biometric data stored in the form of template. A number of methods have been devised for providing template protection. Fuzzy vault is one of the cryptosystem based method of template security. The aim of fuzzy vault technique is to protect the precarious data with the biometric template in a way that only certified user can access the secret by providing valid biometric. In this paper, a modified version of fuzzy vault is presented to increase the level of security to the template and the secret key. The polynomial whose coefficients represent the key is transformed using an integral operator to hide the key where the key can no longer be derived if the polynomial is known to the attacker. The proposed fuzzy vault scheme also prevents the system from stolen key inversion attack. The results are achieved in terms of False Accept Rate (FAR), False Reject Rate (FRR), Genuine Acceptance Rate (GAR) by varying the degree of polynomial and number of biometric samples. It was calculated that for 40 users GAR was found to be 92%, 90%, 85% for degree of polynomial to be 3, 4 and 5 respectively. It was observed that increasing the degree of polynomial decreased the FAR rate, thus increasing the security.*

Keywords: *Biometrics, Fingerprint, Template Security, Crypto-System, Fuzzy vault.*

Received August 2, 2019; accepted January 6, 2020
https://doi.org/10.34028/iajit/17/6/11

1. Introduction

Biometrics is the efficient way of identifying an individual from its physical and behavioural characteristics. A Biometric System uses special biometric traits having some unique characteristics like permanence, universality, collectability etc. for recognition. The Biometric traits used to identify an individual can be a fingerprint, face, Iris, Gait Recognition etc., Fingerprint is one of the most extensively used biometric traits in a biometric system. The features used by most of fingerprint systems are generally called minutia which is the representation of a fingerprint having bifurcation, termination or other. The accuracy of a biometric system can be identified by its possibility of accepting the genuine users and rejecting the imposters. The proportion of imposters that the biometric system will incorrectly accept is demarcated as the False Accept Rate (FAR) of that system and the proportion of genuine users that a system will incorrectly reject is the False Reject Rate (FRR). The total number of genuine users accepted by the system is defined as Genuine Acceptance Rate (GAR). Equal Error Rate (EER) is a point on the graph where FAR equals FRR [13]. Although biometrics is used to provide security to many applications, it is itself vulnerable to attack. The attacker can get hold of the template stored in the database and launch various kinds of attacks to the biometric system like replay attack, substitution attack to attain illegal access to the system. To avoid such kind of attacks various template security schemes have been devised. Jain *et al*. [13] and Jain *et al*. [14], describes various security issues that can be encountered after storing the template. The existing template security schemes have been broadly categorized into two classes, namely the Feature transformation approach and Biometric cryptosystem [19]. In the feature transform approach, a function known as transformation function (f) is applied on the biometric template along with a secret key (k) and the converted template is stored in the database. Biometric cryptosystem involves generating a cryptographic key and using that key for encryption of the template [16]. Feature transformation scheme can be further classified into two approaches: Salting (Bio-hashing)

and Non-invertible transforms (robust hashing). biometric cryptosystem is categorized into key binding (Fuzzy vault and Fuzzy commitment) and Key generation approach (secure sketch fuzzy extractor) [12]. Among these techniques Fuzzy vault scheme is one of the most widely held cryptosystem based technique that combines biometrics with cryptography. Selwal *et al*. [34], proposed a novel method called Octet Indexing method to secure and reduce the storage space of the template database. Dang *et al*. [9], anticipated a locality sensitive hashing based on ranking called the Index of Max (IoM) hashing for template protection. In the presented scheme biometric feature vector is converted into a discrete max ranked hash code. Gomez-barrero *et al*. [11] proposed a scheme to compare variable length data using Homographic encryption technique. Chin *et al*. [7], proposed a multi biometric system using fingerprint and palm print to protect the fused template using 3 stage hybrid feature transformation method. Jin *et al*. [15], proposed a method in which a revocable fingerprint template is generated by transforming a set of minutia into a bit string using polar grid base 3 tuple quantization technique. In literature numerous work has been done on feature transformation scheme while as biometric cryptosystem still needs some more attention. Bhatnagar *et al*. [4], presented a new secure watermarking technique to secure the template from attacks like rotation attack. In this paper, an enhanced version of cryptosystem based template security called fuzzy vault is presented. The capability to deal with unordered data and intra-class variation makes fuzzy vault a promising technique.

This paper is systematized in sections as follows: Section 2 describes the fuzzy vault scheme. Section 3 discusses a brief background on existing template security schemes especially the fuzzy vault. Section 4 provides the proposed fuzzy vault technique. Section 5 shows the experimental results of the enhanced technique. Section 6 discusses the security analysis and comparison of the proposed technique and finally the conclusion and future scope is given in section 7.

