ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 3, Issue 2, pp: (72-79), Month: October 2016 – March 2017, Available at: www.paperpublications.org

A Reliable Cryptosystem for Biometric Template

[1]D. Gifty Thomas, [2]C. Anila Gifty

PG Student, Dept of CSE, Assistant Professor, Dept of CSE

Abstract: **Fingerprint Template based authentication has been widely implemented but still suffers from security and privacy due to information leakage. Bio-cryptosystems provide a solution for both template protection and key management which is to be bounded to the template. In bio-cryptosystems alignment free cryptosystems are used for template protection. Normally fingerprint matching takes place through the template that is stored in the database. To extract the major features for fingerprint matching, minutiae extraction is done. A minutia includes ridge, bifurcation, loop, delta, core...etc. In fingerprint cryptosystems alignment is necessary. In alignment free cryptosystems automatic alignment of templates takes place. This system uses local minutiae structures for verification. But it is not suitable for real time applications and the accuracy level of matching is not satisfactory. In order to increase the accuracy level we propose fuzzy vault fingerprint cryptosystem which uses pair-polar framework. This framework uses repeatable distortion of biometric features to protect the user specific data. Fuzzy vault increases the difficulty of retrieving the original template that is stored in the database. The proposed system performs well among all the systems used for template protection.**

Keywords: **Bio-cryptosystem, pair-polar, Template, Fuzzy, Alignment.**

I. INTRODUCTION

Computer Forensics is the science of obtaining, preserving and documenting evidence and digital electronic storage devices, such as computers, PDAs, digital cameras, mobile phones, and various memory storage devices. All must be done in a manner designed to preserve the probative value of the evidence and to assure its admissibility in a legal proceeding.

Science of forensics is applied in a digital environment where a traditional forensics specialist might collect and preserve fingerprints or other physical evidence, the computer forensics collect and preserves digital evidence.

The collection of digital evidence must be done through carefully prescribed and recognized procedures so that the probative value of digital evidence is prescribed to ensure its admissibility in a legal proceeding.

More people are using computers and devices with computing capability. For example, one can send and receive e-mail messages and handheld devices (mobile phones, or PDAs), participate in online computer games simultaneously with other game players over digital networks, or manage their finances over the Internet. Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioural characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioural characteristics are related to the pattern of behaviour of a

person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

Cancellable biometrics refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data. If a cancellable feature is compromised, the distortion characteristics are changed, and the same biometrics is mapped to a new template, which is used subsequently. Cancellable biometrics is one of the major categories for biometric template protection purpose besides biometric cryptosystem. In biometric cryptosystem, "the error-correcting coding techniques are employed to handle intra class variations." This ensures a high level of security but has limitations such as specific input format of only small intra class variations.

Fingerprint recognition is one of the biometric authentication techniques which express the individuality between the human beings. Fingerprint of humans are unique. Due to some unauthorized persons fake fingerprints are generated. In real life applications in-order to register the identity of the user, proofs are collected. The applications include banking systems and mobile transactions. Nowadays fingerprint is collected for government exams.

Matching of fingerprints is one of the most challenging tasks to be done by the detective agencies in-order to find the criminals. But after finding the original fingerprints, the collected ones are stored in the form of templates. In-order to reduce the accuracy of the fingerprint matching, attackers retrieves the templates from the database and replaces it with the fake ones. This becomes critical in the case of storing fingerprints of criminals.

In-order to avoid such critical situation researchers introduced biometric techniques to protect the template. In biometrics, the authentication techniques rely on measurable, physiological and individual characteristics that can be automatically verified. In such case the needed information can be stored in the database and can be retrieved when it is needed.

To protect the information in the database security must be provided. It can be done using the concept called cryptosystem which include encoding and decoding in it. Encoding and decoding takes place through key management. It is also known as polynomial construction.

