iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4133

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Performance Evaluation of Biometric Cryptosystem Using Fuzzy Vault

Ashish Vijayanand Chakole[1], Asst. Prof. A. Thomas[2]
[1,2]*Computer Science and Engg. GHRCE, Nagpur*

ABSTRACT: Biometric Cryptosystem is a security model which cannot be easily cracked as compared to traditional methods like password, ID card etc to get information. Information regarding a particular person in the database makes it vulnerable to template database attack. Fuzzy vault is a popular biometric cryptosystem technique which basically secure biometric template. In this technique the biometric features are used to lock and unlock the secret key, where coefficient of a polynomial equation is encoded. Existing method for chaff point generation is insufficient for real time implementation of biometric cryptosystem as would be required in today's information security system. Performance of system can be enhanced by adding more number of chaff points to the vault. These paper propose and aim to improvise the performance and security of fingerprint fuzzy vault scheme by using fast chaff point generation algorithm.
Keywords: Biometric, fuzzy vault, chaff point, template protection, chaff generation, security

I. INTRODUCTION

Biometrics is a science of verifying and establishing the identity of an individual through physiology features or behavioral traits. Biometric technologies are developed to use statistical analysis of an individual's biological features to determine his identity. Biometric template is an image of our physical or behavioral trait that is captured or analyzed. During the acceptance phase the biometric template is captured and stored in the smartcards and system database. During authentication of an individual's feature these template is used by applying encryption as well as decryption key. Cryptography provides the means to further protect Biometric Templates. Cryptography is a method encrypting and decrypting data in a particular form so that only those for whom it is intended can read and process it. That way, if the information and data were to be intercepted by a third party, there is not much which can be done unless they possess the keys for organizing the information. This is known as "Bio-Cryptography".

It is important that biometric templates used in biometric cryptosystem should be build and preserve in a secure way because, if the biometric data once replaced or stolen that can't be get back easily. Biometric template need to secure in the way that the attacker would not be able to duplicate biometric data easily even when the templates are compromised. If the template is compromised then the attacker will replicate the appropriate users. This leads to serious problem in privacy and security such that information leakage, imitation and tracking/tracing threats of biometric system.

II. LITERATURE SURVEY

A. Jain, K. Nandakumar et al (2008) has recommended the system in which author explain the attacks on traditional biometric system. Biometric recognition offers a reliable and natural solution to the problem of user authentication in identity management systems[16]. Author present a high-level categorization of the various vulnerabilities of a biometric system and discuss countermeasures that have been proposed to address these vulnerabilities. A.Jain, R.Ross (2004) presented personal recognition schemes to determine the identity of an individual. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. A. Jain and A. Kumar (2010) proposed paper on Biometric on next generation in which the author gives prevailing methods of human identification based on credentials (identification documents and PIN) are not able to meet the growing demands for stringent security in applications such as national ID cards, border crossings, government benefits, and access control[5].

Om Chaurasia (2012) has reviewed different approaches to fingerprint preprocessing in which author included most of the existing algorithms. When a fingerprint image is captured it is made pass through all the algorithms arranged in a particular order. If system process a fingerprint in this particular order, the final output is good enough for minutiae detection and feature extraction [11].

III. PROPOSED FRAMEWORK

Biometric template protection scheme can be broadly classified into feature transformation and biometric cryptosystems. Biometric feature are modified using a transformation function. The fuzzy vault construct is a biometric cryptosystem that secures both the secret key and the biometric template by binding them within a cryptographic framework. A fully automatic implementation of the fuzzy vault scheme based on fingerprint minutiae is done.

