A Bio-Cryptosystem to Mitigate Fingerprint Uncertainty Based on Modified Voronoi Neighbor Structures

Theresa Priyanka A. C [1*], Shemi Mol B[2], Meera Krishna G. H[3]
[1*]PG Scholar, Dept. of computer science and engineering
[2]Assistant Professor, Dept. of computer science and engineering
[3]Assistantt Professor, Dept. of computer science and engineering
TKM Institute of Technology, Kollam, India

***Abstract*-Bio-cryptography is a blend of biometrics and cryptography to enhance security and privacy of a user. Fingerprints are widely used in bio-cryptosystem due to their unique pattern of ridges and valleys. Uncertainty of fingerprints is a major issue. To avoid uncertainty fingerprints should be robust to translation, rotation, scale, shear and clutter. In this paper an alignment free bio-cryptosystem is introduced to reduce fingerprint uncertainty .A fixed length bit string is extracted from the modified VNSs and matching of fingerprints is performed in the encrypted domain. A key that needs protection is generated directly from the biometric features. Fake minutiae are removed after the minutiae extraction technique which enhances the security of the system.**

Index Terms-Fingerprint, Bio-cryptosystem, Voronoi Neighbor Structures

I.INTRODUCTION

Cryptography is the practice and study of techniques for secure communication in the presence of third parties and is related to various aspects of information security, such as authentication, data confidentiality and data integrity. User authentication is of vital importance to the security of computer systems. Authentication is used by server when the server needs to know exactly who is accessing their information or site. In traditional cryptographic systems user authentication is token or password based. Traditional password-based authentication has become inadequate for demanding applications; since the entropy of a password is inherently limited by the capability of human memory, while the computing power used by dictionary attackers is growing steadily. Token-based authentication is much stronger, since the secret key inside the token is usually as big as hundreds or thousands of bits. Furthermore it is generated at random, and well protected by modern electronic technologies. However, tokens may be used by unauthorized people, in case they are lost or stolen. So, in recent years people have turned to authentication methods using automated biometrics such as fingerprint etc. Biometrics which are physical traits of a person such as fingerprint face, iris, and voice can be used for authentication.

However biometrics has two major drawbacks. First is the diverse and noisy nature of biometrics. The second drawback in the biometric authentication is that biometrics cannot be reset or replaced. Hence protecting the biometric templates is a critical issue. Bio-cryptography is an emerging security technology that combines the fields of cryptography and biometrics. The biometrics and the cryptographic systems can be combined together in two ways. The binding of the cryptographic key along with the biometric template ensures user privacy and security as the biological and behavioral characteristics of a user cannot be revealed by another unauthorized user. In the first approach, cryptographic key generation is decoupled with biometric matching. Therefore, the cryptographic key is released when there occurs biometric matching. This approach is known as Biometric based key Release. The second method is the biometric key generation in which both the biometric template and the cryptographic key are combined together .This combination does not need any matching operation to extract the key. The Bio-cryptosystems provide higher level of security since it assists the cryptographic systems to encrypt and decrypt using the biometric templates.

Fingerprint alignment degrades the performance of fingerprint bio-cryptosystem. Alignment is the process of converting the coordinates of one fingerprint into a common coordinate system because the scans taken at different time tend to be different. Fingerprint uncertainties such as distortion, displacement are unavoidable during the process of image capturing. All of these degrade the performance of a fingerprint bio-cryptosystem. In this paper an alignment free bio-cryptosystem based on modified Voronoi neighbor structures are introduced which eliminates fingerprint uncertainty and provide distortion insensitivity. False minutiae are removed using false minutiae removal algorithm. Firstly, Voronoi neighbor structures are created from the minutiae set. Voronoi neighbor structures are mapped into a 3D array to account small distortion. This technique creates a fixed length bit strings which can be applied to Pinsketch. At the encoding stage the secret key is obtained directly from the fingerprint biometrics is bounded with the modified VNSs based

template features by a polynomial which is evaluated at all VNSs. Each VNS is protected by the secure sketch, PinSketch [9]. At the decoding stage, the secret key can be retrieved by concatenating the coefficients of polynomial.

II.RELATED WORKS

Minutiae-based VNSs provides some good features such as the Voronoi tessellation formed from the fingerprint minutiae set has local structural stability [2] and the noise affects the Voronoi tessellation only locally. It also has the advantage of being rotation, translation and distortion tolerant .Because of these characteristics VNSs are used in many fingerprint authentication systems. In [3] Khazaei et al. proposed a fingerprint matching algorithm based on Voronoi diagram. They proposed an approach of associating a unique topological structure with the fingerprint minutiae using Voronoi diagram. Using VD on the topological structure of minutiae set, results in a minutiae as vertices. In the VD diagram find a central cell and such a region is unique based on our approach. The central cell is used for local matching. This approach rejects non-similar fingerprints instantly and provides good accuracy.