The technique used in fingerprint recognition is extracting the minutiae features from the fingerprint image and a template is generated. The template contains features like ridge, bifurcation, valley, etc. By comparing the features with the image of the fingerprint recognition is done. When no match exists the fingerprint is rejected. As minutiae based matching methods considered to be more reliable, one of it is widely used in past decades.

II. RELATED WORK

As per the present scenario, in alignment free fingerprint cryptosystems matching is done by using the relative information between the minutiae and it adds additional information to the fingerprint template to facilitate automatic alignment during the verification process. But pre-alignment is only acceptable in research but it is not practical in real life applications. Automatic alignment produces issues that it relies on the core points and high curvature points and as the result automatic alignment leads to high False Rejection Rate (FRR). Due to the information leakage in alignment free cryptosystems the accuracy level goes low. Based on the survey the research work provided by the authors can be given as follows

T.C Clancy et al[6] have dealt with the authentication based on smart card. The fundamental insecurities hampering a scalable, wide-spread deployment of biometric authentication are examined, and a cryptosystem capable of using fingerprint data as its key is presented. For the application, situations where a private key stored on a smartcard are used for authentication in a networked environment, and assumption is done as an attacker can launch online attacks against a stolen card. Smartcards over a new paradigm for authentication. Now, users' private keys are stored on smartcards. These users can prove their identity by using the card to provide a correctly signed message to an authentication server. Relying on the security of public-key authentication, the private key on the smartcard is protected.

U.Uludag et al [10] have dealt with the fuzzy vault based technique. Biometrics-based user authentication has several advantages over traditional password-based systems for standalone authentication applications, such as secure cellular phone access. This is also true for new authentication architectures known as crypto-biometric systems, where cryptography and biometrics are merged to achieve high security and user convenience at the same time. The realization of a cryptographic construct, called fuzzy vault, with the fingerprint minutiae data is specified. This construct aims to secure critical data (e.g., secret encryption key) with the fingerprint data in a way that only the authorized user can access the secret by providing the valid fingerprint. The results show that 128-bit AES keys can be secured with fingerprint minutiae data using the proposed system.

Xinjian Chen et al[11] have dealt with the problem of matching the fingerprints with non linear distortion. Coping with nonlinear distortions in fingerprint matching is a challenging task. A novel method, a Fuzzy Feature Match (FFM) based on a local triangle feature set to match the deformed fingerprints. The fingerprint is represented by the fuzzy feature set (i.e.) the local triangle feature set. The fuzzy feature set is used to characterize the similarity between fingerprints. The fuzzy similarity measure for two triangles is introduced and extended to construct a similarity vector including the triangle-level similarities for all triangles in two fingerprints. A similarity vector pair is defined to illustrate the similarities between two fingerprints. The FFM method maps the similarity vector pair to a normalized value which quantifies the overall image to image similarity. Experimental results confirm that the FFM based on the local triangle feature set is reliable for fingerprint matching with nonlinear distortions.

N.K Ratha et al[1] have dealt with the cancellable identifiers. Biometrics-based authentication systems offer obvious usability advantages over traditional password and token-based authentication schemes. However, biometrics raises several privacy concerns. A biometric is permanently associated with a user and cannot be changed. Hence, if a biometric identifier is compromised, it is lost forever and possibly for every application where the biometric is used. Moreover, if the same biometric is used in multiple applications, a user can potentially be tracked from one application to the next by cross-matching biometric databases. Several methods to generate multiple cancellable identifiers from fingerprint images is demonstrated to overcome these problems. In essence, a user can be given as many biometric identifiers as needed by issuing a new transformation "key." The identifiers can be cancelled and replaced when compromised. It is empirically compared using the performance of several algorithms such as Cartesian, polar, and surface folding transformations of the minutiae positions. It is demonstrated through multiple experiments that can achieve revocability and prevent cross-matching of biometric databases. It is also shown that the transforms are noninvertible by demonstrating that it is computationally as hard to recover the original biometric identifier from a transformed version as by randomly guessing. Based on these empirical results it is concluded that the feature-level cancellable biometric construction is practicable in large biometric deployments.