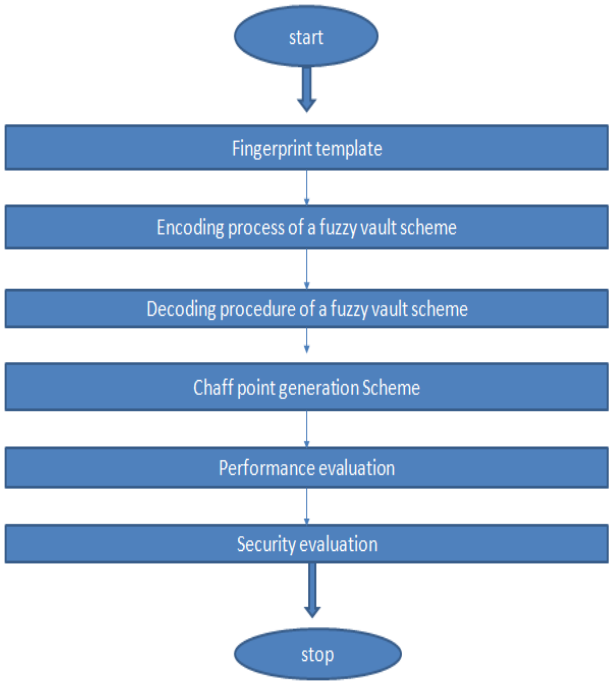


Figure1:- Proposed system flowchart

Fuzzy vault is a cryptographic construction that is designed to work with biometric features which are represented as an unordered set. By using encoding and decoding phase we can easily validate an authenticate user. In encoding phase, a user needs to protect secret key and fingerprint template. Secret key is encoded using cyclic redundancy check (CRC).

The minimum distance between any two selected minutiae is larger than a threshold (∂). Then and then only the chaff point is generated near to that minutiae point. In the encoding process of fuzzy vault scheme first the secret key K= {ki}n i=1 of length q*n bits is encoded using CRC that is cyclic redundancy check because the coefficients were q-bit value is that all the arithmetic operation of proposed fuzzy vault system were based on finite field F=GF(2q). To form the new q(n+1) bit code K' the q-bitCRC is concatenated at end of secret. For constructing the polynomial the secret K' is used. The secret K' is encoded into a polynomial P of degree n in F by partitioning it into (n+1) qbit values (c0, c1, ..., cn) and they are as the coefficients of P (i.e., P(x)=cnxn+...+c0). constructing the vault template, get a new set, V'={xi, yi}r+s i=1, by combining G and C sets together. And the fuzzy vault is created.

In decoding phase user tries to unlock the vault using query fingerprint. If the fingerprint template is matched then coefficient can be obtained and the secret key can be retrieved.

The security strength of fuzzy vault of system is totally based on infeasibility of the polynomial reconstruction problem. Vault performance can be improved by adding more number of chaff points.

IV. CHAFF POINT GENERATION TECHNIQUES

Two popular techniques use for the generation of chaff point i.e. Clancy's chaff point generation method and Khalil-hani's Chaff point generation. In Clancy's method chaff point is placed next to each other at a distance lesser than the threshold and Euclidean distance is used to validate chaff point and in khalil-hani's it is done with circle packing scheme in which point is added if its boundary doesn't overlap with any others existing point. To overcome the disadvantage of existing methods we propose a new method of chaff point generation.

Clancy's Chaff point generation method	Khalil- Hani's Chaff generation method	Our proposed chaff point generation method
Chaff point is placed next to each other at the distance less than δ, the adversary can immediately ignore them as unlikely candidates**.**	It uses a mathematical theorem of circle packing scheme. A new point is added to the fuzzy vault set only if its boundary does not overlap with the boundary of any other existing points	Fingerprint images split into the segments called image cell and the chaff point is generated randomly and unique in the image cell.
They use Euclidean distance to check the validity of chaff point should be located at minimum distance δ from the valid points.	They use addition, subtraction and comparison instead of squaring and square-roots operators in order to reduce computational intension.	This method reduces the number of the needed calculation times compared with the existing method

Table1:- Comparison over chaff point generation techniques

V. PROPOSED CHAFF POINT GENERATION METHOD

To overcome the fault of existing method we proposed a maximize chaff point generation method to enhance the biometric authentication system. Advantage of adding chaff points in the fuzzy vault is to hide the genuine fingerprint minutiae point, so that the chaff points could be chosen in a way that they must be different from genuine points. So that attacker couldn't identify the actual information of any individual. Only the authorized person should validate and access the information.