Bio-cryptosystems can be classified into alignment based and alignment -free methods. One of the existing alignment-free method is five nearest minutiae based scheme [4].In this scheme translation and rotation invariant minutiae-based matching is performed in the encrypted domain. This authentication scheme is protected by Fuzzy Extractor. Arati et al introduced a new way of quantizing and digitally representing the minutiae. Here each fingerprint will be defined by the Descriptor comprising of local and global positions. Another method is the dual layer structure check scheme [5] proposed by Kai Xi et al. Here the concept of Fuzzy extractor is used to secure the secret key. Minutiae local structure features are used to eliminate the process of alignment.

The Dual layer structure check [6] algorithm is based on the minutiae local structure which helps to achieve verification accuracy. Another alignment free scheme proposed by Jiankun Hu is Delaunay Triangle based Fuzzy extractor. This technique eliminates the fingerprint registration process and they depend on error correcting codes to mitigate biometric uncertainty. Delaunay Triangulation also provides structural stability. A new Fuzzy Extractor eliminates fingerprint uncertainty and alignment process.

Fuzzy vault [7] is another cryptographic construct which protects the key as well as the biometric template. Fuzzy vault only stores the transformed version of the input so there is a need for alignment. Alignment is the process of converting one coordinate system into another coordinate. Fuzzy vault has the ability to work with unordered sets in biometrics so it is a promising solution for biometric systems. High curvature points derived from the fingerprint orientation field are used as the helper data for the purpose of alignment of template and query fingerprints.

Juels et al proposed Fuzzy Commitment scheme [8] in which user selects a message D at the encoding stage. The vector difference between the biometric X and D is denoted by t. Calculate Y=hash (D) where hash function is non-invertible. In the decoding stage with the help of biometric representation and Y+t is used to decode the closest keyword. With the help of error correcting codes the error in D' can be corrected to generate the original message D. The main disadvantage is the need for image alignment. It also requires that X and Y to be ordered so that their correspondence is distinct. In real application of fingerprint minutiae matching the extracted minutiae is unordered.

III.FUZZY EXTRACTOR

A Fuzzy Extractor [1] is a cryptographic construct which is used to obtain a unique bit string extracted from the biometric template whenever the query biometric template is close enough to the enrolled biometric template. It consists of two primitives called Secure Sketch and Strong Extractor. Secure Sketch allows the reconstruction of noisy input as follows. On input w the procedure generates some public information called a Sketch. Then given S and a value w' close to w it is possible to recover w by keeping tolerance close to the original input w. The strong extractor is used to map the non-uniform input into a uniform distributed string.

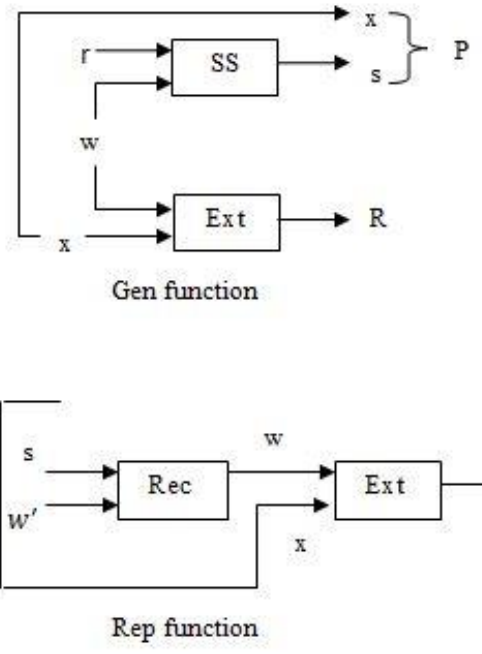

Figure 1: Gen and Rep function of Fuzzy Extractor

Let (SS, Rec) be a (M, m,$\tilde{m}$, t)- a Secure Sketch and let Ext be an average case (n,$\tilde{m}$,l,ϵ)-strong extractor. Then the Fuzzy Extractor (M, m ,l, t,ϵ) has the following properties.

1. Gen(w; r, x):set P=SS(w; r),x),R=Ext(w; x), and output (R,P)
2. 2. Rep(w', (s, x)) : recover w=Rec(w',s) and output R=Ext(w; x).