2. Fingerprint Fuzzy Vault Scheme

Fuzzy vault is a method of biometric crypto-system that is popular for providing security to the keys used in cryptography like Advanced Encryption Standard (AES) encryption technique has a key of 128, 192, 256 bits and the secrecy of these keys need to be maintained, so fuzzy vault can be a procedure to provide security to these cryptographic keys [36]. Fuzzy vault secures the template as well as the key by locking the template with the key and a legitimate user can only get access to the key if his template overlaps with the locked one. Fuzzy vault consists of two stages encrypting and cracking stage. In the encrypting stage, a person 'A' provides his fingerprint from which unordered feature set say (X) is obtained. A secret key is associated with his feature set that needs to be locked. The secret key is encrypted in the form of a polynomial whose coefficients represent the key. The feature vector X is projected over the polynomial to form a set of genuine points. Some points are generated randomly that do not coincide with the polynomial called the chaff points to increase security. The collection of genuine points and the chaff points forms the vault. In the decoding stage, person 'B' wants to unlock the secret key of A. User B presents his own feature set (Y) and can only unlock secret of A of his feature set Y overlaps largely with the feature set X of A [4]. The security of this technique depends on difficulty of polynomial regeneration. Figure 1 shows the general fuzzy vault scheme.

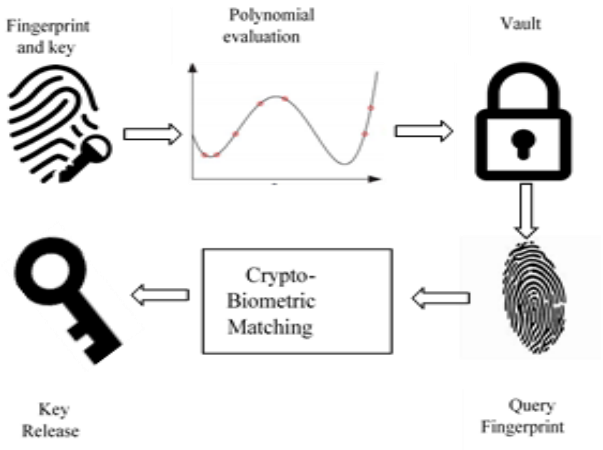


Figure 1. General cryptographic framework of fuzzy vault [29].

3. Related Literature

Panchal and Samanta [31] proposed a novel approach for storage security of biometric data or key. In this paper, a code-word is generated from the biometric feature which is in turn used to generate the key. User is authenticated using Support Vector Machine Ranking Mechanism (SVMRM). Barman *et al*. [2] proposed a new protocol for authentication using fingerprint based fuzzy-commitment scheme. They used three factors for their key agreement scheme which include user's password, smart card and personal biometric. The proposed scheme also shows resistance to various kinds of known attacks like man in the middle attack, denial of service attack etc., Kaur and Sofat [17] designed a multimodal biometric system where they fused traits of fingerprint and face using feature level fusion to provide protection to the template by means of fuzzy vault scheme. The ordered feature set is made compatible with the fuzzy vault by converting it to unordered feature set. The performance of the system is calculated on the basis of

FAR and FRR by varying the degree of the polynomial from the range of 8 to 14. Selwal *et al*. [35] portrayed four conceptual designs to enhance the inter-class variation of two modalities, a strong fingerprint biometric combined with the hand geometry trait. fuzzy based analytic hierarchy technique was employed to evaluate the proposed conceptual designs over five decision factors. Their results show that fusing fingerprint and hand geometry features using feature level fusion are most favourable with an overall ranking of 0.73438 and out of the five decision parameters, template security is found to be of supreme importance with a rating of 0.3940. Kaur and Sofat [18] designed a safe fuzzy vault scheme to protect the fingerprint vault from correlation attack by combining fuzzy vault scheme with Hadamard transformation technique. Fast Walsh Hadamard transformation is applied to the set of minutia point and the chaff points. The experimental results show that FAR is 2% and FRR is 11% after applying Hadamard transformation technique. Sarala *et al*. [33] projected a system in which they showed that the performance of a fuzzy vault system remains unchanged even after the blend substitution attack. They launched a blend substitution attack on the fuzzy vault system, designed a mechanism to detect this attack and provide corrective measures. The presented attack detection method consists of vault database connected to a server containing polynomial genuine points which checks for any change in the database continuously. The fuzzy vault is recovered back after the attack by substituting the compromised points with the genuine points in the server. The obtained average recognition rates are GAR of 86.1389% and FAR of 0.4039%. Amirthalingam and Radhamani [1] presented a new method for selection of chaff points in fuzzy vault in which grouped feature vector is generated and new chaff points are selected by taking the optimal location from the extracted feature vectors using particle swarm optimization algorithm. Leng and Teoh [20] proposed a new scheme in which a cancellable biometric technique called 2DPalmHash Code was combined with the fuzzy vault technique to provide better security to palm print templates. Lafkih *et al*. [19] investigated the vulnerabilities of the fuzzy vault scheme. The fuzzy vault scheme was tested practically with low resolution fingerprint and facial images of genuine users against the masquerade attack. The invader can get access to a fuzzy vault with 100% probability even if the alteration level of the images is high for face images, but for the fingerprint images the alteration level has to be low for the attacker to gain access. Dang *et al*. [8] combines two new components, chaff point generator and chaff point verifier into Fuzzy Vault Scheme that is capable of detecting any change in the Fuzzy Vault and thus protecting the template from blend substitution attack possible in cyclic redundancy check based fuzzy vault scheme. continuous hashing and linear projection are used to generate chaff points during enrolment. The experimental results show a 12% increase in GAR with main polynomial degree 8. Brindha [5] proposed a novel technique in fuzzy vault to protect the templates by extracting feature points from Finger Knuckle Print (FKP). The performance analysis is carried on hong kong polytechnic university FKP database for varying key sizes and studying the effect of adding salt and pepper noise. Feng *et al*. [10] have proposed a masquerade attack algorithm which is a combination of perceptron learning and hill climbing algorithm to create an artificial face image from the transformed binary template and stolen token. They have implemented their algorithm on two scenarios, when the binarization algorithm is known and when it is unknown. Prasad and Kumar [32] proposed a system in which they generated the fingerprint template by constructing M rectangles of different orientation angles around each reference minutia, then selected the minutia that fall in the rectangle, calculated the neighbouring relation that is applied on a plane to generate bit string which is converted into complex vector and transformed using user's pin. Moujahdi *et al*. [24] presented a new method for template protection to ensure revocability, diversity, security and better performance. They used the information extracted from the fingerprint minutia to construct special spiral curves and stored these curves in the database rather than the actual template. The matching is performed by applying similar procedure to query template and using Hausdorff distance to find the difference between the database template and the query template. Mihailescu [23] devised a new enrolment method to secure biometric template. The proposed scheme is based on a cryptographic method called hash chaos-based cryptography. A session key was generated using Rossler map and a pseudo random generator. The session key is then passed to the hash function that is used in the enrolment scheme. This scheme provides almost same computational security as that provided by davies-mays scheme. Nguyen *et al*. [30] proposed and implemented a novel algorithm for generation of chaff points in order to decrease the time complexity of the fuzzy vault scheme. In this paper, a novel method was employed where a fingerprint image was divided into cells and different points were generated randomly in those image cells. The point in the image cells can be chaff points only if it is unique and the difference between this point and the neighbouring points is larger or equal to the threshold. The experimental results show that the EER comes out to be 2.4% and 1.9% for FVC2002-DB1A and FVC2002-DB2A. Moon *et al*.