C.Lee et al[12] have dealt with alignment free cancellable fingerprint template. To replace compromised biometric templates, cancellable biometrics has been introduced. The concept is to transform a biometric signal or feature into a new one for enrolment and matching. For making cancellable fingerprint templates, the relative position of a minutia to a core point in a given fingerprint image is specified. Thus, a query fingerprint is required to be accurately aligned to the enrolled fingerprint in order to obtain identically transformed minutiae. A new method for making cancellable fingerprint templates that does not require alignment is based on the local minutiae information. For each minutia, a rotation and translation invariant value is computed from the orientation information of neighboring local regions around the minutia. The invariant value is used as the input to two changing functions that output two values for the translational and rotational movements of the original minutia, respectively, in the cancellable template. When a template is compromised, it is replaced by a new one generated by different changing functions. This approach preserves the original geometric relationships (translation and rotation) between the enrolled and query templates after they are transformed. Therefore, the transformed templates can be used to verify a person without requiring alignment of the input fingerprint images. Evaluation takes place in two criteria: performance and changeability. When evaluating the performance, verification accuracy varies as the transformed templates were used for matching. When evaluating the changeability, the dissimilarities between the original and transformed templates, and between two differently transformed templates, which were obtained from the same original fingerprint has been measured. The experimental results show that the two criteria mutually affect each other and can be controlled by varying the control parameters of the changing functions.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 3, Issue 2, pp: (72-79), Month: October 2016 – March 2017, Available at: www.paperpublications.org

K. Nandakumar et al[13] have dealt with the implementation and performance of fuzzy vault. Reliable information security mechanisms are required for increasing the magnitude of identity theft in the society. While cryptography is a powerful tool to achieve information security, the challenge in cryptosystems is to maintain the secrecy of the cryptographic keys. Though biometric authentication can be used to ensure that only the legitimate user has access to the secret keys, a biometric system itself is vulnerable to a number of threats. A critical issue in biometric systems is to protect the template of a user which is typically stored in a database or a smart card. 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 presented. Since the fuzzy vault stores only a transformed version of the template, aligning the query fingerprint with the template is a challenging task. Extract high curvature points derived from the fingerprint orientation field and use them as helper data to align the template and query minutiae. The helper data itself do not leak any information about the minutiae template, yet contain sufficient information to align the template and query fingerprints accurately. Further, apply a minutiae matcher during decoding to account for nonlinear distortion and this leads to significant improvement in the genuine accept rate. It is also shown that performance improvement can be achieved by using multiple fingerprint impressions during enrollment and verification.

III. PROPOSED SYSTEM

In Alignment free cryptosystem the accuracy level is not satisfactory. In order to overcome this issue we propose fuzzy vault fingerprint cryptosystem. This system uses pair-polar minutiae structure. It uses the reference minutiae and all others within the polar coordinate space. In this technique minutiae extraction takes place from the fingerprint image which can be known as the template and to the template chaff points are added. The genuine points and the chaff points are distinguished; chaff points are bound to the template to create a fuzzy vault. The template is stored in the database. When the query is send to the database for retrieving the template. The spurious minutiae get reduced and the original template is retrieved.