In this paper, a secure sketch construction called Pinsketch is used to construct the Fuzzy Extractor. Inputs to Pinsketch are relatively small subsets of a huge universe.

This also represents an object by a list of its features. Example includes representing minutiae in fingerprint. The distance between two set w and w' which is a subset of U is the size of their symmetric difference.

$$\text{Dis set}(w,w')=|w\Delta w'| \quad (1)$$

Pinsketch is linear over GF (2).A biometric set can be represented by its characteristics vector $x_w \epsilon \{0,1\}^u$ with 1 at positions if a is present in the universal set and 0 if a is present in the subset. The resulting construction can be applied if the symmetric difference between w and w' must has at most t elements. Pinsketch construction is based on syndrome encoding. To use it, consider the universe U as a set of strings of length α U is then identified with a non-zero elements of the field GF(2^α).The steps are illustrated below

To compute syndrome[10]

1. Set $S_i=\sum_{a\epsilon w} a^i$
2. Output SS(w)=$(S_1, S_3, S_5, \ldots S_{2t-1})$

To compute recover Rec(w', (S_1,S_3, … S_{2t-1}))

1. Compute ($S'_1, S'_3, \ldots S'_{2t-1}$)=SS($w'$)
2. $\sigma_i=S'_i-S_i$
3. Find a set V of size at most t such that Syn(x_v)=(σ_1,σ_3,…,σ_{2t-1})
4. Output w=$w'\Delta v$

IV.PROPOSED SCHEME

The entire processing flow of the proposed scheme mainly consists of six steps –Minutiae extraction, Fake Minutiae removal, formation of VNS, generation of modified VNSs, generation of fixed length bit-string representations and encrypted matching. Firstly, VNS are generated to account for small distortions since it can provide good local and global structural stability. The minutiae extraction algorithm creates a number of false or fake minutiae which can be removed by fake minutiae removal algorithm. Next the modified VNSs are created which have the properties of being reliable, distortion insensitive, rotation and translation-invariant. Thirdly, all VNSs are quantized and mapped into a pre-defined 3D array to generate fixed length bit-strings which can be directly applied to the existing secure sketch construction. Finally encrypted matching is performed using a key generated from fingerprint biometrics. During the encrypted matching, at the encoding stage, a secret key that needs protection is bound with modified VNS by a polynomial that is evaluated at all the VNSs and each VNS is protected by PinSketch. At the decoding stage, the secret key can be efficiently retrieved by sequentially concatenating the coefficients of the reconstructed polynomial if a enough number of secure sketches can be decoded.

A. Minutiae Extraction

Minutiae such as ridge ending and bifurcation are major features which can be extracted from a fingerprint by which comparisons of fingerprints can be done in an efficient manner. Minutiae extracted from any fingerprint image can be represented by a set of features m= (x, y, θ, t) where (x, y) denotes the coordinates of the minutiae point extracted, $\theta\epsilon[0,2\pi]$ is the minutia orientation and t represents the type of the minutia whether ridge ending or bifurcation.

B. Fake Minutiae Removal

After the minutiae extraction algorithm a lot of fake minutiae are produced such as broken ridge, bridge structure, short ridge structure and hole structure. These structures should be detected and eliminated if not the existence of false minutiae will increase both FAR and FRR. The following method is based on the flow of ridges and minutiae distance connectivity. Broken ridge structure creates two endpoints which can be identified by the following rules.

1. $\sqrt{(x_1-x_2)^2+(y_1-y_2)^2} < Dist_1$ (3)
2. The line formed by connecting two endpoints and two ridges connected with a minutia should flow in same direction
   $tan^{-1}\left(\frac{y_2-y_1}{x_2-x_1}\right) \simeq \frac{1}{2}(OR_A + OR_B)$ (4)
3. Two ridges should be flowing in the opposite direction and should not be connected.

Bridge structures are created due to the excessive finger pressure or noise that leads to the formation of two separate ridges. The following rules are applied to detect bridge structures

1. Consider a bifurcation point and start tracking three ridges connected to it, if one of the ridges meets another bifurcation calculates the orientation and distance between two bifurcations.
2. If the distance between two bifurcation points is less than a threshold value and the difference between the orientation and average orientation of two bifurcations must be larger than a specified angle $\frac{\pi}{4}$.

