Volume 3, Issue 7, July 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Meliorating Fingerprint Fuzzy Vault using Multiple Polynomials

Sahil Gupta*, Manvjeet Kaur

Department of Computer Science and Engineering
PEC University of Technology
Chandigarh , India

Abstract— Biometrics is a science which uses persons distinguishable characteristics like fingerprints, iris, retina, hand geometries or behavioral characteristics like keystroke dynamics, gait etc for authentication. The biometric template is a digital representation of an individual's distinct characteristics extracted from biometric sample. The templates are the crucial elements of the biometric system. Once the templates are compromised, then the authenticity of the biometric systems is at risk, as the original biometric can be interchanged by the imposter's template or the template could be used to do replay attack or the original template can be spoiled so that the authenticated user of the system does not possess access. Keeping in ind the above situations and the consequences which template protection is holding, it's tried to implement the Fuzzy vault technique with multiple polynomials which works progressively without decreasing the performance of system for fingerprint biometric templates. Fuzzy vault is a high promising technique for securing user template by binding randomly generated secret keys with biometrics within cryptographic framework. Fuzzy vault is a state of the art technique for securing templates proposed Juels and Sudan which uses single polynomial for hiding genuine minutiae points. This paper proposes the Fuzzy vault technique using multiple polynomials. Security of Fuzzy vault depends on the polynomial reconstruction problem. In proposed worked, genuine points are hide using multiple independent polynomials. So it becomes very hard for attacker to reconstruct the multiple polynomials correctly which in turn gives very low FAR and FRR values.

Keywords— Fingerprint, Fuzzy Vault, FAR, FRR, Template, Multiple Polynomials.

I. Introduction

The word biometrics has its roots in Greek words "bios" (life) and "metrikos" (measure). It refers to the field that examines the unique physical traits like fingerprints, iris, retina, hand geometries or behavioral traits like keystroke dynamics, gait etc that can be used to determine a person's identity. Biometric recognition is the automatic identification of a person based on one or more of these traits. The word "biometrics" is also used to denote biometric recognition methods. Biometric technology can thwart fraud, enhance security, and curtail identity theft [1] [2]. Biometrics field is not new, it is evolved from the science of identifying a person based on his anatomical or behavioral features was introduced in the late nineteenth century by Alphonse Bertillon, a French policeman [3]. Later, Galton, Herschel, and Faulds noticed the usefulness of the ridge patterns present on our fingertips for identifying an individual. This led to the development of fingerprint matching systems. Initially, the fingerprints were manually matched by the experts but later, with the advancement in computing field, systems were developed to automate the processing (acquisition, matching and storage) of fingerprints. In addition to fingerprints, automatic processing of other personal traits such as palm prints, face, iris, etc. were also developed in parallel. Currently, biometric based recognition systems are being extensively used in a wide range of applications spanning governmental, forensic, and commercial sectors. The worldwide biometrics industry is also expected to grow steadily from annual revenue of 2 billion USD in 2009 to 11 billion USD in 2017 [4].

Traditionally, user authentication was performed based on passwords (*something you know*) or tokens such as smartcards (*something you have*). These techniques are, however, less secure since passwords can be forgotten or guessed and the tokens can be lost or stolen. But on the other hand, Biometrics provides a convenient means of authentication as it is based on *something you are* that cannot be lost or forgotten [5]. So, biometrics brings about a sea change in field of authentication systems. A reliable identity management system is urgently needed in order to combat the widespread growth in identity theft and to meet the increased security requirements in a variety of applications ranging from international border crossings to securing information in databases. Biometric recognition is the science of establishing the identity of a person using his/her anatomical and behavioral traits. Commonly used biometric traits include fingerprint, hand geometry, face, iris, voice, palm print, handwritten signatures and gait [6]. There are five major components in a generic biometric authentication system, namely, sensor, feature extractor, template generator, matcher and decision module (see Fig. 1).

Biometric authentication system has been increasingly deployed recently because they are more secure compared with traditional authentication mechanisms based on password. But the widespread application of biometric brought about new problems of privacy and security. That is, once the systems are compromised, the biometric data (i.e. template) is compromised permanently and it is hard to reissue a new one.