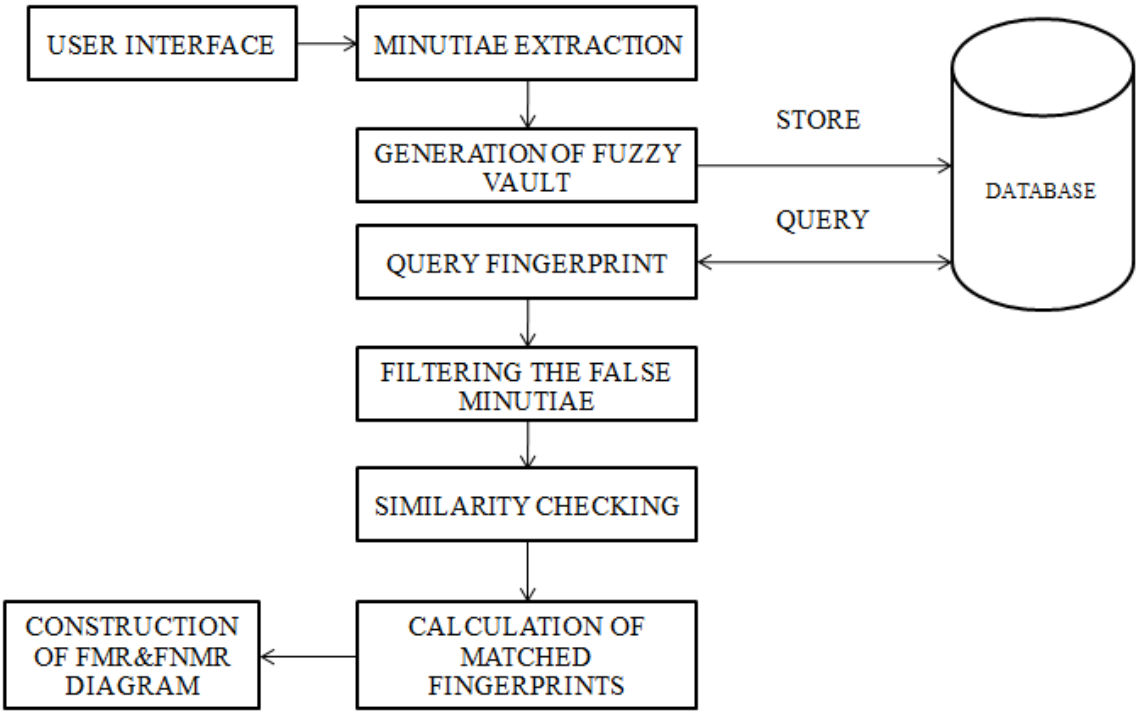

Fig: Architecture of fuzzy vault system

User Interface is the one where the images of the fingerprint are sensed and the different image of the same fingerprint is collected. Then the collected fingerprints are stored in the database. The fingerprint image is not stored in the database, only the template of the fingerprint image is stored in the database. Formation of the template can be done through the

minutiae extraction. Minutiae extraction is done to extract ridge and the bifurcations from the fingerprint image. The extraction of ridge and bifurcation is done check the similarity between the fingerprints using minutiae based methods. The extracted minutiae points can be called as the genuine points or original minutiae points. The genuine points must be treated as the confidential one. In the case of certain applications fingerprint matching takes place trough the genuine points. The third party can easily retrieve the template on knowing the genuine points.

To provide security to the template the fuzzy vault creation is done. Here the fuzzy vault indicates the addition of chaff points to the template. The chaff points are placed at the certain distance. The genuine points and the chaff points are distinguished. Then the template is stored in the database. The template is queried from the database. To the query fingerprint the filtering of the false minutiae takes place. At this case the chaff points get reduced. The original template of the fingerprint image is retrieved.

The similarity between the fingerprint retrieved and fingerprints in the database is checked. The similarity is computed using the score value. Similarity computation is done to evaluate the number of structures find the successful match. Based on the score value the FMR and FNMR diagrams are constructed. The construction of FMR AND FNMR is done to evaluate the performance of the system. When the error rate decreases the recognition accuracy is satisfactory.

A. Template Generation:

The general shape of the fingerprint is generally used to pre-process the images, and reduce the search in large databases. This uses the general directions of the lines of the fingerprint, and the presence of the core and the delta. The minutia is extracted from the fingerprint image and the minutia consists of features including ridge, core, bifurcation etc. A critical step in automatic fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images. The image is converted to binary image. After the operation, ridges in the fingerprint are highlighted with black colour while furrow are white. Ridge thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide, then the template of the fingerprint image is generated. The corresponding template is stored in the database for future use.

