Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering pp. 89–92
DOI: 10.15439/2017R55
ACSIS, Vol. 10 ISSN 2300-5963

Authentication scheme using novel chaff generation method in fuzzy vault

Mahatim Singh[1], Rabi Shaw[2], Arpita Sarkar[3], Binod Kumar Singh[4]
Department of Computer Science & Engineering
NIT Jamshedpur
[1]mahatim221@gmail.com, [2]Shaw.rabi@gmail.com,[3]asarkar.cse@nitjsr.ac.in, [4]bksingh.cse@nitjsr.ac.in

Abstract: **Key Management is the critical issue of a cryptographic system and it requires a better security mechanism. Bio-cryptology provides a strong solution for the said critical issue. Fuzzy vault scheme is a popular scheme to design bio-cryptosystems. Key is secured with the biometric data mixed up with some noise points known as chaff points in a secure storage i.e. vault. Generation of chaff points is the important part of the fuzzy vault system. This work is mainly aims to present an authentication scheme (Key matching) with reducing the complexities of chaff generation. In chaff generation, circle packing, geometrical hashing etc. techniques are used to protect the real data from the noisy data, but these techniques are complex. Here a novel method of chaff generation is used where newly generated chaff point compared with genuine points (stored in a dataset) to assure that it is different, hence genuine points are protected. Experimental results shows that our method have less complexity and performs better than other existent methods.**

Keywords: ***Key management, cryptographic system, Bio-cryptology, fuzzy vault, chaff generation.***

I. INTRODUCTION

Now a day various services over the highly networked society require reliable means of personal authentication schemes. Preserving Integrity, Confidentiality and Availability of information is the major goals of the information security. There are different methods for user authentication, i.e. using password, smartcard or biometric traits based. For Information security various techniques like Cryptography Biometrics and Data hiding are used, but alone these solutions are not sufficient for the given issue. Mixing one technique with other gave a better solution in order to enhance the security level. Bio-cryptic system is one of those techniques where application of cryptography is mixed with biometrics. It provides better security for the critical issue of cryptography i.e. Key Management. Due to its good safety measures Biometric authentication is widely used as it provide better protection to avoid information theft and safety harassment [1]. Thus, for providing complete authentication mechanism or for securing the traditional cryptographic keys Biometrics-based authentication becomes an alternative of password-based authentication system in now a days. Biometric authentication systems also have many exploitable vulnerabilities, [8] especially in the networked infrastructure, like SQL injection attacks may cause a serious threat to the database. Hence combination of biometric property with cryptography may also have some exploitable vulnerability. We need to add some extra feature in it to enhance its architectural level security.

To design such bio-cryptosystem the application of a fuzzy vault scheme [7] is applied. For those applications where biometric based authentication and cryptography both are combined together fuzzy vault scheme is more suitable. As far as other practical cryptosystems is concerned where key management is the critical issue, fuzzy vault also overcomes this issue. Here in our work, this scheme is used to protect the key; key is mixed up with the user's biometric trait (fingerprint) and the generated chaff points [6]. Key from the user is encoded as the coefficients of a polynomial and mixed with the minutiae points extracted from the fingerprint and the generated chaff points. The generated chaff points are mixed with minutiae points which are used in user authentication to make it hard for an attacker to guess or extract the minutiae points. Combination of minutiae and chaff points make attacker harder to extract the polynomial coefficients i.e. the key. Bio-cryptosystems can include fingerprints, iris, face and palm-print. In fuzzy vault scheme the chaff generation module is the most computable heavy block. This module generates false minutiae points which is used to hide the genuine points from the attacker. A novel chaff generation method is used and compared with some existing chaff generation methods [4].

The remainder of this paper is organised as follows. In Section II Background work of the chaff generation is discussed. Section III deals the fuzzy vault scheme. In Section IV deals with our novel chaff point generation method. Experimental results are discussed in the Section V and Section VI concludes the paper.