[25] gave three solutions to improve sanctuary of fingerprint fuzzy vault. Use of geometric hash table for aligning the fingerprint was suggested in this paper. Further the fuzzy vault proposed is resistant to correlation attack and uses one time template for each fingerprint. Liu *et al*. [22] presented a key binding system which considers only the n- nearest minutia points of fingerprint in the encrypted domain. Three levels of secure sketch is used namely, Shamir's secret, Pinsketch and wrap-around construction. Li *et al*. [21] developed a method which can avoid alignment procedure in fingerprint fuzzy vault by blending the local features, minutia descriptor and minutia local structure using three fusion strategies. Moreover Huffman coding is applied to reduce the storage volume of vault. Nandakumar and Jain [27] designed a fuzzy vault scheme in which the vault was constructed using fingerprint and iris to achieve better security to the different templates of a single user. Nandakumar *et al*. [28] proposed a scheme for increasing security of fingerprint fuzzy vault by using password. This scheme has resulted in reduction of FAR and prevented cross matching. Nandakumar *et al*. [29] implemented a fuzzy vault scheme that is an extension of the idea of Uludag *et al*. [36] which eliminated the need for Reed-Solomon polynomial decoding and fingerprint alignment. The analysis is performed on FVC-DB1 and MSU-DB1 fingerprint databases. Cappelli *et al*. [6] introduced an approach to reconstruct the fingerprint images from the original minutia template to study the success rate of masquerade attacks against eight fingerprint matching algorithms. This approach has shown that it is possible to generate fingerprint images which have ridge patterns very close to original fingerprint patterns and thus a successful masquerade attack can be performed with 72.8% of success rate at a high level of security and 83.9% at medium level of security. Uludag and Jain [37] presented the execution of the fingerprint fuzzy vault using helper data that was mined from the orientation field of fingerprint. The query fingerprint is aligned with the template on the basis of helper data using iterative closest point algorithm. Bansal *et al*. [3] proposed a novel technique of combining cryptosystem based technique with the non-invertible transformation technique to achieve revocability. They used Hadamard transformation to transform minutia points in enrolment and verification phase. GAR for 70 images was found out to be 82% and 77 % for FVC2002-DB1_B fingerprint database and live fingerprint database respectively.