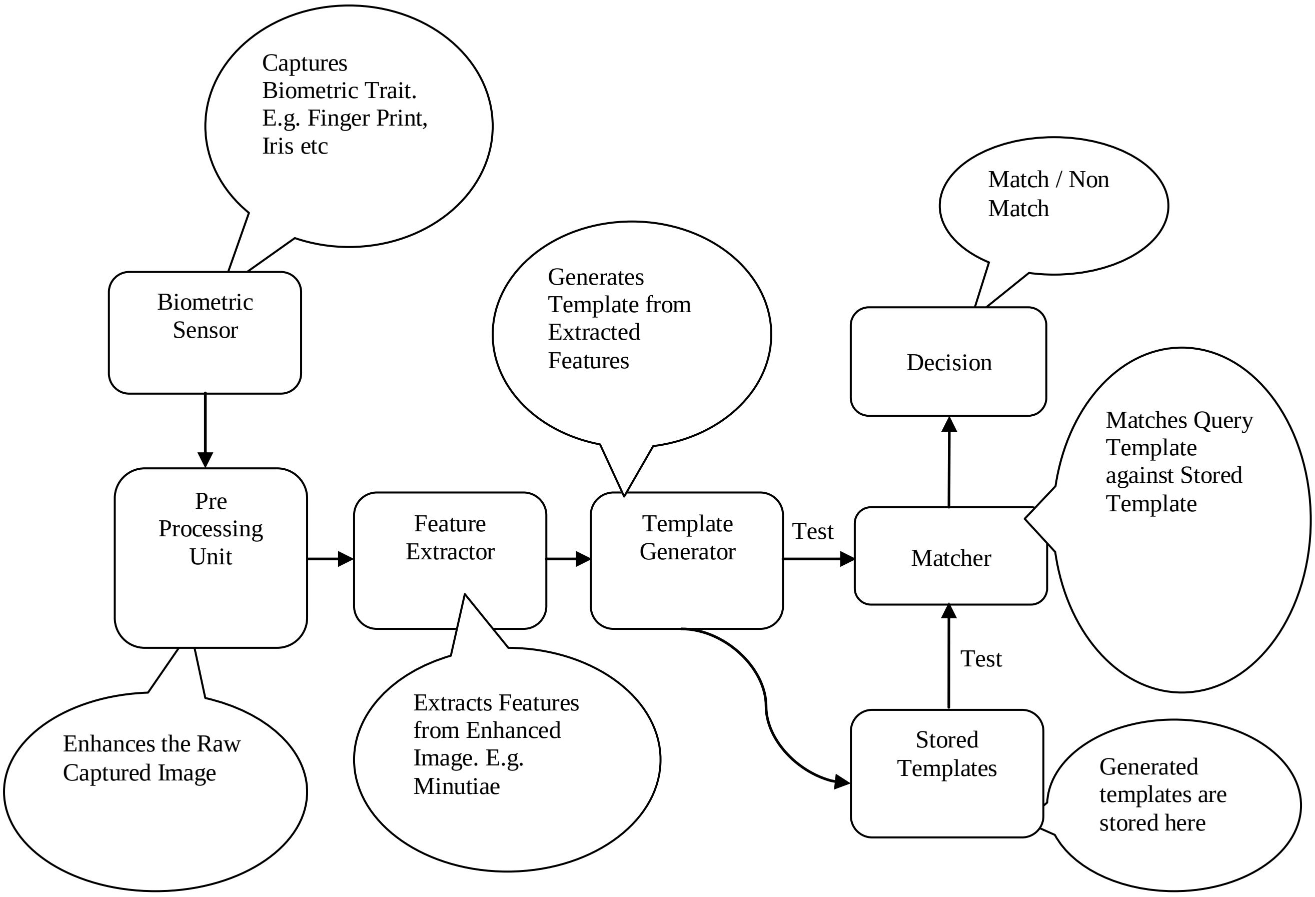
Captures Biometric Trait. E.g. Finger Print, Iris etc
Biometric Sensor
Pre Processing Unit
Enhances the Raw Captured Image
Feature Extractor
Extracts Features from Enhanced Image. E.g. Minutiae
Generates Template from Extracted Features
Template Generator
Test
Matcher
Matches Query Template against Stored Template
Decision
Match / Non Match
Test
Stored Templates
Generated templates are stored here