II. BACKGROUND WORK

Our work focused on the authentication scheme and to propose a less complex chaff generation method. Fuzzy vault scheme is applied to secure the key that is used for the matching in order to process the authentication request of a user. In the fuzzy vault scheme different methods have been used to generate chaff points by different researchers. In [4] the concept of circle packing which is a theorem in geometrical mathematics is used. It is less computational heavy than the other existing methods. In [5] authors applied the geometric hashing to find geometric objects of the same or similar shape even though they may be rotated and/or translated. In [3] author proposed a method in which the fingerprint images are splits into the various segments which is known as image cells and each of these cells have eight adjacent image cells. There were two criteria for generation of a new chaff point: (i) points are just pixels with X-coordinate value not having similar X-coordinate value as the valid points and the existing chaff points, and (ii) The Y-coordinate value should not be equal to polynomial P(x).

Based on these approaches our novel method is proposed to reduce the complexities in the chaff generation process so that it takes less system execution time.

III. FUZZY VAULT SCHEME

Juels and Sudan proposed a scheme [9] termed as fuzzy vault. As discussed earlier fuzzy vault scheme aims to shield the important data like secret encryption key, with the help of biometric traits so that only the right user can access the secret by providing the valid biometric trait.

A. Encoding Phase

The encoding process of fuzzy vault is shown in the fig. 1.
In this phase the key from user is taken and mixed with user's own biometric trait i.e. his fingerprint in order to hide the key. The key and biometric traits are represented as points having coordinates values in a 2-D plane. Apart from these points some false points are added into the template to protect the genuine points.

The procedure is as follows:

1. A finite field size of order S lies on the quantised biometric features construct the fuzzy vault.
2. The secret key K (128 bits) is encoded and represented as the coefficients of an n^{th}-order polynomial P. For this CRC-32 function is used, which computes the CRC-32 checksum value of the data stored in a vector. Polynomial bit positions have been reversed, and the algorithm is modified to improve the performance. Fig 2 displays the polynomial coefficients in X-Y plain.

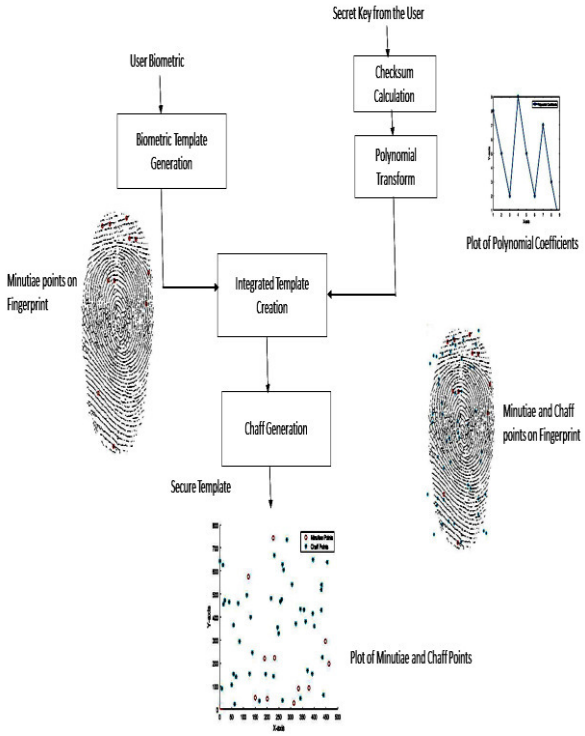

Fig 1: **Encoding Phase**

3. $M = \{m_i\}_{i=1}^{r}$, where $m_i \in Integers$ and r is the number of minutiae points is a user's fingerprint template. To obtain genuine points evaluations of P are computed on the elements of M, treating the elements of M as distinct x-coordinates. These points stored in a set. Initially a large number of minutiae will generate, a processing will require to extract useful minutiae. Based on the distance between a termination and a bifurcation and a threshold value number of minutiae can be adjust. If the distance between a termination and a bifurcation is smaller than the threshold value, those minutiae will be removed.
4. After getting the genuine points set some noise points (i.e. chaff points) will be added in it, in order to enhance the security level. Chaff points are also stored separately in a set.