B. Fake Minutiae Addition:

To provide security to the template fake points (chaff points) are generated randomly. It resembles as the genuine minutiae. A well-established minutiae matcher in global minutiae matching algorithms is seamlessly transformed into a transformation-invariant feature-applicable version, information about the original feature is largely retained using a fine quantization, which only removes the decimal parts of the features. Unlike many fuzzy vault constructions that choose chaff points separated by a minimum distance d from any genuine point and previously added chaff point, where d is the distance inside which a query feature and vault point are considered matched during verification, the proposed vault selects both genuine and chaff features greater than 2d away from each other. As this design removes the probability that a query feature matches multiple points in the vault, decoding time is significantly reduced.

C. Similarity Computation:

In global minutiae matching algorithms, after two fingerprints (a template and query) are aligned, their corresponding minutiae are paired. This minutiae matcher is widely adopted in minutiae-based fingerprint matching because it can effectively deal with the intra-class variations between different captures of the same fingerprint. At first glance, the above well-established minutiae matcher cannot be applied directly to the P-P coordinate vectors which represent relative information and do not contain Cartesian positions. The filtering of the fake minutiae takes place and then the template matching takes place for the fingerprints in the database. The different images of the same fingerprint is taken and stored in the database. The similarity value is computed and then the FMR and FNMR diagram is drawn with the computed score to diagnose the performance.

IV. EXPERIMENTAL RESULTS

Performance evaluation focuses in measuring the progress and process of achievement of project results and how inputs and outputs are producing outcomes and impacts. Performance evaluations are designed to identify accomplishments, performance issues, and constraints in the implementation. The performance of the implemented system can be analysed with the help of x-graph utility for generating 2-D graphs. The values for analysing performance can be retrieved from trace files obtained during simulation.

Performance metrics used for biometric systems are:

False Match Rate [14] (FMR, also called FAR = False Accept Rate): The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs that are incorrectly accepted. In case of similarity scale, if the person is an imposter in reality, but the matching score is higher than the threshold, then he is treated as genuine. This increases the FMR, which thus also depends upon the threshold value.

False Non-Match Rate [14] (FNMR, also called FRR = False Reject Rate): The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs that are incorrectly rejected.

Receiver Operating Characteristic or relative operating characteristic (ROC)[14]: The ROC plot is a visual characterization of the trade-off between the FMR and the FNMR. In general, the matching algorithm performs a decision based on a threshold that determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts. Conversely, a higher threshold will reduce the FMR but increase the FNMR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviation scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

Equal Error Rate or crossover error rate (EER or CER)[14]: The rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate.

Failure To Enroll Rate (FTE or FER)[14]: The rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

Failure To Capture Rate (FTC)[14]: Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.

Template Capacity [14]: The maximum number of sets of data that can be stored in the system.

MATCHING OF SAMPLES:

Two different protocols (the 1vs1 and standard FVC)[2] to evaluate the recognition performance of the proposed system In the 1vs1 protocol, the first image of each finger is compared with the second image of the same finger to compute the FRR and then compared with the first images of the remaining fingers to compute the FAR. To avoid a duplicate comparison, if image 1, as the template, has been compared with image 2, when image 2 is chosen as the template, it is not compared with image 1 again. Therefore, for FVC 2000, FVC 2002 and FVC 2004, this results in 100 genuine and $(1 + 99) * 99/2 = 4950$ imposter matching attempts, while for FVC 2006, 140 genuine and $(1 + 139) * 139/2 = 9730$ imposter ones. The P-P minutiae structure describes the relationships between a reference minutia and all the other minutiae in a fingerprint within its polar coordinate space. As a fingerprint usually contains 30 to 50 minutiae, the features extracted from this structure are more discriminative than those from other local minutiae structures, such as the five-nearest neighbor, Voronoi neighbor and triangle.