Fig. 1: Biometric authentication system

For protecting the template or biometric data, Ari Juels and Madhu Sudan has unearthed the fuzzy vault, this scheme combines biometric with cryptography, so that the biometric template can be utilized for authentication and its security can be protected. Fuzzy vault is comprised of two steps i.e. locking and locking. In this paper, novel locking process is proposed.

II. Fuzzy vault

Fuzzy vault was brought up by Juels and Sudan [7], that aims to secure vital data with the biometric template in a way that exclusively the authorized user can access the secret by providing the genuine biometric. A fuzzy commitment scheme can be understood with the help of simple example of Alice and Bob where Alice places a secret value S in a vault and lock it using an unordered locking set **L.** Bob, using an unordered set **U,** can unlock the vault only if **U** overlaps with **L** to great extent.

A. Locking process [8]:

Below steps will throw light on how secret key is kept hidden with the aid of biometric.

- **Preprocessing and minutiae extraction**: Preprocessing of the raw fingerprint image of a user is done in order enhance image quality and to remove false minutiae points & noise from it. After preprocessing, real minutiae points are extracted from the fingerprint image, that are stored in set X.
- **Secret key selection and checksum computation: S**ecret key **S** (e.g. 32 bit) is randomly selected using random function. CRC-16-CCITT is used to compute checksum on selected secret key. 16 bit checksum value is generated from CRC-16-CCITT, which is embedded in the end of selected secret key to form 48-bit modified secret key **S'**.
- **Polynomial formation:** The 48-bit key is divided into 8 equal parts to form the polynomial **P** with degree 5. Now, all the real minutiae points are projected on the polynomial **P**.
- **Chaff point generation:** Chaff points are simple dummy points that are randomly generated, which do not lie on **P** in order to hide and protect real minutiae points.
- **Vault generation:** The combination of real minutiae points and chaff points generates the fuzzy vault.

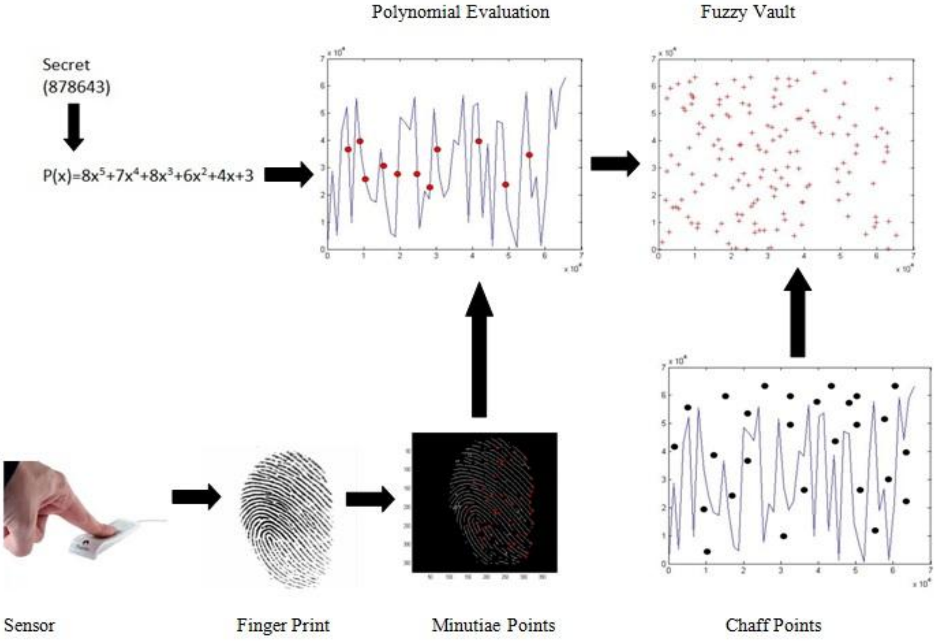

Fig. 2: Fuzzy Vault Locking Process

B. *Unlocking process* [8]*:*

Unlocking process is the step that reconstructs the polynomial from minutiae of query fingerprint image.