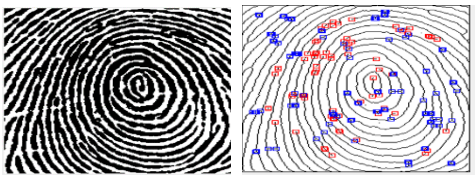
4. Proposed Fuzzy Vault Technique

The proposed work aims to fulfil the characteristics of an ideal template security scheme. The work has been carried out on the fingerprint as a biometric trait. An enhancement on the existing fuzzy vault technique has been employed in this paper. Key is of utmost importance in fuzzy vault scheme so its security is the prime concern. Key should not be visible to the attacker as he can gain an unauthorized access to the system. So, in this paper a polynomial transformation based method is employed in which the polynomial whose coefficients represent the key is further transformed using an integral function to maintain the secrecy of the key. Moreover, the integral function used increases the degree of the polynomial thus increasing the time complexity to regenerate the key back from the polynomial, thus making it difficult for the attacker to get the key. The whole procedure can be understood with the help of an example. Let's presume a user desires to secure a key k say '216' along with his fingerprint data represented by a set 'X={1,2,3}'. The system will generate a polynomial p(x) from the key to be preserved as 2x2+x+6, elements of key being the coefficients of the polynomial. Then to further preserve this polynomial an integral function '∫p(x)' is applied to the polynomial to transform it which then becomes '(2/3)x3+(1/2)x2+6x' to maintain its secrecy which in turn preserves the secrecy of key. Degree of the polynomial depends on the size of the key. The key of size n will generate a polynomial of degree n after transformation. Now the fingerprint set X is projected onto the polynomial to form the genuine minutia set as {(1, 7), (2, 19), (3, 40)}. Some randomly generated chaff points are also selected to form another set {(5, 12), (8, 13)} and the vault is formed from the combination of these two sets {(1, 7), (2, 19), (3, 40), (5, 12), (8, 13)}. Similarly decryption is done by comparing the abscissa value of vault points with the minutia set of new input. If there is the maximum match then the polynomial is reconstructed from the vault set. The transformed polynomial based fuzzy vault involves two stages: Locking and unlocking.

4.1. Locking Stage

The proposed technique of locking the fingerprint biometric template involves broadly three steps. Firstly, the minutia features are mined from the fingerprint and concatenated, then the polynomial is transformed using the integral function and finally the vault is constructed that locks the template and the key.

1. *Extraction of minutia points*: firstly a fingerprint is taken as an input and the fingerprint image goes through various enhancement processes like thinning, binarization etc. to increase its quality before extraction. After that the minutia points ridges and bifurcations are selected from a given modified image as shown in Figure 2:



a) Input Image. b) Minutia Points.

Figure 2. Extraction of minutia points from fingerprint.

2. *Polynomial transformation*: Taking the key as input a polynomial is generated to hide the key. The polynomial generated is transformed using integral function to maintain the secrecy of the polynomial itself and in turn the secrecy of the key.
3. *Creating the vault*: The minutia points are the projected onto the transformed polynomial to form a set of genuine minutia points. Vault is created from this set of genuine minutia points and the chaff points set selected randomly that do not coincide with the polynomial. The proposed technique of locking is shown in the form of a Figure 3:

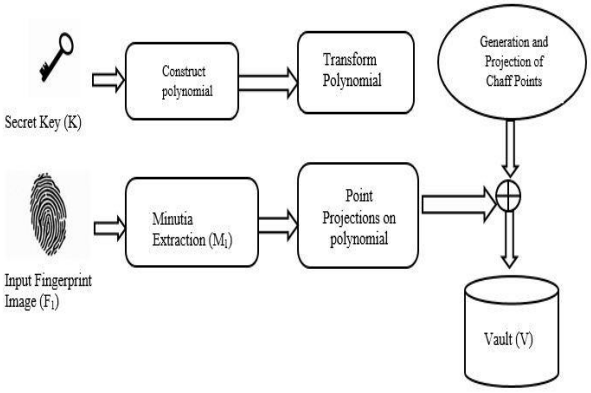


Figure 3. Constructing the vault in locking phase.

The algorithm for the proposed locking stage is given below:

Algorithm 1: Proposed Algorithm for Fuzzy vault encoding.

Input: Fingerprint F_I and key k
Output: Vault V
1. Start
2. for each fingerprint Image (F_I):
Extract genuine minutia points with coordinates (x_i, y_i)

$$M_i = (x_i, y_i)$$

3. Concatenate the x and y coordinates of the minutia points to get a single coordinate

$$X_i = x_i \mid y_i$$

4. Select a random secret key (k).
5. Divide secret key k into n+1 equal parts where n is the degree of polynomial and generate the polynomial P(X) of degree n.
6. Transform the polynomial (P(X)) by integrating it which reduces the degree to n-1.

$$P'(X) = \int P(X)$$

7. Compute Y_i projections from the concatenated minutia points X_i as

$$Y_i = P'(X_i)$$

to form a set of points as (X_i, Y_i).
8. Generate chaff points C_j which are δ distance apart from the given polynomial.

$$C_j = (x_c, y_c) \qquad 1<j<m$$

where m is the number of chaff points to be generated.
9. Project the chaff points on the given polynomial to get $P'(C_j)$ to form a set (C_j, $P(C_j)$).
10. Combine the set of genuine minutia points with the set of chaff points to form the fuzzy vault