Also, distortions in local areas are no longer determinants of structure matching. To test the discriminative power of the P-P minutiae structure, the experiments are conducted on the publicly available database FVC2002DB2. In this experiment, compare the first image of each finger, firstly with the second image of the same finger and then with the first images of the remaining fingers to evaluate the number of structures that successfully find a match in either case. For simplicity, the thresholds d and θ are fixed as $d = 9$ and $\theta = 20$. Two P-P minutiae structures are deemed matched if they have no less than n matched P-P coordinate vectors. The results are shown in Figure 5.1, when $n = 3$, the percentage gap is slightly less than 60% and, when $n = 4, 5, 6$, increases to more than 70%. Obviously, the P-P minutiae structure is more discriminative than five-nearest neighbor (40%), Voronoi neighbor (20%), and triangle structures (25%).

FMR AND FNMR DIAGRAM:

The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs that are incorrectly accepted. In case of similarity scale, if the person is an imposter

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 3, Issue 2, pp: (72-79), Month: October 2016 – March 2017, Available at: www.paperpublications.org

in reality, but the matching score is higher than the threshold, then he is treated as genuine. This increases the FMR, which thus also depends upon the threshold value.

The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs that are incorrectly rejected. The rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate.

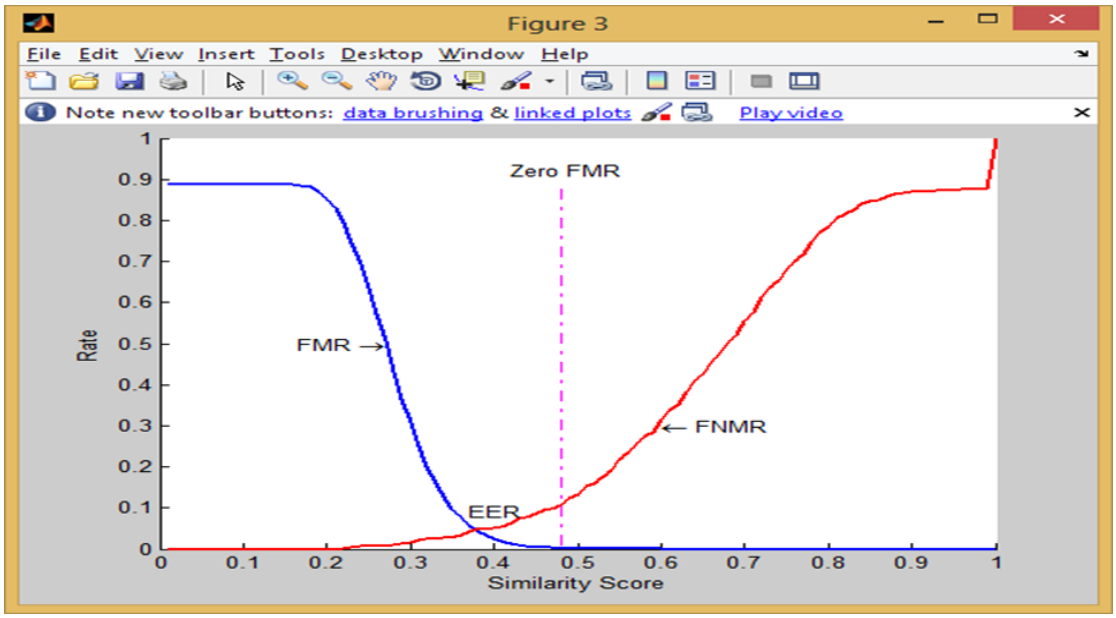

Fig 2: FMR and FNMR Diagram

V. CONCLUSION AND FUTURE WORK

Alignment-free fingerprint cryptosystems provide a promising solution for template/key protection without registration, the recognition accuracy of previous work is insufficiently satisfying due to poor discriminative power of the features used as well as improper handling of nonlinear distortions in the quantized/encrypted domain. To address this issue an alignment-free fuzzy vault using pair-polar (P-P) minutiae structures is proposed. This system improves recognition accuracy. The P-P minutiae structure is more discriminative than local minutiae structure. The fine quantization used in our system can retain more information about a fingerprint template to a greater extent, the recognition accuracy is satisfying when compared to the previous work and enable the direct use of a well-established minutiae matcher, which is specially designed to deal with intra-class variations.