- **Preprocessing and minutiae extraction:** Preprocessing of the ***query*** fingerprint image is done in order enhance image quality and to remove false minutiae points & noise from it. After preprocessing, real minutiae points are extracted from the ***query*** fingerprint image are stored in set Y.
- **Equating biometric data:** Execute fingerprint matching by comparing set Y with set X stored in the locking process. The matched minutiae points are stored in another set Z, which are used for polynomial reconstruction.
- **Polynomial formation:** Lagrange interpolation is used to construct the possible polynomials using the set Z.
- **Checksum calculation:** The coefficients of polynomial are concatenated to form a string of bits. Then the string is divided into two parts where last part has 16 bits and rest of the bits is in the first part. Checksum of the first part all the polynomial is calculated.
- If the checksum calculated is equal to the last part of any polynomial then that polynomial is the required one and secret key is released to the user

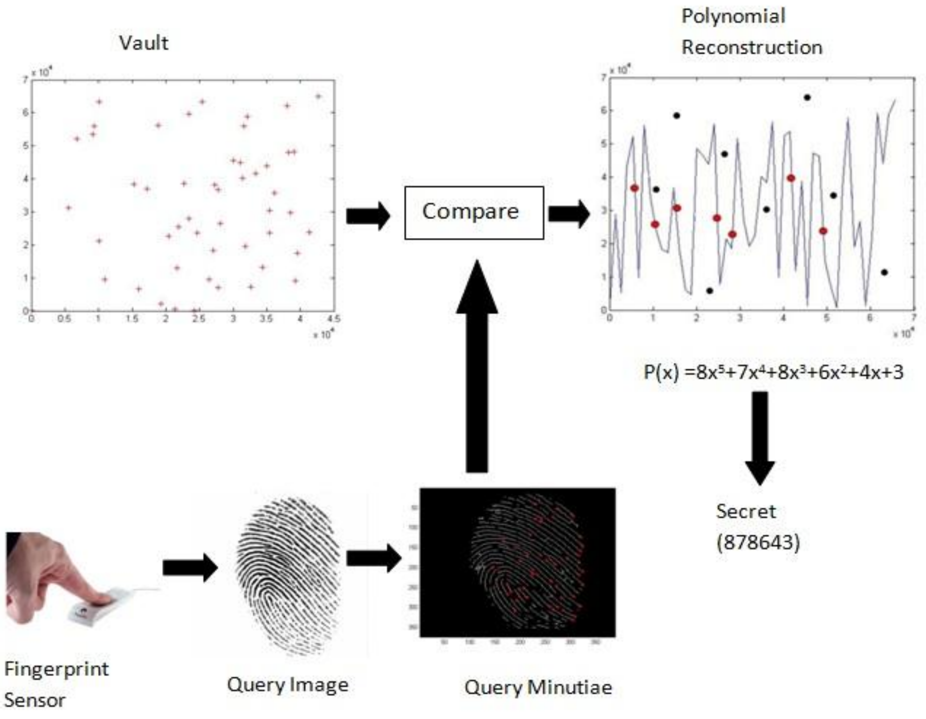

Fig. 3: Fuzzy Vault Unlocking Process

III. Proposed Method Using Multiple Polynomials Having Multiple Secret Keys

In proposed scheme, multiple polynomials are applied instead of single polynomial for the up gradation of Fuzzy Vault. Real minutiae points are projected on multiple polynomials, thus it aids in better obscuring out of minutiae points. So, it becomes very hard for attacker to reconstruct the correct multiple polynomials having real minutiae points. The proposed scheme will provide meliorated fuzzy vault for biometric systems which possesses good performance and security by curtailing the value of FAR (False Acceptance Rate) and FRR (False Rejection Rate).