Short ridge structures are created due to the ridge segmentation and thinning. To detect short ridge structures start tracking ridges from ridge end and if it meets another endpoint or a bifurcation within a distance, two minutiae are considered to be false minutiae. Hole structure can be identified if two tracked ridges meet to form another bifurcation. Thresholds are selected adaptively to the ridge structure.

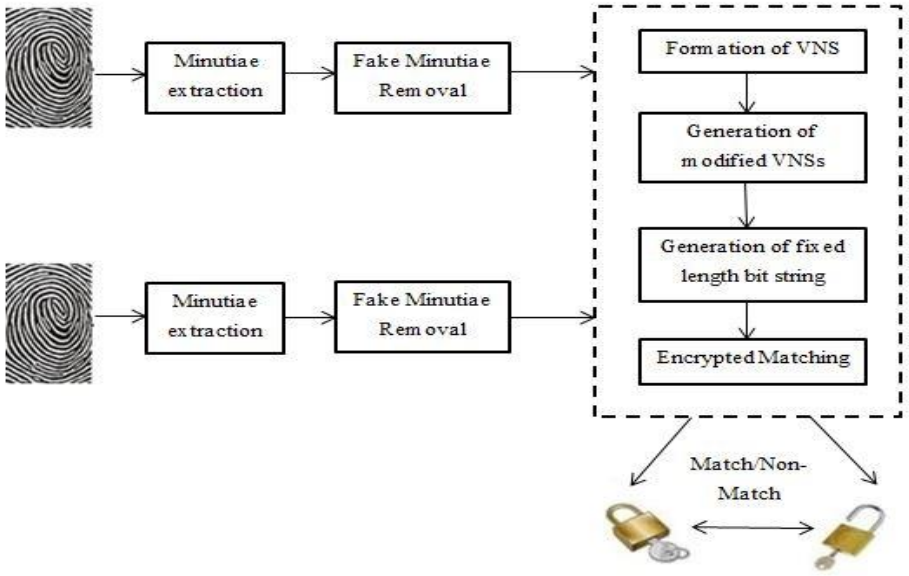

Fig. 2. Overall Processing Flow

C. Formation of VNSs

Voronoi diagram is a geometric naturalistic method to determine neighbors in a set of particles. Consider M=$\{m_1, m_2, \ldots m_n\}$ as a set of distinct minutiae in a fingerprint image and d(m_i, m_j) as the Euclidean distance between two minutiae m_i and m_j.We define the Voronoi region of a minutiae ,V(m_i) consists of all the points whose nearest minutiae is m_i.

$$V(m_i) = \{x: d(m_i, x) \leq d(m_j, x), \forall j \neq i\} \quad (5)$$

The union of the Voronoi regions of all sites represents a tessellation of the space that is called Voronoi tessellation:$V(M) = \cup_{i=1}^{n} V(m_i)$.Given a set of minutiae M=$\{m_1, m_2, \ldots m_n\}$,Voronoi tessellation partitions a whole fingerprint region that is composed of minutiae set M into many smaller regions and presents the closest neighbor structures of minutiae. With the Voronoi tessellation by connecting the centers of every pair neighboring Voronoi regions VNS can be formed.

D. Formation of modified VNSs

Modified VNSs is created to account for large distortion which alters the neighborhood structure. Even though the VNS have good local structural stability and keeps the same neighborhood structure in case of small distortion, the movement of minutiae caused by distortion should be within a small tolerance region. Construct convex quadrilateral for each missing neighbor minutia. It can be retrieved by simply flipping the shared edge of two triangles. If flipping of edges is valid the newly added minutia can be considered as the neighbor of central minutia.

E. Generation of fixed-length bit-string

Transform each VNS into fixed-length feature vectors by a method called 3D array mapping. The parameters of the 3D array include W_x ,W_y,W_z, which are length, width and height of the array. The central minutiae m_0=$\{x_0, y_0, \theta_0\}$ of each VNS is selected as reference and it is located in the center of the first layer of the 3D array. Other (k-1) Voronoi neighbor minutiae m_i'=$\{x_i', y_i', \theta_i'\}$ in the 3D array as follows:

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} cos\theta_0 & -sin\theta_0 \\ sin\theta_0 & cos\theta_0 \end{bmatrix} \begin{bmatrix} x_i - x_0 \\ -(y_i - y_0) \end{bmatrix} + \begin{bmatrix} \frac{W_x}{2} \\ \frac{W_y}{2} \end{bmatrix} \quad (6)$$

$$\theta_i' = \begin{cases} \theta_i - \theta_0 & if\ \theta_i \geq \theta_0 \\ 2\pi + \theta_i - \theta_0 & if \theta_i < \theta_0 \end{cases} \quad (7)$$

A bit-string can be obtained for the 3D array , according to the rule that if a cell in the 3D array contains the minutiae then it will be assigned 1, otherwise 0.