But before generation of chaff point some necessary steps should have to be done. For getting optimistic result the quality of image or fingerprint should be enhance. It could be done by image preprocessing and minutiae point extraction after this two step we carry forward for chaff point generation scheme.

A. Image Preprocessing

Fuzzy vault aims to secure critical data with the biometric template that only the authorized user can access the information regarding any individual. In the proposed paper fingerprint is used as a biometric trait, initially the image is filtered and pre-processing scheme is applied for the Conversion of 8-bit Gray image into a 1-bit image called Binarization and Elimination of redundant pixels of ridges called Thinning.

Figure 2:- Image filtering

B. Minutiae Extraction

Minutiae are important information extracted from the fingerprint image and stored in the database in the form of template. The basic features of minutiae include the position of minutiae(x, y) and orientation (€). Feature of minutiae is used as private attributes.

Extraction of minutiae point heavily depends upon the quality of input fingerprint image. To ensure that the performance of a

fingerprint authentication system would be powerful with respect to the quality of fingerprint images.

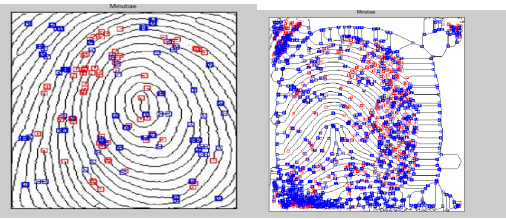


Figure 3:- Minutiae point extraction

Invalid minutiae are affecting the accuracy of matching. So, removing dishonest minutiae are essential to keep the system effective. With the combination of secret key and minutiae point a polynomial is evaluated and produces a secure vault.

A chaff point is randomly generated according to two criteria i.e. we can randomly generate unique chaff points in an arbitrary image cell and if that cell already contain a genuine point the that image cell is ignored. The distance between the new point and existing eight points is greater than or equal to the threshold ∂. This method reduces the number of calculation over previously existing methods.

Let G,N is the number of genuine points and the chaff points. K_i is the number of failed points (candidate points) for i^{th} chaff point.

$$S' = \sum_{i=1}^{N} (G+i-1) + \sum_{j=0}^{Ki} j(G+i-1)$$

Figure 4: chaff point generation

Once the minutiae point is created we can create a vault by applying a secret key k in encoding phase. And which is validate or give authentication to those who apply perfect decryption key. Then and then only the access will be allowed otherwise it is denied.

VI. PERFORMANCE EVALUATION

The propsed method was tested by creating 240 chaff points to hide 24 genuine minutiae point, the proposed method can achieve 4 times faster execution than clancy's and khalil-hani's method respectively. As the number of chaff point is increasing the execution time required for Clacy's and Khalil hani's algorithm is increasing exponentially, while in chaff point generation algorithm execution time increases linearly.

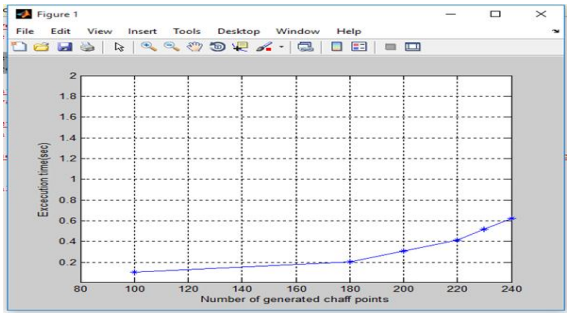


Figure5:- execution time of generating chaff points for proposed system

NO OF GENUINE POINT	NO.OF CHAFF POINT	CLANCY'S (SEC)	KHAILIL HANI'S (SEC)	CHAFF POINT GENERATION
10	100	0.03	0.20	0.09
20	200	0.33	0.55	0.25
24	240	52.05	38.90	0.61