A. Fuzzy Vault Locking

- **Minutiae extraction**: Firstly, preprocessing of fingerprint image F is done in order to remove false minutiae points and to get real minutiae points. Set M constitutes of real minutiae points extracted from given fingerprint image. Set M is stored along with some helper data extracted from fingerprint for alignment purpose. After that, a minutiae selection algorithm is applied on set M in order to get only best quality minutiae points. Selected best quality minutiae points are stored in other set N. Stored minutiae points in set N is now divided and stored equally in two different sets namely X and X’ respectively (e.g. if total of 50 real minutiae points are stored in set N, then set X contains first 25 minutiae points and X’ contains last 25 minutiae points) instead of all real minutiae points in one set X.
- **Secret key selection and checksum computation:** The scheme is designed to have better key management and to secure a secret key K of length 16*n, where n is the degree of the encoding polynomial. CRC-16-CCITT is used to compute checksum on selected secret key K. 16 bit checksum value is generated from CRC-16-CCITT, which is embedded at the end of selected secret key K to form a new secret key K’ of 16*(n+1) bits. A secret key K is randomly selected using random function, which is further divided into two overlapping sub keys SK1 and SK2 of (16*n)/2-bit each. Now, CRC-16-CCITT is used to compute checksum on two sub keys i.e. SK1 and SK2 [9]. Two 16 bit checksum values are generated from CRC-16-CCITT, which are embedded in the end of sub keys SK1 and SK2 respectively to form sub keys SK1**’** and SK2’. Overlapping property of sub keys helps in crossing the secret key. Segregation of secret key S into SK1 and SK2 is done as following method.

$$S=C_0C_1C_2C_3C_4C_5C_6C_7$$
$$SK1= C_0C_1C_2C_3C_4$$
$$SK2= C_3C_4C_5C_6C_7$$
$$SK1'= C_0C_1C_2C_3C_4 + \text{16-bit CRC value}$$
$$SK2'= C_3C_4C_5C_6C_7 + \text{16-bit CRC value}$$

- **Polynomial formation:** Now two sub keys SK1’ and SK2’ are divided into n + 1 equal parts respectively to form two polynomials **P** and **P’** with degree n each instead of forming single polynomial. Now, first half of the total real minutiae points are projected on polynomial **P** and other half are projected on polynomial **P’** instead of all the real minutiae points are projecting on the single polynomial (see Fig. 4) [10]. This method will lead to sparsely projection of minutiae points and also to very strict matching against query image in fuzzy vault unlocking. As domain for matching contains very few real minutiae points. So there is very minute chance of false matching and there is more obscuration of minutiae points as they are projected on two polynomials. Thus, makes very hard for attacker to reform the correct polynomial, as each polynomial contains very few minutiae points.