$V = (S_i \cup T_i)$ *where* $Si \in (X_i, Yi)$ *and* $T_i \in (Cj, P'(Cj))$

11. Stop

4.2. Unlocking Stage

This is the stage for verification of the user where the query input image is taken and minutia features are taken out from it and compared to the vault generated in the locking stage. If most of the points of the vault match with the minutia features then those points are added to the list and a series of polynomial is generated from that list using langrage's interpolation. The coefficients of any one of the polynomial represent the key. The unlocking stage can be shown in Figure 4 below:

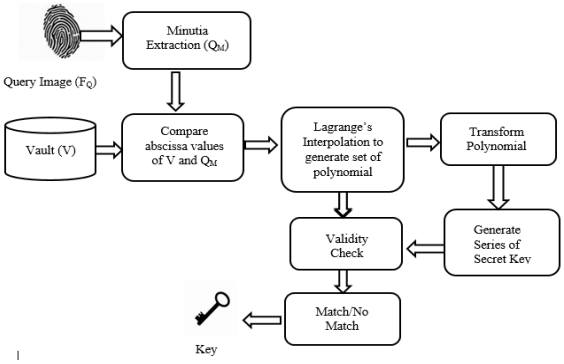


Figure 4. Generating key from the vault in Unlocking Phase The algorithm for unlocking phase is shown below.

Algorithm 2: Proposed algorithm for Fuzzy vault unlocking

Input: Vault V and Query fingerprint F_Q
Output: Key k
1. Start
2. for each query fingerprint image F_Q:
Extract the minutia points (x_i,y_i) from F_Q.
3. Concatenate the minutia points (x_i,yi) to form

$$Q_M = concat\ (xi, yi)$$

4. Compare abscissa values of Vault V with Q_M
Dis= compare ((X_i,Y_i),Q_M)
If (Dis<= Threshold)
Add (S_i,T_i) to vault FV
Else
Discard (S_i,T_i)
5. Generate a set of polynomial that satisfy the vault V using langrage's interpolation.
6. Differentiate the polynomial generated to get back the secret key.

7. *Concatenate the coefficients of the polynomial to generate a series of key.*
8. *If(key matches):*
   User authenticated
   Else:
   User rejected
9. *Stop*

5. Experimental Results

The exp rimental results were carried out using FVC2002-DB1, DB2, DB3, DB4 set B database. These databases were selected as they are the unrestricted databases easily available and the images are of relatively better quality. Each database has 80 imprints containing fingerprint images of 10 users, each user having 8 images. The description of these databases is given in the form of a Table 1.

Table 1. Description of FVC2002 database [26].

Database	No. of fingerprints	Images/finger	Image size	Sensor
DB1	10	8	388x374	Optical
DB2	10	8	296x560	Optical
DB3	10	8	300x300	Capacitive
DB4	10	8	288x384	SFINGE

The parameters used for computing performance of the given proposed scheme are FAR, FRR, GAR and EER. Number of imposter users being falsely accepted by the system to the total number of imposter tries gives the False Accept Rate and number of genuine users being falsely rejected by the system out of the total number of genuine attempts gives the False Reject Rate. Genuine accept rate is the number of positive genuine attempts. Equal error Rate shows the curve where FAR equals FRR. Identification Accuracy (IA) is the percentage of how accurate the system is to identify the genuine user and can be calculated as 1-[(FAR+FRR)/2]*100. The analysis at first was carried out using 10 users from DB1 database where every user has 8 imprints when the degree of polynomial (n) was set to 3. The user was enrolled using the first fingerprint image in the set then the rest of the images including the first image were taken as the query images to find various performance metrics. FAR came out to be 3% and FRR as 1% which is quite acceptable. Similarly the results were generated by increasing the number of users to 25 and 40 and also the degree of polynomial was changed to n=4 and n=5. The values of various performance metrics like FAR, FRR, GAR and Identification accuracy during the practical analysis are formulated in the form of table. During the analysis it was observed that as the degree of polynomial was increased, FAR declined but FRR amplified which is a trade-off. Since the system tends to improve the security so it won't let an imposter being accepted by the system thus decreasing the false accept rate. From this analysis we can conclude the more is the degree of polynomial the better the system would be. Table 2 shows the results of various parameters when degree of polynomial is 3. Similarly Table 3 shows the results when n=4 and finally Table 4 shows values for n=5.

Table 2. Experimental Results of the proposed scheme when n= 3.

No. of samples	FAR	FRR	GAR	IA
10	0.03	0.01	0.99	98%
25	0.04	0.05	0.95	95.5%
40	0.06	0.08	0.92	93%

Table 3. Experimental Results of the proposed scheme when n= 4.

No. of Samples	FAR	FRR	GAR	IA
10	0.01	0.04	0.96	97.5%
25	0.03	0.07	0.93	95%
40	0.05	0.1	0.90	92.5%

Table 4. Experimental Results of the proposed scheme when n= 5.