The generated fuzzy vault template has the combination of valid and chaff points in x-y plain.

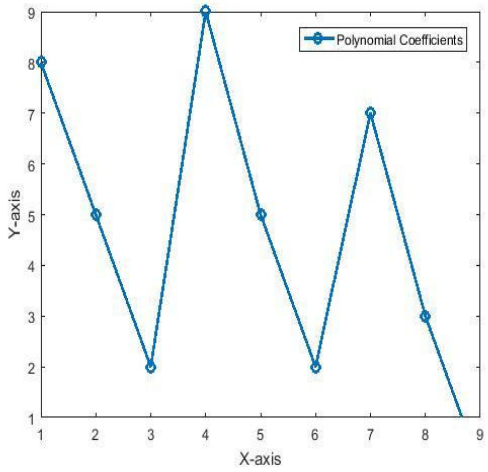

Fig 2: **Polynomial Coefficients**

B. Decoding Phase

Decoding of the fuzzy vault is shown in the figure 3, and its steps are described as follows

1. The user who needs validation or authentication will give his biometric trait (here fingerprint) and the secret key.
2. After getting the secret key again the key will be encoded as the coefficients of an n^{th}-order polynomial same as in encoding process and also generate required number of minutiae points (as in encoding phase) by user's taken biometric trait.
3. In Biometric Data Mapping process the new biometric feature is compared with the saved fuzzy vault members of the database. Those minutiae points which matched with the stored database minutiae points will be removed from the saved fuzzy vault member (temporarily for matching).
4. Load the saved chaff point set for that particular fuzzy vault member and remove chaff points from it to get the polynomial coefficients.
5. This polynomial coefficient is matched with the polynomial coefficients generated in step 2. If user is a registered person and given his right secret key, both the polynomial should produce same coefficients hence both two will get matched and user can be authenticated.

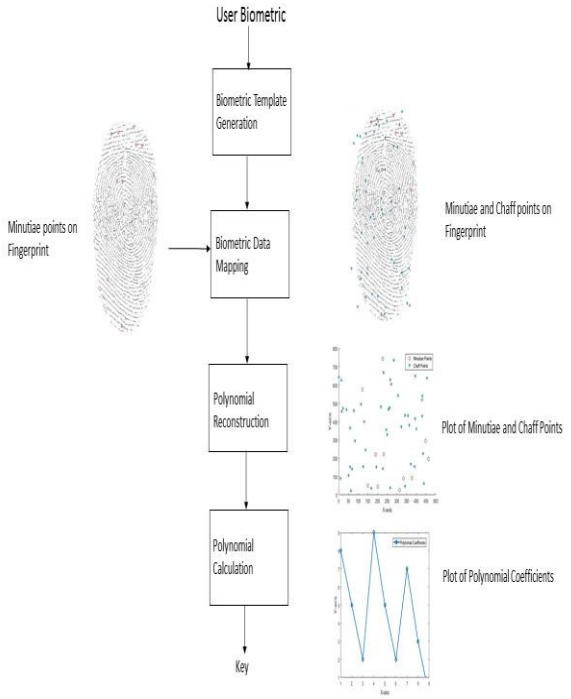

Fig. 3: **Decoding Phase**

IV. CHAFF GENERATION METHOD

To generate random noise or false points in the fuzzy vault encoding process, Chaff generation method is used. Chaff points generated and mixed with the real minutiae points and secret key to hide these points from the attacker, so it becomes very hard for an attacker to recognize the real points and the chaff points. These Chaff points are scattered over the fuzzy vault randomly and without any set pattern. Quantised biometric feature area should be taken into consideration while generating the chaff points and every chaff point should maintain a minimum distance with other chaff point. Clancy chaff generation algorithm [2] is very popular for this purpose.