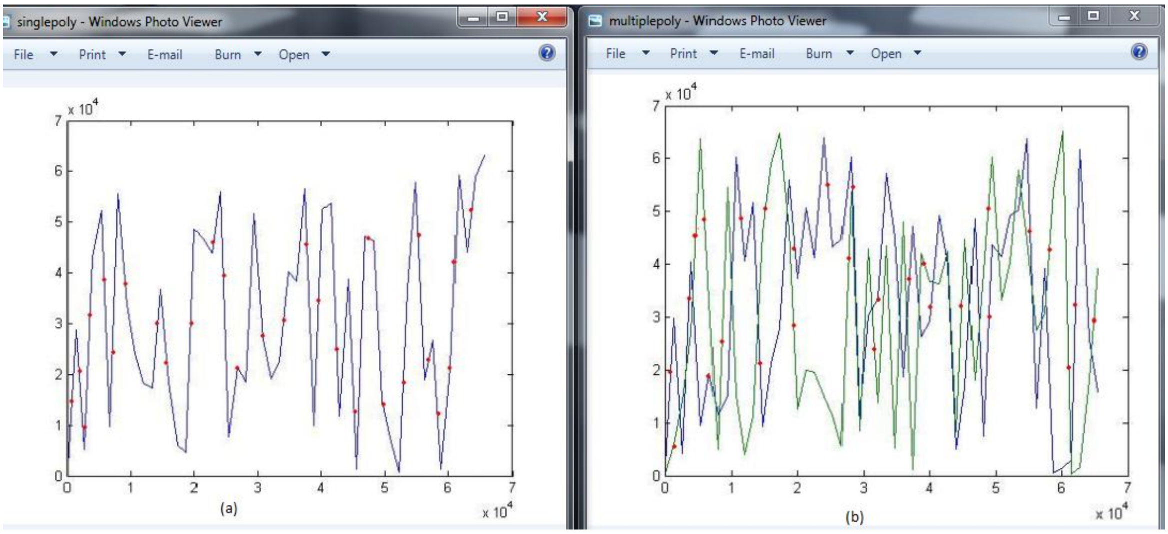

Fig. 4: Polynomial projection. (a) Previous method (b) Proposed method

- **Chaff point generation:** Random dummy points are generated and mingled up with minutiae points in order to obscure them. Some definite threshold distance δ is maintained from minutiae points projected on polynomials so that no chaff point will lie on either of the polynomials.

- **Vault generation:** The combination of real minutiae points and chaff points generates the fuzzy vault. Now, two fuzzy vaults are generated instead of single fuzzy vault.
  FV= X+X'+C

B. Fuzzy Vault Unlocking

- **Minutiae extraction:** Similarly, preprocessing of query fingerprint image is done in order to remove false minutiae points and to get real minutiae points. Set P constitutes of real minutiae points extracted from given fingerprint image. Set P is stored along with some helper data extracted from query fingerprint for alignment purpose. After that, a minutiae selection algorithm is applied on set P in order to get only best quality minutiae points and are well separated so that the minimum distance between any two selected minutiae is greater than δ (threshold distance). Selected best quality minutiae points are stored in other set Y and is used to filter the chaff points in the vault
- **Equating biometric data:** Execute fingerprint matching by comparing set Y with set X and set X' stored in the locking process. The matched minutiae points are stored in another set Z and set Z'; Lagrange interpolation is applied on set Z and Z' for polynomial reconstruction. From all the reconstructed polynomials the coefficients are extracted to form a series of sub keys. For a 2w bit key the last w bits are for the checksum. The checksum will be computed for all the polynomials using CRC for the first w-bits. If the checksum computed for the first w-bits match with the value of last w-bits. Then that will be the secret sub key released which is initially selected for the polynomial construction. Similarly after checksum computation and comparison, second sub key will be released. Union of SK1 and SK2 will provide original secret key S.
- **Key Release:** But if set Z contains more than n + 1 points and set Z' contain less than n + 1 points then only SK1 will be released, SK2 will not be released. This will be considered as Non-Match. If set Z' contains more than n + 1 points and set Z contain less than n + 1 points then only SK2 will be released, SK1 will not be released. This will also be considered as Non-Match. Partial key release will be considered as Non-Match. So, if both overlapping sub keys SK1 and SK2 are released then it is considered as genuine match otherwise not. This whole process can contribute a lot in reducing values of FAR and FRR.

IV. EXPERIMENT RESULTS

For the evaluation of the performance of the proposed method using multiple secret keys and multiple polynomials, testing is done on a standard database FVC-2004 database and also on live database acquired using Cross Match's Verifier 300 LC scanner. Each sample was matched against the remaining samples of the same finger in order to compute the False Rejection Rate (FRR) and Genuine Acceptance Rate (GAR). Likewise, the first sample of each finger was matched against the samples of the remaining fingers to compute the False Acceptance Rate (FAR). The experimental result predicts this novel locking process is suitable for lowering down the values of FAR and FRR, hence honing the biometric system.

TABLE I

	SINGLE POLYNOMIAL FUZZY VAULT	*MULTIPLE POLYNOMIAL FUZZY VAULT*
GAR (%)	75.55	80 FOR BOTH DATABASES(LIVE AND FVC 2004)
FAR (%)	8.8889	• 0 FOR LIVE DATABASE • 1.8 FOR OFFLINE DATABASE FVC 2004
FRR (%)	24.4445	20 FOR BOTH DATABASES (LIVE AND FVC 2004)

Table.1 shows that proposed scheme is able to lower down the values of FAR and FRR while enhancing the performance (GAR) of the biometric system.