No. of Samples	FAR	FRR	GAR	IA
10	0.01	0.08	0.92	95.5%
25	0.017	0.12	0.88	93.15%
40	0.03	0.15	0.85	91%

To better understand the effect of degree of polynomial on the performance metrics of the system the results can be plotted in the form of graphs. The graphs plotted from the table give a better analysis of the security perspective of the system proposed. Figures 5, 6, and 7 gives the variation of FAR and FRR with the increase in the degree of polynomial. From the graph it could be seen that with the increase in degree of polynomial the system increases its capacity to reject the imposters as false accept rate decreases considerably. But for every Pro there is a Con. Increasing the degree could minimize the false accept rate but the system also rejected some of the genuine users due to increased complexity of verification of higher degree polynomial, thus increasing the FRR. Figure 8 gives the Receiver operating characteristic curve for varying degree of polynomial.

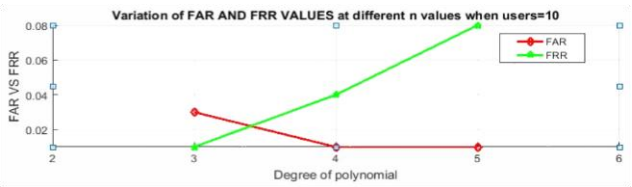


Figure 5. FAR and FRR at varying degree of polynomial when users=10.

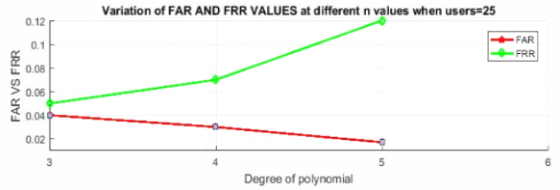


Figure 6. FAR and FRR at varying degree of polynomial when users=25.

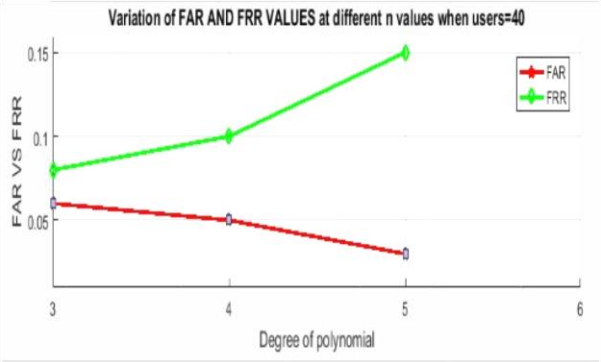


Figure 7. FAR and FRR at different degree of polynomial when users=40.

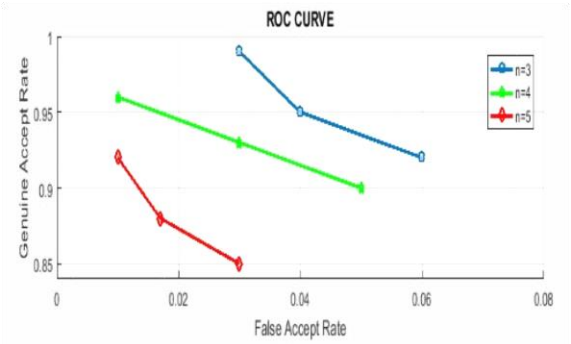


Figure 8. Receiver operating characteristic curve at varying degree of polynomial.

6. Security Analysis and Comparisons

Fuzzy vault scheme is a data securing cryptosystem based method that is used to protect the template. But a fuzzy vault scheme can face some of the issues in the practical scenario. It can encounter attacks like stolen key inversion attack and blend substitution attack from the attacker trying to steal the personal information. In stolen key inversion attack, if the invader by chance gets hold of the key entrenched in the vault, he can interpret the vault to acquire the biometric pattern. But in the proposed fuzzy vault scheme the key which is embedded in the vault is not the actual key but the transformed one. So, even though the invader gets hold of the key from the vault, he cannot get the biometric template of the user, thus preventing stolen key inversion attack. The proposed scheme has managed to improve the security and performance of the system but diversity and revocability are difficult to achieve in the fuzzy vault scheme as if the attacker gets access to two different vaults resulting from the biometric template of a single user, he can recognize the genuine points in two vaults by comparison and hence decrypt the vault. The proposed work can be compared to a few papers to determine the efficiency of the proposed method. The comparison results are shown in the form of a table below in Table 5.

Table 5. Comparison of proposed Technique to other similar methods.

S.No.	Technique	Author	Database	Performance Metrics
1.	Fuzzy vault with helper data	Nandakumar and Jain [27]	FVC2002-DB2	GAR= 91%, 91% AND 86% for n=7,8 and 10 respectively
2.	Fuzzy vault using Hadamard transformation	Bansal *et al.* [3]	FVC2002-DB1_B and live fingerprints	GAR= 82% and 77% for two databases
3.	Proposed Fuzzy Vault	Mehmood and Selwal	FVC2002-DB1,DB2,DB3,DB4	GAR= 92%,90%, 85% for n= 3, 4, and 5 resp.