A well-known issue regarding the fuzzy vault is that it is vulnerable to the cross-matching attack. If the attacker has access to multiple vaults generated from the same biometric data, he can easily identify the genuine features by comparing the genuine features between the vaults. This issue, however, can be addressed in the future work by setting a distinct seed for the random number generators in each application. In this way, the same biometric data is transformed to different features encoded in the fuzzy vault. Once a vault is compromised, a new vault can be created from the same fingerprint data by replacing the current vault. While implementing this technique the genuine points could not retrieved easily and critical to retrieve the original template.

REFERENCES

[1] Bolle R.M , Connell .J.H, Chikkerur .S, and Ratha .N.K (2007), 'Generating cancelable fingerprint templates,' IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no.4, pp. 561–572.

[2] Cai Li, Jiankun Hu," A Security- Enhanced Alignment-Free Fuzzy Vault-Based Fingerprint Cryptosystem Using Pair-Polar Minutiae Structures," IEEE Trans. Inf. Forensics Security, vol.11, no.3, pp. 543-555, March.2016

[3] Cao .K, Li .P, Tao .X, Tian .J, Wang .R, and Yang .X (2010) 'An alignment free fingerprint cryptosystem based on fuzzy vault scheme,' J. Netw. Comput. Appl., vol. 33, no. 3, pp. 207–220.

[4] Chen .X, Tian .J,Yang .X, and Zhang .Y (2006), 'An algorithm for distorted fingerprint matching based on local triangle feature set,' IEEE Trans.Inf. Forensics Security, vol. 1, no. 2, pp. 169–177.

[5] Choi .J.Y, Kim .J, Lee .C, Lee .S, and Toh .K.A (2007), 'Alignment-free cancelable fingerprint templates based on local minutiae information,' IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 37, no. 4, pp. 980–992, Aug. 2007.

[6] Clancy .T.C, Kiyavash .N,Lin .D.J(2003), 'Secure smartcard based fingerprint authentication,' in Proc. ACM SIGMM Workshop Biometric Methods Appl., Berkeley, CA, USA, pp. 45–52.

[7] Hu .J, and Wang .S (2012), 'Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach,' Pattern Recognit., vol. 45, no. 12, pp. 4129–4137.

[8] Jain .A.K, Nandakumar .K, and Pankanti .S (2007), 'Fingerprint-based fuzzy vault: Implementation and performance,' IEEE Trans. Inf. Forensics Security, vol. 2, no. 4, pp. 744–757.

[9] Jain .A.K, Pankanti .S, Prabhakar .S, and Uludag .U (2004), 'Biometric cryptosystems: Issues and challenges,' *Proc. IEEE*, vol. 92, no. 6, pp. 948–960.

[10] U. Uludag, S. Pankanti, and A. K. Jain (2005), "Fuzzy vault for fingerprints," in Proc. Audio-Video Based Biometric Person Authentication, pp. 310–319.

[11] X. Chen, J. Tian, X. Yang, and Y. Zhang(2006),"An algorithm for distorted fingerprint matching based on local triangle feature set,"IEEE Trans. Inf. Forensics Security, vol. 1,no. 2,pp. 169- 177.

[12] C. Lee, J.-Y. Choi, K.-A. Toh, S. Lee, and J. Kim (2007) "Alignment-free cancelable fingerprint templates based on local minutiae information,"IEEE trans.Syst., Man, Cybern. B, Cybern., vol.37, no. 4, pp.980-982.

[13] K. Nandakumar, A. K. Jain, and S. Pankanti(2007) "Fingerprint-based fuzzy vault: Implementation and performance," IEEE Trans. Inf. Forensics Security, vol. 2, no. 4, pp. 744–757.

[14] https:// en.wikipedia.org