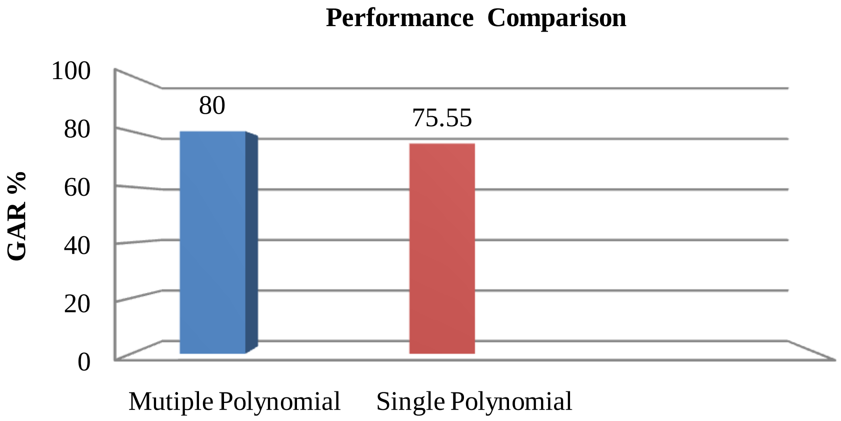

Fig. 5: Graph shows the difference between the GAR values of fuzzy vault using multiple polynomial and single polynomial

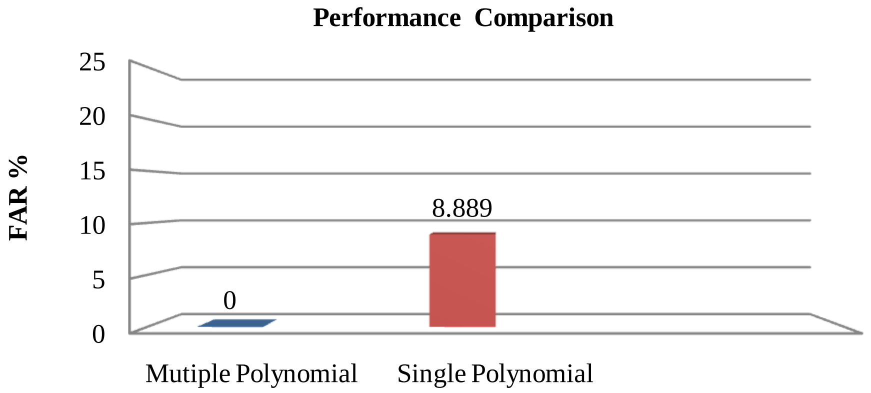

Fig. 6: Graph shows the difference between the FAR values of fuzzy vault using multiple polynomial and single polynomial (live data base result)

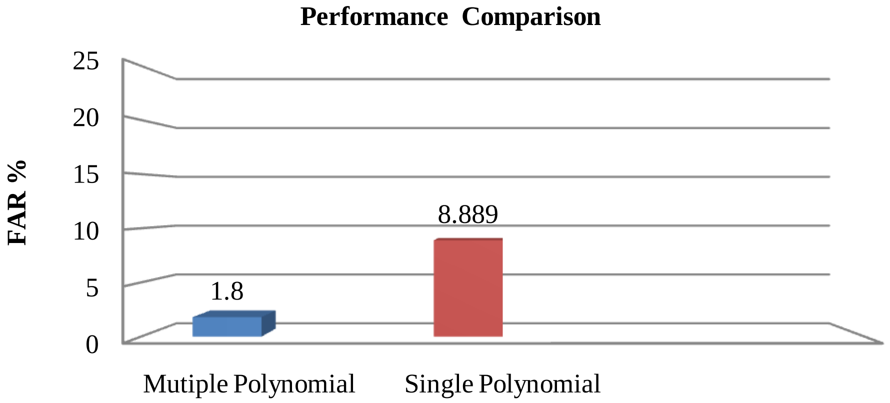

Fig. 7: Graph shows the difference between the FAR values of fuzzy vault using multiple polynomial and single polynomial (FVC database result)

Results shown in Fig. 6 shows results taken from testing of live database on proposed scheme and Fig. 7 shows results taken from testing of FVC database on proposed scheme. Both Fig. 6and 7 shows use of multiple polynomials have significant impact on FAR value. Below Fig. 8 shows that value of FRR has decreased in case of multiple polynomials as compare to single polynomial.