7. Conclusions and Future Scope

The major concern in biometrics today is the security of the template of a biometric user. There are several techniques for template protection but it is hard to have an ideal scheme. In this paper, an enhanced fuzzy vault scheme has been presented with better security and increased performance. The proposed method uses a function to transform the polynomial in order to hide the key. The system achieves better GAR values at different degree of polynomial. For 40 users GAR was found to be 92%, 90%, 85% for degree of polynomial to be 3, 4 and 5 respectively. With increase in the degree of polynomial FAR was observed to get reduced with slight increase in the FRR values. The variation in the FAR and FRR values may be due to intra-user variation which affects the fingerprint alignment. Hence during comparing enough genuine points do not get extracted for polynomial regeneration. The proposed system also prevents the system from stolen key inversion attack. The proposed system improves the security of the system but fails to provide revocability. Thus there is the need to develop hybrid system by combining transformation approach like salting with the fuzzy vault scheme, thus providing advantages of both the techniques in single application.

References

[1] Amirthalingam G. and Radhamani G., "New Chaff Point Based Fuzzy Vault for Multimodal Biometric Cryptosystem using Particle Swarm Optimization," *Journal of King Saud University-Computer and Information Sciences*, vol. 28, no. 4, pp. 381-394, 2016.

[2] Barman S., Das A., Chattopadhyay S., Samanta D., Rodrigues J., and Park Y., "Provably Secure Multi-Server Authentication Protocol using Fuzzy Commitment," *IEEE Access*, vol. 6, pp. 38578-38594, 2018.

[3] Bansal D., Sofat S., and Kaur M., "Fingerprint Fuzzy Vault Using Hadamard Transformation," *in Proceedings of International Conference on Advances in Computing, Communications and*

Informatics, Kochi, pp. 1830-1834, 2015.

[4] Bhatnagar G., Wu Q., and Raman B., "Biometric Template Security Based on Watermarking," *Procedia Computer Science*, vol. 2, pp. 227-235, 2010.

[5] Brindha V., "Finger Knuckle Print As Unimodal Fuzzy Vault Implementation," *Procedia Computer Science*, vol. 47, pp. 205-213, 2015.

[6] Cappelli R., Lumini A., Maio D., and Maltoni D., "Evaluating Minutiae Template Vulnerability," *in Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies*, Alghero, pp. 174-179, 2007.

[7] Chin Y., Ong T., Teoh A., and Goh K., "Integrated Biometrics Template Protection Technique Based on Fingerprint and Palmprint Feature-Level Fusion," *Information Fusion*, vol. 18, no. 1, pp. 161-174, 2014.

[8] Dang T., Nguyen M., and Truong Q., "Chaff Point Generation Mechanism for Improving Fuzzy Vault Security," *The Institution of Engineering and Technology Biometrics*, vol. 5, pp. 147-153, 2015.

[9] Dang T., Huynh V., and Truong H., "A Hybrid Template Protection Approach using Secure Sketch and ANN for Strong Biometric Key Generation with Revocability Guarantee," *The International Arab Journal of Information Technology*, vol. 15, no. 2, pp. 331-340, 2018.

[10] Feng Y., Lim M., and Yuen P., "Masquerade Attack on Transform-Based Binary-Template Protection Based on Perceptron Learning," *Pattern Recognition*, vol. 47, no. 9, pp. 3019-3033, 2014.

[11] Gomez-barrero M., Galbally J., Morales A., and Fierrez J., "Privacy-Preserving Comparison of Variable-Length Data with Application to Biometric Template Protection," *IEEE Access*, vol. 5, pp. 8606-8619, 2017.

[12] Jain A., Ross A., and Uludag U., "Biometric Template Security : Challenges and Solutions," *Secure Watermarking Multimedia*, vol. 4675, no. 4, pp. 629-640, 2002.

[13] Jain A., Ross A., and Nandakumar K., Introduction to Biometrics, *Springer Lik*, 2011.

[14] Jain A., Nandakumar K., and Nagar A., "Biometric Template Security," *EURASIP Journal on Advances in Signal Processing*, pp. 1-17, 2008.

[15] Jin Z., Teoh A., Ong T., and Tee C., "Fingerprint Template Protection with Minutiae-Based BitString for Security and Privacy Preserving," *Expert Systems with Applications*, vol. 39, no. 6, pp. 6157-6167, 2012.

[16] Juels A. and Sudan M., "A Fuzzy Vault Scheme," *in Proceedings of IEEE International Symposium on Information Theory*, Lausanne, pp. 408, 2002.

[17] Kaur M. and Sofat S., "Fuzzy Vault Template Protection For Multimodal Biometricsystem," *in Proceedings of International Conference on Computing, Communication and Automation*, Greater Noida, pp. 1131-1135, 2017.

[18] Kaur M. and Sofat S., "Secure Fingerprint Fuzzy Vault using Hadamard Transformation to Defy Correlation Attack," *in Proceedings of 6th International Symposiumon Embedded Computing and System Design*, Patna, pp. 122-126, 2016.

[19] Lafkih M., Lacharme P., Rosenberger C., Mikram M., Ghouzali S., and Haziti M., "Vulnerabilities of Fuzzy Vault Schemes Using Biometric Data with Traces," *in Proceedings of IEEE International Wireless Communications and Mobile Computing Conference*, Dubrovnik, pp. 822-827, 2015.