F. Encrypted Matching

Encrypted matching consists of encoding and decoding stages. At the encoding stage the key that needs protection is obtained from the input fingerprint image which enhances the security of the proposed work. The following steps illustrate the key generation method.

1. The extracted minutiae points are represented as:$M_P = \{m_i\} i = 1, \ldots . . NP$ (Size of minutiae set)
2. The initial key vector is defined as follows:
   $K_v = \{x_i: p(x_i)\}$ i=1… KI (Key length)
   $p(x) = M_p[I\%NP] + M_p[(i+1)\%NP]$
3. Seed value is equal to the total number of minutiae points and it is changed dynamically as follows
   $S = K_v(i)\%SI, -1, i, KI$

4. Convert initial key vector into a matrix $K_m = (a_{ij})\ KI/2*KI/2$
5. Generate intermediate key vector
$$KIV = \{K_i : m(k_i)\}$$
6. Final key vector is formed as follows
$$K_v = 1, if\ KIV[i] > mean(KIV)$$
$$= 0, otherwise$$

From the template fingerprint image T, NT local structures , $\{VNS_i^j\}_{i=1}^{NT}$ based on modified VNSs are generated and represented by their bit-string representations, $\{B\_VNS_i^j\}_{i=1}^{NT}$.An irreversible universal hash function ,H(.) is applied to each $B\_VNS_i^j$ and a hashed value set $\{H(B\_VNS_i^T)\}_{i=1}^{NT}$ is outputted. Here, $H(B\_VNS_i^T)$ is a distributed random string. The key is encoded into a polynomial P(x) of degree num by dividing it into (num+1) segments and using them as the coefficients of P(x), e.g.,$P(x) = k_{num}x^{num} + \cdots + k_0$.P(x) is evaluated at all the elements of $\{H(B\_VNS_i^T)\}_{i=1}^{NT}$ to obtain the value set $\{P(H(B\_VNS_{i=1}^T))\}_{i=1}^{NT}$.To protect the template data, each $B\_VNS_i^T$ is secured by PinSketch and the sketch data can be obtained by $SB\_VNS_i^T = SS(B\_VNS_i^T)$.The union of polynomial value set $\{P(H(B\_VNS_{i=1}^T))\}_{i=1}^{NT}$ and the sketch data set $\{SB\_VNS_i^T\}_{i=1}^{NT}$ form the lock set for the secret key and are stored for decoding.

The procedure of decoding is explained in steps as follows. In order to retrieve the encoded secret key, an unlock set which is composed of the decoded value from sketch data set $\{SB\_VNS_j^Q\}_{i=1}^{NT}$ by $\{B\_VNS_j^Q\}_{j=1}^{NQ}$ should be generated first. Specifically, the central minutiae's types of local structures, VNS_j^Q and VNS_j^T are compare firstly. If they are different a fail is reported and next decoding attempt is carried on. If they are same, both are $B\_VNS_j^Q$ and $SB\_VNS_i^T$ are inputted into the recover module, Rec of PinSketch which outputs a recovered value $Rec(B\_VNS_j^Q, SB\_VNS_i^T)$ or an error report. PinSketch has the capability of correcting t errors between two VNSs. Consider that two VNSs are matched if $N_{threshold} = \lceil k * \emptyset \rceil$ minutiae are matched between template and query. Here $\emptyset \in (0,1]$ is a similarity threshold so t=2(k-$N_{threshold}$) symmetric differences can be tolerated. $\emptyset$ is set to be 0.65 and there are k=8 minutiae in both VNS_i^T and VNS_j^Q, then symmetric difference that can be tolerated is t=6. If $dis(B\_VNS_j^Q, SB\_VNS_i^T) \leq t$, the recovered value, $Rec(B\_VNS_j^Q, SB\_VNS_i^T)$ is equal to $B\_VNS_i^T$.Otherwise, a fail will be reported if $dis(B\_VNS_j^Q, SB\_VNS_i^T) > t$ and the next decoding will continue.