A. Proposed Chaff Generation Algorithm

1. Calculate the feature area
FeatureArea (R) = del_X * del_Y;
Where, **del_X** = Xmax-Xmin and
del_Y = Ymax-Ymin
Xmax is maximum X-coordinate value for genuine points,
Xmin is minimum X-coordinate value for genuine points,
Ymax is maximum Y-coordinate value for genuine points and
Ymin is minimum Y-coordinate value for genuine points,

2. Generate random chaff point and insert with following conditions:

while(index < Number_of_chaff)
{
Generate Temporary random chaff_point;
Check_if(whether generated chaff points lie between R and does not belong to genuine points (stored in a data set))
{
Include chaff_pointff;
Increase the index;
}
else
ignore the Temporary chaff_point & continue;
}

Minimum number of iterations required to generate desired chaff points will be equals to number of chaff points we need.

V. RESULT OF THE PROPOSED CHAFF GENERATION ALGORITHM

Result of our chaff generation algorithm is shown in the following figures, Fig 4 and Fig 5. In the figures red dots are the minutiae points and blue points are the chaff points. Chaff points scattered all over the template region as allowed by the proposed Algorithm.

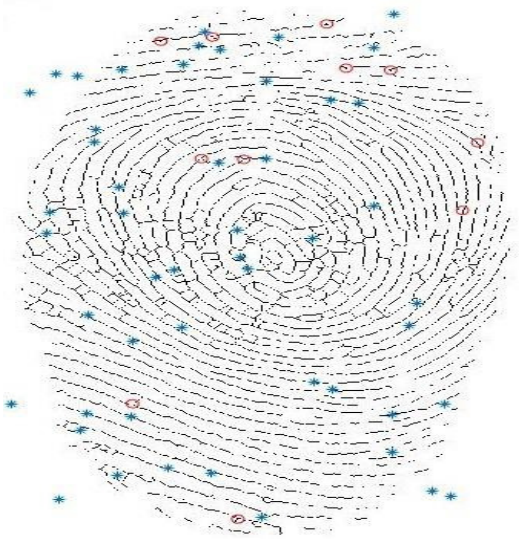

Fig 4: **Minutiae and chaff on fingerprint**

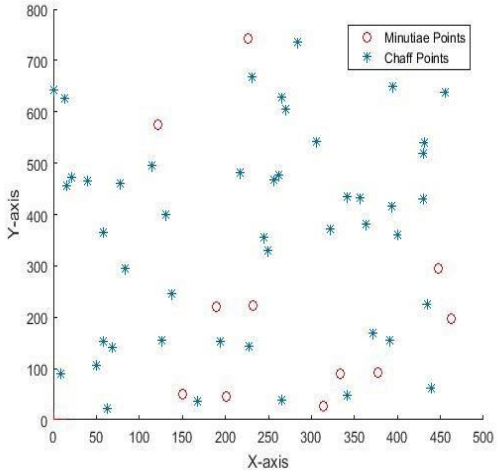

Fig. 5 **Minutiae and chaff on X-Y plain**

VI. RESULT AND ANALYSIS

Here secure key is taken from the user as an input and securing it by the means of bio-cryptic system. To generate polynomial coefficients CRC32 function is used. The CRC32 computes the CRC-32 checksum value of the data stored in the vector. The result is an unsigned 32-bit integer. Here the number of

polynomial coefficients is limited to 10, coefficients less than 10 allowed but not more than 10.

Performance of some chaff point generation methods are tabulated in the Table 1 with different number of minutiae and chaff points. Table 1 includes the Clancy method, a method published in a research paper [4] and our proposed method. The computation times of the Chaff point generation methods are recorded in the Table 1 for different cases based on the number of minutiae and chaff points. For the evaluation of performance gain, speed-up is calculated between our proposed method and referred method for each case. Table shows as the number of chaffs increased, the commutation time is also increased with a great margin. In our proposed method also system execution time increased as the chaff points increased, but the margin of increment is very less as compared to the referred method. Hence our method is getting a better performance gain as compared to other methods listed in the Table 1. The unit of the system execution time for each chaff generation method is taken in seconds.