[20] Leng L. and Teoh A., "Alignment-Free Row-Co-Occurrence Cancelable Palmprint Fuzzy Vault," *Pattern Recognition*, vol. 48, no. 7, pp. 2290-2303, 2015.

[21] Li P., Yang X., Cao K., Tao X., Wang R., and Tian J., "An Alignment-Free Fingerprint Cryptosystem Based on Fuzzy Vault Scheme," *Journal of Network and Computer Applications*, vol. 33, no. 3, pp. 207-220, 2010.

[22] Liu E., Zhao H., Liang J., Pang J., Xie M., Chen H., Li Y., Li P., and Tian J., "A Key Binding System Based on N-Nearest Minutiae Structure of Fingerprint," *Pattern Recognition Letters*, vol. 32, no. 5, pp. 666-675, 2011.

[23] Mihailescu M., "New Enrollment Scheme for Biometric Template Using Hash Chaos-Based Cryptography," *Procedia Engineering*, vol. 69, pp. 1459-1468, 2014.

[24] Moujahdi C., Bebis G., Ghouzali S., and Rziza M., "Fingerprint Shell: Secure Representation of Fingerprint Template," *Pattern Recognition Letters*, vol. 45, no. 1, pp. 189-196, 2014.

[25] Moon K., Moon D., Yoo J., and Cho H., "Biometrics Information Protection using Fuzzy Vault Scheme," *in Proceedings of Eighth International Conference on Signal Image Technology and Internet Based Systems*, Naples 2012.

[26] Maio D., Maltoni D., Cappelli R., Wayman J., and Jain A., "FVC2002: Second Fingerprint Verification Competition," *in Proceedings 16th International Conference on Pattern Recognition*, Québec City, pp. 811-814, 2002.

[27] Nandakumar K. and Jain A., "Multibiometric Template Security Using Fuzzy Vault," *in Proceedings of IEEE 2nd International*

Conference on Biometrics: Theory, Applications and Systems, Arlington, pp. 1-6, 2008.

[28] Nandakumar K., Nagar A., and Jain A., "Hardening Fingerprint Fuzzy Vault Using Password," *in Proceedings of International Conference on Biometrics*, Seoul, pp. 927-937, 2007.

[29] Nandakumar K., Pankanti S., and Jain A., "Fingerprint-Based Fuzzy Vault : Implementation and Performance," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 744-757, 2008.

[30] Nguyen T., Wang Y., Nguyen T., and Li R., "A Fingerprint Fuzzy Vault Scheme Using A Fast Chaff Point Generation Algorithm," *in Proceedings of IEEE International Conference on Signal Processing, Communication and Computin*g, KunMing, pp. 1-6, 2013.

[31] Panchal G. and Samanta D., "A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage," *Computers and Electrical Engineering*, vol. 69, pp. 461-478, 2018.

[32] Prasad M. and Kumar C., "Fingerprint Template Protection using Multiline Neighboring Relation," *Expert Systems with Application*s, vol. 41, no. 14, pp. 6114-6122, 2014.

[33] Sarala S., Karki M., and Yadav S., "Blended Substitution Attack Independent Fuzzy Vault for Fingerprint Template Security," *in Proceedings of International Conference on Circuits, Controls, Communication and Computing*, Bangalore, pp. 1-6, 2016.

[34] Selwal A., Gupta S., and Surender., "Low Overhead Octet Indexed Template Security Scheme for Multi-Modal Biometric System," *Journal of Intelligent and Fuzzy Systems*, vol. 32, no. 5, pp. 3325-3337, 2017.

[35] Selwal A., Gupta S., and Surender., "Fuzzy Analytic Hierarchy Process based Template Data Analysis of Multimodal Biometric Conceptual Designs," *Procedia Computer Science*, vol. 85, pp. 899-905, 2016.

[36] Uludag U., Pankanti S., and Jain A., "Fuzzy Vault for Fingerprints," *in Proceedings of International Conference on Audio and Video Based Biometric Person Authentication*, Rye Brook, pp. 310-319, 2005.

[37] Uludag U. and Jain A., "Securing Fingerprint Template : Fuzzy Vault with Helper Data," *in Proceedings of the Conference on Computer Vision and Pattern Recognition Workshop*, New York, pp. 163-163, 2006.

Reza Mehmood has completed her M. Tech in Computer Science and Technology from Central University of Jammu in 2019. Her area of interest includesBiometrics, MachineLearning, Pattern Recognition and Image Processing.

Arvind Selwal is presently working as Sr.Assistant Professor in the Department of Computer Science and Information Technology at Central University of Jammu, J&K,India. He has more than 14 years experience of teaching of UG and PG classes. He has successfully guided 12 M.Tech and one M.Phil students. His research interests include Machine Learning, Biometric Security, Image Processing and Advanced Database Systems. He has contributed more than 20 research articles in the International/National Journals indexed in reputed databases like Scopus and SCI, DBLP etc. He has authored a book on Fundamentals of Automata Theory and Computation