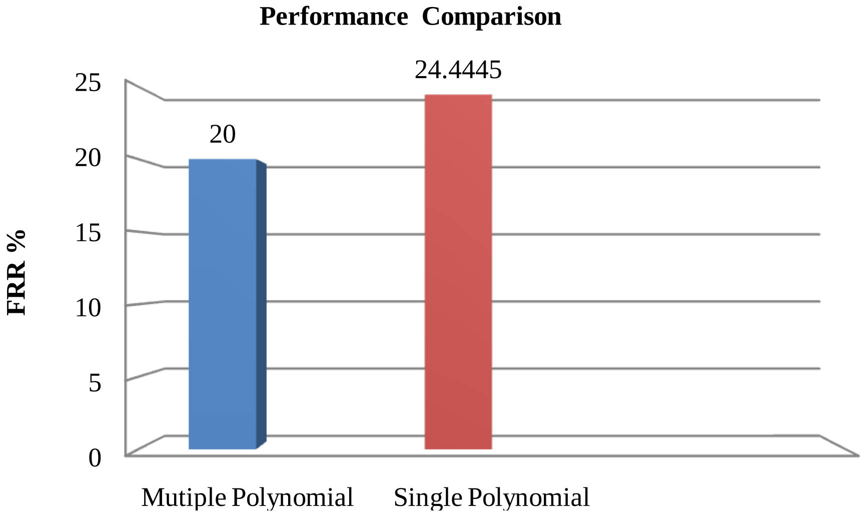

Fig. 8: Graph shows the difference between the FRR values of fuzzy vault using multiple polynomial and single polynomial

V. Conclusion

In this paper, a novel fuzzy vault scheme is proposed and implemented in which secret key is split into two overlapped sub keys and two polynomials are generated using two sub keys respectively. The experimental results demonstrate that proposed fuzzy vault scheme using multiple polynomials has better performance than fuzzy vault scheme using single polynomial.

REFERENCES

[1] Marcos Faundez-Zanuy, “Biometric Security Technology", in IEEE A&E Systems Magazine, Vol. 21, No. 6, June 2006, pp. nos. 15-26.

[2] “Biometrics Research Group”
http://biometrics.cse.msu.edu

[3] David Maltoni, Dario Maio, Anil K .Jain, Salil Prabhakar, “Handbook On fingerprint Recognition”, Springer 2003.

[4] “The future of Biometrics Market Research Report”
http://www.acuity-mi.com/FOB_Report.php

[5] Abhishek Nagar, "Biometric Template Security", Ph.D. Thesis, 2012.

[6] Vani Perumal, Dr.Jagannathan Ramaswamy, “An Innovative Scheme For Effectual Fingerprint Data compression using Bezier Curve Representation”, in International Journal of Computer Science and Information Security, Vol. 6, No. 1, 2009.

[7] Ari Juels and Madhu Sudan, “A Fuzzy Vault Scheme” , in IEEE International Symposium Information Theory, Lausanne, Switzerland, pp. 408, 2002.

[8] Karthik Nandakumar, Anil K. Jain and Sharath Pankanti, “Fingerprint-Based Fuzzy Vault: Implementation and Performance”, in IEEE Transition for Information Forensics & Security, pp. 744-757, 2007.

[9] Lifang Wu, Peng Xiao, Siyuan Jiang and Xin Yang, “A Fuzzy Vault Scheme For Feature Fusion”, in Springer-Verlag Berlin Heidelberg, pp. 237-243, Vol. 7098, 2011.

[10] Daesung Moon, Woo-Yong Choi, Kiyoung Moon and Yongwha Chung,” Fuzzy fingerprint Vault using Multiple Polynomials”, in IEEE International Symposium Consumer Electronics, pp. 290-293, 25-28 May 2009.