Table 1. **Performance evaluation of chaff generation method**

Minutiae points	Chaff points	Clancy Method	Referred work method	Proposed Method	Speed-up with referred method
10	50	106.5	9.8	6.8	1.44
10	100	347.4	17.6	7.20	2.44
20	200	7098	50.4	7.80	6.46
30	400	17624	207.4	8.92	23.25
30	500	32697	310.0	9.47	32.73

Performance of the both proposed method and referred method are shown by the following plot. Following plot clearly displays how the system execution time increased with the increment in the chaff points.

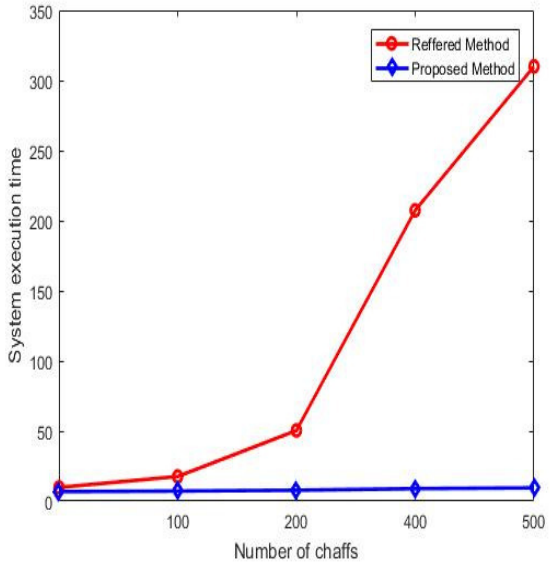

Fig 6. **Performance Analysis**

The above experiment is performed using MATLAB 2016 Software on a system with 64 bit Windows 10 Operating System, 4GB RAM, Intel Core i5-2430M Processor and CPU @ 2.40GHz.

VII. Conclusion

In this work as a Biometric feature fingerprint is taken to construct the fuzzy vault. Security level of the user's secret is increased by the addition of the Chaff points. If an attacker gets the saved fuzzy vault by any means it would be very hard for him to distinguish between the real minutiae points from the mixture of the minutiae and chaff points. Also if any attacker wants to authenticate himself falsely for a registered he will not get success because of the bio-cryptic combination. Result and analysis shows that our proposed method for chaff generation achieved a good performance gain.

We can add the features of multi-biometrics system to enhance the security of the existing system. It is also a future scope of our work.

References

[1] A. K. Jain, K. Nandakumar, and A. Ross., "50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities", Pattern Recognition Letters, 2016.

[2] R. Hooda1 and M. Kaur, "Novel Chaff Generation for Fingerprint Fuzzy Vault ", British Journal of Mathematics & Computer Science, 2015, vol. 10 (3), pp. 1-9,

[3] T. H. Nguyen, Y. Wang, Y. Ha, and R. Li, "Improved chaff point generation for vault scheme in bio-cryptosystems," IET Biometrics, 2013, vol. 2, no. 2, pp.48-55.

[4] Mohammad Khalil-Hani and Rabia Bakhteri, "Securing Cryptographic Key with Fuzzy Vault based on a new Chaff Generation Method" International Conference on High Performance Computing and Simulation (HPCS), 2010, pp. 259-265.

[5]S. Lee, D. Moon, Y. Chung, "Inserting chaff minutiae for the geometric hashing-based fuzzy fingerprint vault", Journal of Information Science and Engineering, vol. 25, no. 4, pp. 1177-1190, 2009.

[6] Jason Jeffers and Arathi Arakala, "Minutiae Based Structures for a Fuzzy Vault,"in Biometric Symposium IEEE, RMIT University, Melbourne, 2006, pp. 1-6.

[7]K.Nandakumar, A.K.Jain, and S.Pankanti, "Fingerprint-based fuzzy vault: implementation and performance," IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4, December 2007, pp. 744-757.

[8] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security and Privacy, 2003, Vol. 1, pp. 33-42.

[9] A. Juels, M. Sudan, "A Fuzzy Vault Scheme", in IEEE International Symposium on Information Theory, p. 408, 2002.