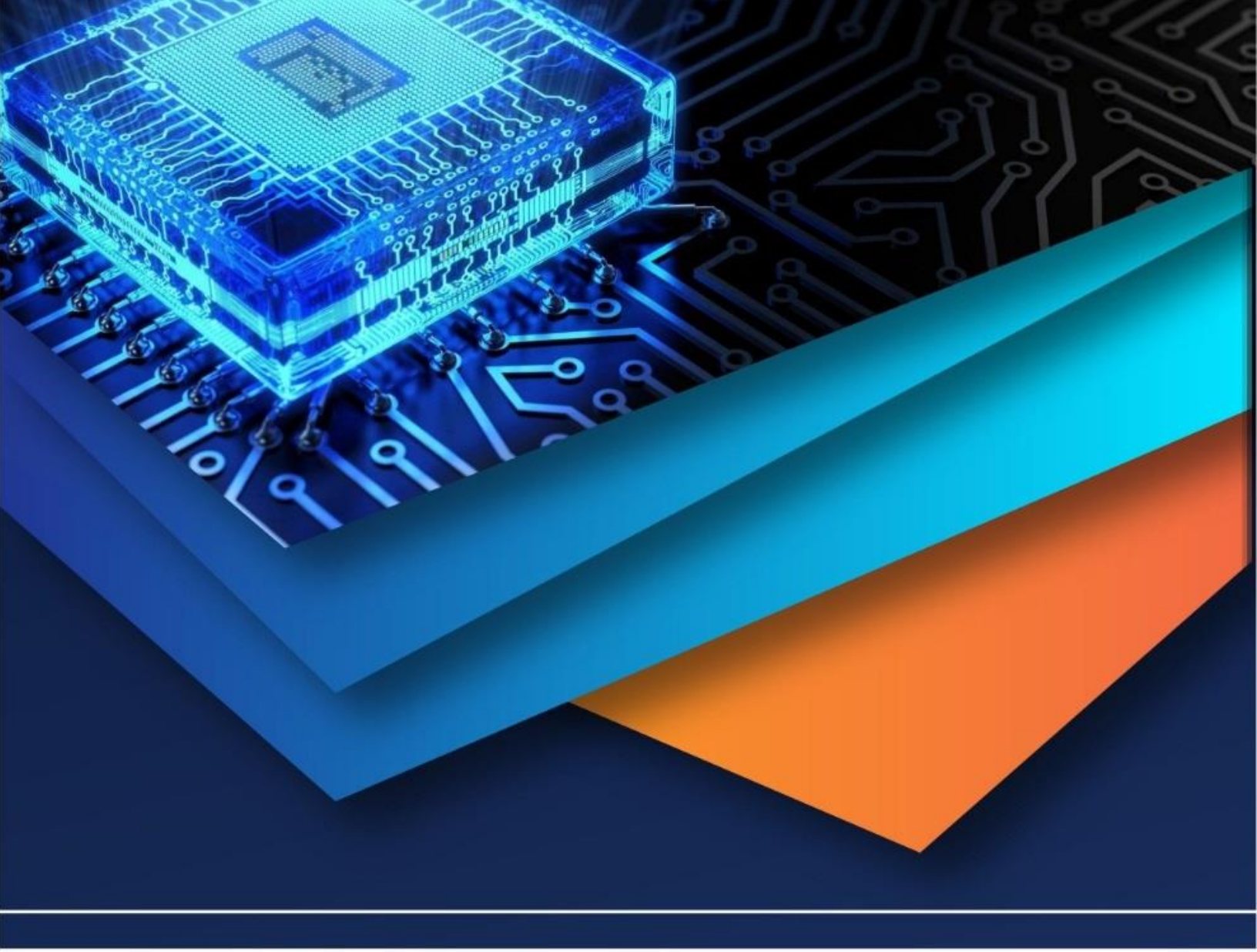
TABLE 2 PERFORMANCE COMPARISON

VII. CONCLUSION

This paper proposed and employed Chaff point generation algorithm to improve the performance and security of fingerprint fuzzy vault scheme . The chaff point generation algorithm achieves four to five times faster than previously existing methods. These results shows the proposed chaff point generation algorithm can achieve good performance and can ensure the security of fingerprint template and secret key.