If the decoding is successful the recovered value $Rec(B\_VNS_j^Q, SB\_VNS_i^T)$ is hashed using the same hash function H(.) as in the encoding stage and a hashed value is generated. The hashed value $H(Rec(B\_VNS_j^Q, SB\_VNS_i^T))$ together with and the stored corresponding polynomial equation value $P\left(H(B\_VNS_i^T)\right)$ are added into the unlock set as an element to reconstruct the polynomial P(x).At last if the number of true elements in the unlock data set is less than a predefined threshold value, then a non-match is reported. If not then the polynomial, P(x) can be correctly reconstructed by using Lagrange interpolating polynomials and the secret key can be obtained.

V.PERFORMANCE EVALUVATION

Three performance indices are used for performance evaluation: (1) false reject rate (FRR), which is defined as the ratio of unsuccessful genuine attempts to the total genuine attempts, (2) false accept rate (FAR) which is defined as the ratio of successful imposter attempts to the total imposter attempts, and equal error rate (ERR), which is defined as the error rate when the FRR and FAR are equal. In order to compare the results database is divided into one data set containing only the first and second images of each finger. For data sets that contain images 1 and 2, the first image from each finger in the data set is compared with the second image from the same finger to compute the FRR. The first image from each finger in the data set is compared with the first image from the remaining fingers in the data set to calculate the FAR. The ROC curves of this method under the parameter setting achieve the best EER performance compared to the existing scheme.

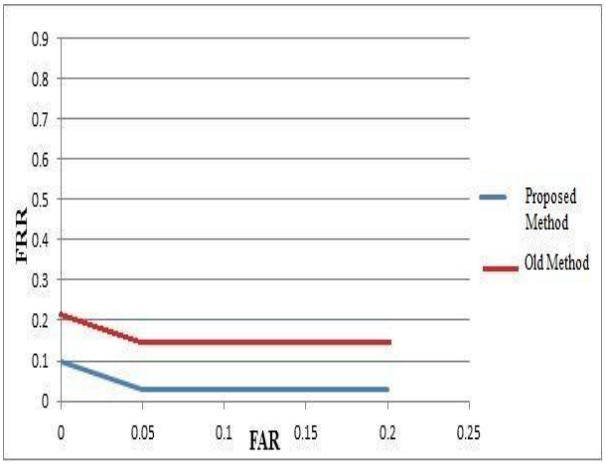

Fig. 3.Performance Evaluation graph

VI. CONCLUSION

The two challenges in bio-cryptosystem such as fingerprint uncertainty and pre-alignment are solved using this scheme. The construction of VNSs addresses the issue of fingerprint uncertainty. Another contribution of the new scheme is the Fake minutiae removal and key generation scheme directly from the biometrics. This new scheme performs better than the existing technique.

REFERENCES

[1]Wencheng Yang, Jiankun Hu, Song Wang and Milos Stojmenovic,"An Alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures "Pattern Recognition 47, 2014.

[2] A Okabe, B. Boots, K. Sugihara, S.N. Chiu, Spatial Tessellations: Concepts and Applications of Voronoi Diagrams, Wiley 2009

[3] H. Khazaei, A. Mohandas, "Fingerprint matching algorithm based on Voronoi diagram", in: Proceedings of the International Conference on Computational Sciences and its Applications (ICCSA'08), IEEE 2008, pp. 433-440.

[4] Arathi Arakala, J. Jeffers, K. Horadam, Fuzzy Extractors for minutiae-based fingerprint authentication, Advances in Biometrics (2007) 760-769

[5] Kai Xi, Jiankun Hu and Fengling Han, "An Alignment Free Fingerprint Fuzzy Extractor using near equivalent Dual Layer Structure Check (NeDLSC) Algorithm",ICIEA,pp,1040-1045,2011

[6] Wencheng Yang, J. Hu, S. Wang, "Delaunay triangle based fuzzy extractor for fingerprint authentication" Proceedings of the IEEE11th International Conference on Trust, Security and Privacy In Computing and Communications, 2012

[7] Karthik Nandakumar, Anil K. Jain, and Sharath Pankant, "Fuzzy vault implementation and performance", IEEE Transactions on Information Forensics and Security, 2007

[8] A. Juels, M. Sudan, A fuzzy commitment scheme, in: Proceedings of the 6th ACM Conference on Computer and Communications Security, ACM, 1999, pp. 28-36.

[9]Y. Dodis, L. Reyzin, A. Smith Fuzzy Extractors: How to generate strong keys from biometrics and other noisy data, Advances in cryptography-Euro crypt, Springer (2004) 523-540

[10] K. Harmon ,S. Johnson, L. Reyzin, An Implementation of syndrome encoding and decoding for binary BCH codes, Secure sketches and Fuzzy Extractors, in 2006