REFERENCES

[1] Cai Li, Jiankun Hu, "A Security-enhanced Alignment-free Fuzzy Vault-based Fingerprint Cryptosystem Using Pair-polar Minutiae Structures", IEEE Transactions on Information Forensics and Security, 2016
[2] TK Dang, QC Truong, TTB Le, H Truong "Cancellable fuzzy vault with periodic transformation for biometric template protection", IET Biometrics Volume 5, Issue 3, September 2016, p. 229 – 235
[3] S.R. Soruba Sree, N. Radha "Cancellable multimodal biometric user authentication system with fuzzy vault", 2016 International Conference on Computer Communication and Informatics (ICCCI)
[4] S.Usha and M.Karthik, "A Robust Digital Image Watermarking for Biometric Template Protection Applications", International Journal of Advanced Research in Electrical, Electronics, and Instrumentation Engineering, ISSN 2320-3765, Volume 4, Issue 4, pp. 2067-2072, 2015.
[5] Rubal Jain and Dr. Chander Kant, "A Novel Approach for Securing Fingerprint Template using Steganography", International Journal of Innovations & Advancement in Computer Science, ISSN 2347 – 8616, Volume 4, Issue 6, pp. 503–512, June 2015.
[6] V.Wagh and S.Sonvane, "Minutiae Point Extraction using Biometric Fingerprint Enhancement", Journal on International Research in Engineering and Advance Technology, ISSN 2320-8791 Volume 2, Issue 1, pp. 777-789 March 2014.
[7] N.Hajare, A.Borage, N.Kamble, and S.Shinde, "Biometric Template Security using Visual Cryptography", International Journal of Engineering Research and Application, ISSN 2248-9622, Volume 3, Issue 2, pp. 1320-1323, March 2013
[8] S.Sowakarthika and N.Radha, "Securing Iris and Fingerprint Templates using Fuzzy Vault and Symmetric Algorithm", International Conference on Intelligent System and Control (ISCO), pp. 189-193, 2013.
[9] Thi Hanh Nguyen, Yi Wang, "A Fingerprint Fuzzy Vault Scheme using a Fast ChaffPoint Generation Algorithm", Signal Processing, Communication and Coming(ICSPCC), IEEE International Conference, pp. 1-6, 2013.
[10] S. Ponnarasi and M.Rajaram, "Impact of Algorithm for Extraction of Minutiae Points in Fingerprint Image", Journal of Computer Science, Volume 8, Issue 9, pp. 1467-1672, 2012.
[11] R. Verma, A. Gole, " Wavelet Application in Fingerprint Recognition", International Journal of Soft Computing and Engineering, Volume 1, Issue 4, pp. 129-134, 2011.
[12] A. Nagar, K. Nandakumar, and A. Jain, "Securing Fingerprint Template: Fuzzy Vault with Minutiae Descriptor," International Conference on Pattern Recognition, Volume 6, pp. 822-825, 2008.
[13] K. Nandakumar, A. Jain, S. Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation and Performance", IEEE Transaction on Information Forensics and Security, Volume 2, Issue 4, pp. 744-754, 2007.
[14] N. Raha, S. Chikkerur, and J. Connell, "Generating Cancelable Fingerprint Template", IEEE Transaction on Pattern Analysis and Machine Intelligence, Volume 29, Issue 4, pp. 561-572, 2007.
[15] Geetika, & Kaur, M. (2013, April). Fuzzy Vault with Iris and Retina: A Review. International Journal of Advanced Research in Computer Science and Software Engineering, 3(4).
[16] Jain, A., Nandakumar, K., & Nagar, A. (2008). Biometric Template Security. EURASIP Journal on Advances in Signal Processing (2008).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY