International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 9309-9324
© Research India Publications
http://www.ripublication.com

A Delaunay Pentangle-Based Template Protection Using Topology Code for Fingerprint Authentication and Local Registration

Suganya.A[1], Mary Amirtha Sagayee.G[2]
PG Student[1], Department of Electronics and Communication Engineering,
Parisutham Institute of Technology and Science, Thanjavur, Tamilnadu, India.
E-mail: suganganth@gmail.com
Professor[2], Department of Electronics and Communication Engineering,
Parisutham Institute of Technology and Science, Thanjavur, Tamilnadu, India.
E-mail: gmasagayee@gmail.com

Abstract

This paper presents design and implementations of Delaunay pentangle based fingerprint authentication system for enhancing the security level of biometric template data and withstand local structural change in presence of nonlinear deformity. Feature vector extracted from the Delaunay pentangle is of fixed length and alignment free is less sensitive and more discriminative to nonlinear distortion. Additionally, it is being proposed to construct a unique topology code from each and every Delaunay pentangle to carry through accurate local registration. The proposed topology code not only that helps to carry through accurate local registration and also it improves the security level of biometric template data. The proposed Delaunay pentangle based structure has more attributes and also more discriminating abilities than existing Delaunay quadrangle based structures. Moreover, the proposed system promised two layer of security protection to template data. Experimental results on three public databases of FVC2002 DB1, DB2 and DB3 using Delaunay pentangle based structures with topology code can achieve better performance and higher security level than Delaunay quadrangle based structures. The performance of proposed system certificate low FRR= 1.4%, FAR = 0% and EER = 0.74% on FVC2002 DB2 than existing system. So, this proposed Delaunay pentangle based fingerprint authentication with topology code shows superior performance than Delaunay quadrangle based structures and Delaunay triangle based structures.

Keywords: Delaunay pentangle, Quantization operator, Pinsketch and Topology code.

Introduction

A. Biometrics

Biometric is an automated methodology to uniquely identify human based on a physiological and behavioural characteristics. Many biometric characteristics have been proposed for authentication purpose. Consistently, biometric method can be pronounced into two types: behavioural-based method and physiological based method.

In behavioural based method perform task of authentication based on human behavioural Characteristics. The major issue with behavioural based method is not unique, they all have more variation, cannot cope with and difficult to measure because of influences such as stress, thrust or stain. But the Implementation of behavioural based method less cost.

Physiological-based method perform authentication by means of his and her physiological characteristics. The advantages of the physiological based method are more stable and more invasiveness and rare hacking only than behavioural based method.

B. Fingerprints

In the world of biometrics one of the most invasiveness and mature biometric recognition owning to the more Distinctiveness and stability that using fingerprint based authentication can provide better performance compare to other method. Fingerprint biometrics method can be classified into two types are texture and ridge feature based, method compare to texture based, ridge feature based method has more social acceptability and more reliable. Fingerprint identification system represents fingerprints in terms of their feature points. The two popular eminent minutiae points are termination and ridge bifurcation. Once the minutiae points are extracted from fingerprints and then Delaunay pentangle structures can be generated from feature points easily.

Table 1: Comparison between Delaunay Pentangle and Delaunay Quadrangle.

Parameter	Delaunay Pentangle	Delaunay Quadrangle
Attributes	It has more aspects (e.g., five edges and five angles).	Quadrangle has less aspects (e.g., four edges and angles) than Pentangle
Topology code	Five topology codes can be extracted from Delaunay pentangle for better local registration.	From Delaunay Quadrangle based structure, they extract only four topology code.
Security	Very high	Very high

Related Work

In [10] Bebies et al. proposed index based approach and Delaunay triangulation. The index based approach for fingerprint identification and Delaunay triangulation for extracting unique topology code. The leading demerit of this approach is local structures changed in presence of noise or distortion. In [3] Amirani et al. combined both Delaunay triangulation and voronoi diagram to generate hybrid matching algorithm. In [3], [8] Delaunay triangle based structure has proved some excellent Characteristics. Firstly, it provides excellent structural stability under random positional disruptions [9] each minutia likely to maintain a similar structure with its neighbouring minutiae under translation, rotation and small scale change because of nonlinear distortion.

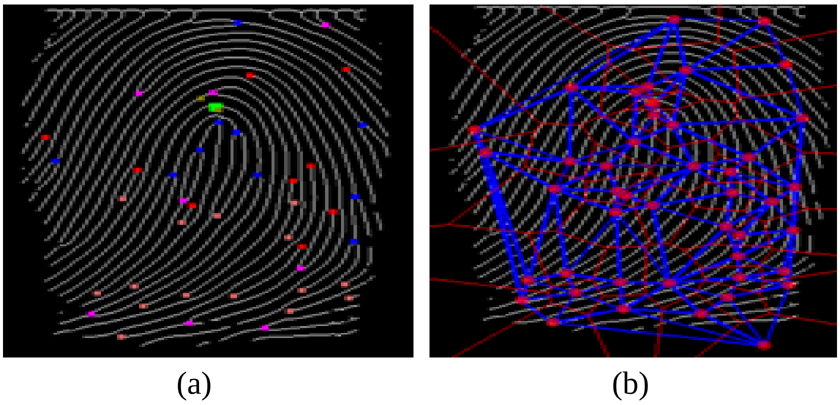


Figure 1: Examples of (a) set of minutiae points, (b) Voronoi diagram (lean line) and Delaunay triangulation (thick line).

Secondly Delaunay triangulation is influenced locally by virtue of missing and spurious minutiae. which means that by reason of random positional disturbances, some part of Delaunay triangulation can still maintain structural stability[6] [19].figure 1(a) shows a number of minutiae points and figure 1(b) gives the Delaunay triangulation net (bold line) and voronoi diagram (thin line) formed by minutiae (feature) points. To find the nonlinear deformation of fingerprints cappelli et al. [2] proposed elastic deformity of fingerprints. Firstly described three region of distinguishable in fingerprint images and used some distortion variable for describe the distortion mechanism. The Delaunay quadrangle-based structure has some excellent characteristics [1]. Firstly, it has good Structural stability under nonlinear distortion. Provide guaranteed fixed length, alignment free feature, but it has only less attributes than pentangle and less security because topology code less than Delaunay pentangle.

D. Template Protection Method

During image acquisition uncertainty of fingerprint caused by nonlinear distortion is one of issues in biometric system. Template protection is another necessary issue that needs more attenuation. Template are stored in database compare with query image for identify individual [11], [3]. Two major secure protection biometric techniques are cancellable and cryptosystem for biometric templates. In cancellable biometrics [4] [5], original template features are transformed into new format by non invertible transformation function at the enrolment stage. In authentication moment also adoption the same non invertible to query features. In this case performed matching between template and query images rather than original images. Hence original template features are concealed and protected. The main demerits of cancellable biometrics only provide the matching/non-matching sign.

In [5] cancellable fingerprint template created by authors in the form of binary string for avoid the registration and computationally infeasible of fingerprint minutiae to recover original minutiae data. In biometric cryptosystem, for extract security key from biometric features either technically or directly. The pinsketch [10] is real biometric template features are encrypted by secure sketch provides the helper data. In this case the helper data encrypted by non-reversible process. To obtain original template features from helper data is computationally complex.

E. Delaunay Triangles Based Structural Change Because of Non-Linear Distortion

None of the afore-hand work, the local Delaunay triangle based structural change by reason of distortion. Figure 2 gives an example of local Delaunay structural change on account of distortion. If distortion appear in the local Delaunay structures that transfers minutiae point d inside the tolerance area, convex pentangle of P(abcde) occupied triangles, T(abe), T(bde) and T(bcd) could not change in this Case, as show in figure 2(a). Nevertheless, if distortion transfers minutiae point d out of tolerance area, pentangle P(abcde) occupied triangles T(abe), T(bde) and T(bcd) will be interchanged into T(abc), T(ace) and T(cde) as show in figure 2(b). We assume that the convex pentangles in figure 2(a) and 2(b) are template and query image respectively.

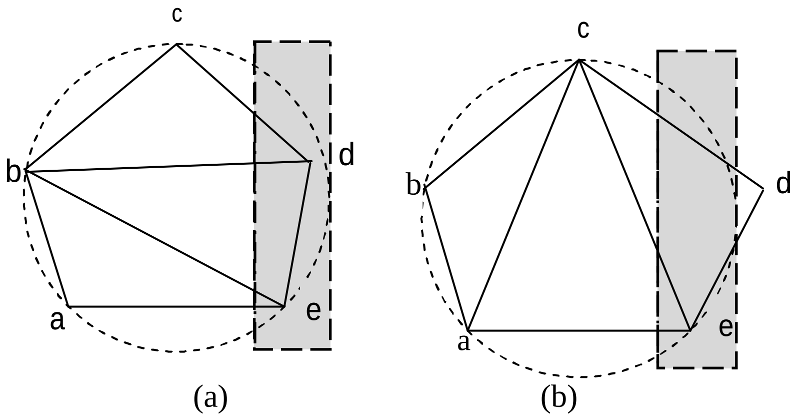


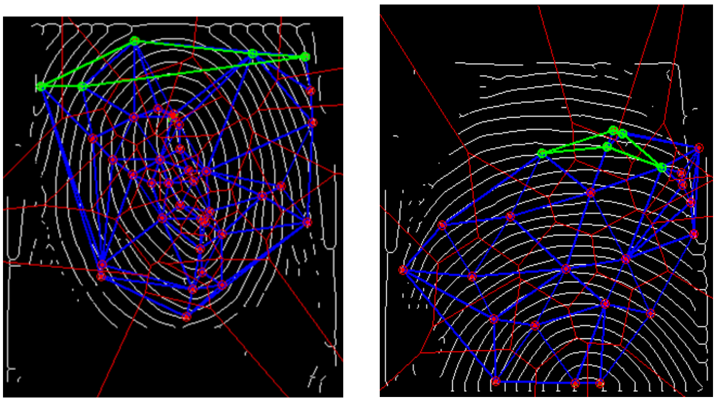
Figure 2: Local Delaunay structural changes under nonlinear distortion: (a) feature point ‘d’ moves inside the tolerance area, (b) feature point ‘d’ moves out of the tolerance region.

In this case, during matching process template image of triangles, T(ace), T(bde) and T(bcd) not match with query image of triangles T(abc), T(ace) and T(cde). So tolerate this issue, we proposed quantization operator. It is only retaliation to small scale variation.

Proposed Method

The objective of this proposed Delaunay pentangle based fingerprint authentication systems to tolerate the local structural change in presence of nonlinear distortion, suffered by Delaunay triangle based structure under nonlinear distortion and also to provide double layer of secure protection for template data by using fuzzy vault and pinsketch for authentication purpose. Unique topology code procured from Delaunay pentangle is of fixed length and alignment free. It is used to carry out precise local registration under distortion and also improves the security level of biometric template data. In figure 3 shows on example of Delaunay pentangle based structure (bold line) don't alter but Delaunay triangle based structures altered under distortion.

Delaunay pentangle is built upon the construction of Delaunay triangulation net. The algorithm for producing Delaunay triangulation is detailed in [18]. Here we given a set of minutiae $M = \{m_i\}i^{N}=1$, Where N is a set of minutiae, as showed in figure 3. In order to construct Delaunay triangulation, first need to construct voronoi diagram. The role of voronoi diagram split entire region into small region based on minutiae points in the images. All the points in the cell around m_i or closure to m_i than to any other minutiae. After that the Delaunay triangulation is formed by joining the centre of every pair of neighbouring in voronoi region. Next Delaunay pentangle can be formed by combining any three Delaunay triangles. The user specified seed key bound from topology code for security enhancement and Secrete key is extracted from pentangle features. This proposed system occupy two stages are enrolment and verification, if both stage feature points, topology code and secrete key same the person allow to access control otherwise not allowed.



101-1(impression) 101-2(impression)

Figure 3: Delaunay pentangle based structures from FVC2002 DB2 101-1, 2 impressions.

Proposed Delaunay pentangle based fingerprint authentication provides better matching accuracy of 99% in FVC2002 DB2.

A. Topology Code for Local Registration

Finger print image registration is a critical process in fingerprint matching. The fingerprint registration fortunately takes place in the encrypted domain. This is because for fingerprint authentication system with template protection, the original template features are not available to compute the alignment parameters. For instance, reference points, e.g., singular point, are usually used as the reference to establish a rotation and translation relationship between query and template images; however, the reference point exposure during the alignment procedure would leak important information about the fingerprint data, thus weakening the security of the associated fingerprint authentication system.

The proposed Delaunay pentangle-based structure can avoid this global image registration process because only local registration is needed by using local minutiae information. For example, there is a pair of corresponding Delaunay pentangle, *P (ABCDE)* and *P (A'B'C'D'*E'*)* from the template and query images, respectively. The key to matching *P (ABCDE)* with *P (A'B'C'D'*E'*)* is that *P (A'B'C'D'*E'*)* has to be correctly aligned with *P (ABCDE).* Assume that the points *A, B, C, D E* in *P(ABCDE)* are corresponding to points *A'B'C'D'*E' in *P(A'B'C'D'*E'*),* respectively, and that the feature extraction procedure starts from point *A*, the vertex angle of small, in *P (ABCDE)* and then moves to point *D* in the clock-wise direction. In this case, the correct local registration is about precisely finding *A*'s corresponding point *A*' in *P (A'B'C'D'*E'*).* A straightforward method is to search the vertex of the minimum angle from *P(A'B'C'D'*E'*)* and consider it as the starting point of the pentangle P(A'B'C'D'E').

This method, which uses an absolute geometrical measurement, is worth only when no structural change happens. Unfortunately, nonlinear distortion caused by elastic finger skin always exists in fingerprint images, thus structural change is unavoidable. Distortion may occur the genuine corresponding angle A of the smallest angle A in P (ABCDE) to be the second smallest angle in P(A'B'C'D'). As a result, point B' would be not correctly chosen as the starting point of P(A'B'C'D'E'). Then, the matching result between P (A B C D E) and P (A'B'C'D'E') would definitely be negative because the corresponding attributes (e.g. edge length, orientation of minutiae) of these two Delaunay pentangles are different. From the above analysis, we can see that using absolute geometrical measurement in deciding a starting point under distortion is inaccurate.

Naturally, the quantization operation is expected to solve this issue because it can make angle values insensitive to small-scale differences and assign same symbols to those angles that are located in the same range. The value of an angle in a Delaunay pentangle is in the range of 0 to 2π. Assume the quantization step size is $ss_{tc} = \pi/6$ and the quantized angle value is expressed as a binary string of m_{tc} bits or an integer ranging from 0 to 2^{m}tc , then the first two smallest angles, A and B, in P(ABCDE) are both quantified into the same integer value '2' or '0010' in a binary form(0,1). Similarly, A' and B' in P (A'B'C'D'E') are also quantified into the same value '2' or '0010' in a binary form. We use the different values in the remaining part of the paper unless stated otherwise. In this way, point B' won't be chosen for the starting point of the Delaunay pentangle P (A'B'C'D'E') However, other issue arises from this

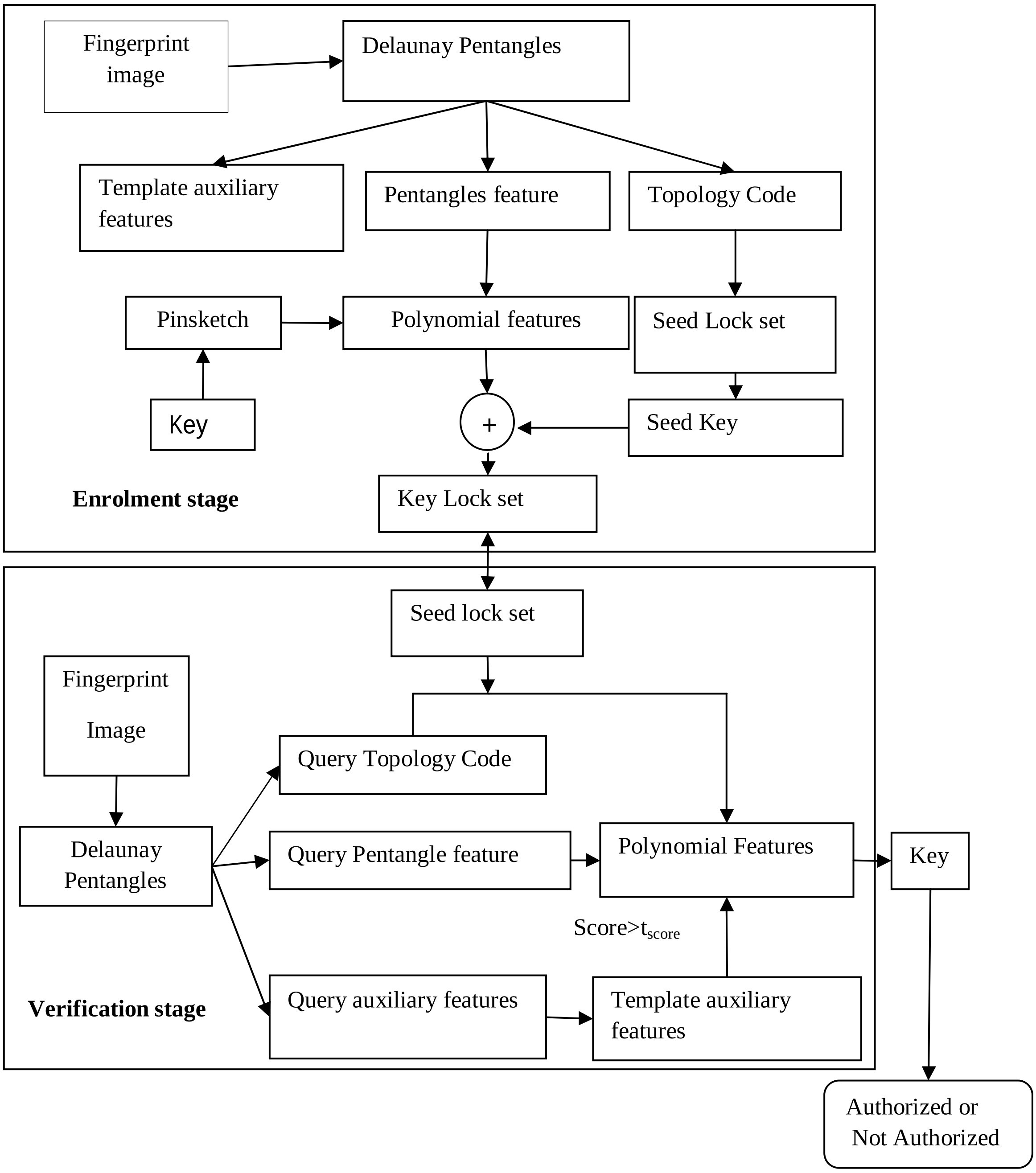
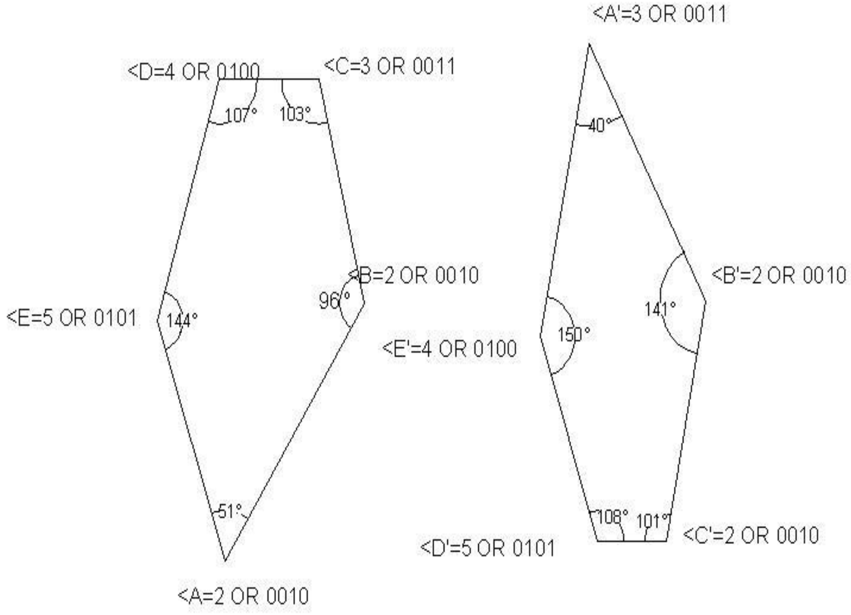


Figure 4: Architecture of Delaunay pentangle based structure.

Treatment. Since the values of the first two smallest angles, A and B, after quantization, are both denoted by the same integer value ‘2’, which point should be considered as the starting point. The angles, A, B, C, D, E of P(ABCDE) are quantified into ‘2’, ‘2’, ‘4’, ‘5’,’6’ respectively. We discover that, by changing the starting point from A to E and counting the quantized angle values in clock-wise direction sequentially, five different code strings 2-2-3-4-5, 2-3-4-5-2, 3-4-5-2-2,



(a) (b)

Figure 5: Corresponding Delaunay pentangles P(ABCDE) and P (A' B' C' D' E') in (a) the template image & (b) the query image.

4-5-2-2-3 and 5-2-2-3-4, can be generated. Likewise five different code strings 2-2-3-4-5, 2-3-4-5-2, 3-4-5-2-2, 4-5-2-2-3 and 5-2-2-3-4 can also be produced for P (A'B'C'D'E'). The equation (1) using us to find the starting point of Delaunay pentangle in local registration. So make each pentangle correspond to a descriptor of individual, equation use from [11] as follows.

$$TC= P_1\times\Gamma^4 +P_2 \times\Gamma^3+P_3 \times\Gamma ^2+P_4\times\Gamma^1+P_5 \times\Gamma^0 \qquad (1)$$

Where $\{pi\}_{i=1}^{5}$ are the quantized angle values of the Delaunay pentangle and Γ =max(p1, p2, p3, p4,p^5) + 1. Using equation (1), we calculate a value for each of the five code strings and choose the smallest value to be the descriptor of the Delaunay pentangle under consideration. The descriptor founded by equation (1) is very unique. Since the descriptor TC describes the shape feature of the Delaunay Pentangle, because we call it topology code in this paper.

According to the topology code TC generation norm, each Delaunay pentangle can be inscribed by an isolated value. For example, it refers from equation (1) that the resulting values of the five code strings, 2-2-3-4-5, 2-3-4-5-2, 3-4-5-2-2, 4-5-2-2-3 and 5-2-2-3-4, from P (ABCDE) are 3161, 3413, 4946, 6351 and 7006 respectively. Hence, the minor value 3161, which correlates to the starting point of A, is chosen as the topology code of P (ABCDE). Likewise, the topology code of P (A'B'C'D'E') is also calculated to be 3161, which is corresponding to the starting point A'. The starting points A of P (ABCDE) and A' of P (A'B'C'D'E') are just the correct corresponding points that we need to find. By this means, accurate local registration is achieved and the mistake that point B' is considered as the starting point of P (A'B'C'D'E') by using the absolute geometrical measurement can be avoided.

B. Invariant Feature Extracted From Delaunay Pentangle

A number of invariant features can be extracted from Delaunay pentangle for increasing reliability of fingerprint Matching. Some invariant features are Translation, Rotation, Invariant local features of Delaunay pentangle. Totally 25 = (5×5) invariant features can be extracted from Delaunay pentangle. The invariant features extracted from Delaunay pentangle, a certain extent of deformity should be admitted due to the elasticity of the finger skin.

C. Auxiliary Feature Extracted from Delaunay Pentangle

Auxiliary feature extracted from each Delaunay pentangle for increasing discriminative ability of system. In that, to be specific, initially we need to find the centre points of each Delaunay pentangle and that is considered as a reference point of polar correlate space. This features also used to reduce the non linear distortion effects.

Two auxiliary features similarity can be acquired from equation (2),

$$score\left(a_{f_i}, a_{f_j}\right) = \frac{\sum_{k=1}^{L_{af}}\left(a_{f_{i,k}} - \overline{a_{f_i}}\right)\left(a_{f_{i,k}} - \overline{a_{f_j})}\right)}{\sqrt{\sum_{k=1}^{L_{af}}\left(a_{f_{i,k}} - \overline{a_{f_i}}\right)^2 \sum_{k=1}^{L_{af}}\left(a_{f_{j,k}} - \overline{a_{f_j}}\right)^2}} \tag{2}$$

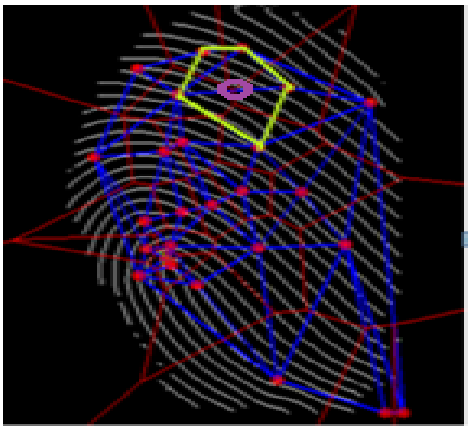


Figure 6: An example of Delaunay pentangle based auxiliary features point.

D. Pinsketch

In this paper, we also propose to construct pinsketch techniques for recover biometric template data and in the meanwhile, to provide secure protection of template data. We give below a brief construction of pinsketch, which contains two models, are Encode and Decode modal.

1. Encode Model:

Let assume that ω be a template feature vector that need protection in that apply secure protection ss(.) to template data is ss(ω). It will provide helper data for verification stage. ss(ω) is expressed as

$$ss\,(\omega) = syn(\omega) = (s_{1,}\, s_{3,\ldots}s_{2t-1}) \tag{3}$$

2. Decode Model:

Let assume that $\omega^{'}$ be a query feature vector is give into recover module with helper data for extract original key from helper data. To extract the original key from helper data by using irreversible encryption process proposed. $ss(\omega^{'})$ is computed by

$$ss(\omega^{'}) = syn(\omega^{'}) = (s^{'}_{1,} s^{'}_{3....} s'_{2t-1}) \quad (4)$$

After that distinguish between $ss(\omega)$ and $ss(\omega^{'})$ is computed as,

$$syn(\lambda) = ss(\omega) - ss(\omega')$$

$$= (s_1 - s_1^{'}, s_3 - s_3^{'}, s_5 - s_5^{'}, \dots, s_{2t-1} - s_{2t-1}^{'}) \quad (5)$$

Next the ω can be computed from recover module expressed as,

$$\omega = Rec(\lambda, \omega') = syn(\lambda) + syn(\omega') \quad (6)$$

E. Enrolment stage

In the enrolment stage, a security key K that needs protection is professionally bounced with template features which are protected by pinsketch. The procedure of enrolment stage is shown in figure 4. The detailed steps are explained below:

1. Given template fingerprint image, template auxiliary features, template pentangle features and template topology code is acquired from template fingerprint image by using the approach described in section 2.
   The user specific secrete key k that require protection is technically bounce with the template feature set. To be specific, it is encoded into a polynomial p of degree n by dividing it into (n+1) segments using as the coefficient of p, $p(x)=k_n x^n+\dots+k_1 x+k_0$[12][13]. The p is assessed at all the elements in the feature sets. To protect the feature sets, the sketching procedure ss(.) is applied to each element in sketch data, which output some helper data, the helper data for verification stage.
2. In order to further enhancing the security level of system, a security enhancement method using topology code set is applied to each sketch data [13]-[17], [20]. A user specific seed value K_{tc} is derived from topology code set by using the polynomial p of degree of n. The topology code derived from Delaunay pentangle using the scheme described in section 2.
3. K_{tc} react as a seed to a hash function (.) that generate two binary strings CS_1^T and CS_2^T of same length. The random binary string CS_1^T is XORed with sketch data. To generate security enhanced sketch data, where the helper data has been hidden. The same CS_2^T also XORed with each element to generate a secure data set. Alternatively storing the original feature set, a double secret key lock set is applied to template feature set is stored in the database and the original template data is destroyed. By this means template protection is achieved.

F. Verification stage

In the verification stage enough sketch data from key lock set can be decoded, the secret key K can be retrieved by reconstructing the polynomial P. The procedure of verification stage is shown in figure 4. The detailed steps are explained below:

1. Given query fingerprint image, query auxiliary features, query pentangle features and query topology code is acquired from query fingerprint image by using the approach described in section 2.
2. To retrieve the secret key K, a sufficient number of elements should be decoded from the secured key lock set. Since the key lock set are encrypted by random binary string CS_1^T and CS_2^T generated from seed K_{tc}, it should be retrieved first. The retrieval process of K_{tc} is similar to the fuzzy vault decoding procedure [17].
3. The restored seed k'_{tc} is applied to the same hash function hash(.) used in the enrolment stage, outputting binary strings are further XORed with the security enhanced sketch data's, to generate the recover helper data set and polynomial value set. For each element, we check whether the element from the query feature set can decode or it. First, the similarity between af_i and af_j is checked. If the similarity score score(af_i af_j) is less than the threshold t_{score}, then next matching attempt will be carried on; other recover helper data, further inputted into the recover module Rec(.) of pinsketch, which output a recovered value.
4. Step 3 is repeated until matching between all the elements in template and query feature sets is carried out. All the recovered feature data and their corresponding polynomial values in the form of key unlock set. Then the polynomial P can be reconstructed by Lagrange interpolation and the secret key k can be retrieved sequentially concatenating the (n+1) coefficients.

G. Security Analysis

The proposed system protected by two layers, pinsketch (similar to fuzzy vault techniques) is the first security layer; it can be extracted from min entropy feature vector. Code offset construction equal to pinsketch construction. Min entropy of pinsketch can be expressed as

$$E_{ps} = \log (\frac{(2^{L_q - i})}{\binom{L_q - i}{t_{ps}}} \tag{7}$$

Second layer of security provided to proposed system by topology code set helps to bind seed (k_{tc}) using fuzzy logic techniques. The seed can be computed as

$$E_{tc} = -\log (\frac{\binom{N_{tc}}{n+1}}{\binom{N_{tc}+N_{cf}}{n+1}} \tag{8}$$

Hence the proposed feature points can be protected by two layers.

Experimental Results

To evaluate the performance of proposed system on three publicly available databases are FVC2002 (DB1, DB2 and DB3) with the 1VS1 protocols. Comprehensive information on all three databases is shown in Table I. The Matlab software was used to extract minutiae in fingerprint images. In this paper, proposed small quantization step size increases sensitivity to modest distortion, while large quantization step size is not discriminative sufficient.

Table 2: Information about the FVC databases Used in Proposed System Experiments

Parameter	**2002DB1**	**2002DB2**	**2002DB3**
Resolution	500dpi	569 dpi	500dpi
Number of fingers	10	10	10
Number of images per finger	8	8	8
Sensor type	Optical sensor	Optical sensor	Capacitive sensor
Image size	388x374	560x296	300x300
Image quality	Medium	Medium	Medium – Low

A. Performance Evaluation

To evaluate the performance of the Delaunay pentangle based fingerprint authentication system, there are utilized three indicants performances: (1) false reject rate (FRR), which is defined as the ratio of unsuccessful genuine attempts to total genuine attempts, (2) false accept rate (FAR), which is defined as the ratio of successful impostor attempts to the total impostor attempts, (3) equal error rate (EER), which is defined as the error rate when FAR and FRR are equal.

On all the three databases the 1VS1 protocol are involved. According to the norm of this 1VS1, we set the 1st image from each finger in the dataset as the template image and compare it with 2nd image from same finger in the dataset as the query image to calculate the FRR. To calculate FAR, we set the 1st image from each finger as the template image and it compare with 1st image from remaining finger as the template image. In order to avoid correlation, if x image has been matched with y image and then the comparison of symmetric in not executed. The standard 1VS1 protocol contains eight impressions per finger, but only using first two impressions for matching purpose, because 1st two impressions restrain only less distortion and variations. Consequently using the 1VS1 protocol results in 10 genuine matching attempts and ((10×9)/2) = 45 imposter matching attempts for each of databases of FVC2002DB1, DB2 and DB3.

B. Performance comparison of two different structures

In order to evaluate the effects of Delaunay pentangle based fingerprint authentication system with topology code, we compared and tested with two different structures (1) Delaunay quadrangle based structures with topology code for local registration, and (2) Delaunay pentangle based structures with topology code for local registration, in FVC2002 DB2 databases by using 1VS1 protocol.

The performance comparison with two different structures is illustrated in figure 8. It can be observed from figure 8. The Delaunay pentangle based structure with topology code (EER=0.71%) exhibits the best performance compare to Delaunay quadrangle with topology code (EER=1.02%).This

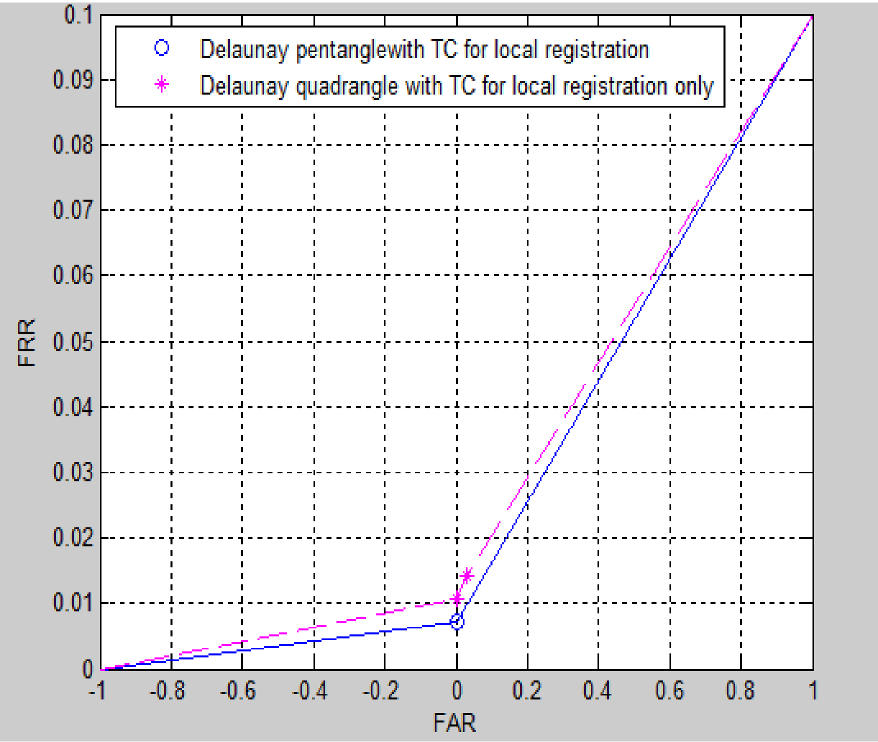


Figure 7: Performance comparison of two different structures on database FVC2002 DB2.

Proves that the Delaunay pentangle is more stable than Delaunay quadrangle and feature extracted from Delaunay pentangle is more discriminative than Delaunay quadrangle because it has richer characteristics. Under the topology code used in both structures, which is summarized by Delaunay pentangle EER = 0.71% with topology code, Delaunay quadrangle EER =1.02%, compare with Delaunay quadrangle EER = 1.67% without topology code.

C. Performance Evaluation with three public databases

We evaluate the performance of proposed system using 1VS1 protocol of FVC2002 (DB1, DB2 and DB3). To represent features by using these three databases based on Delaunay Pentangle with topology code for local registration and improving security. Performance over three databases used in proposed system varies because these three databases contain different image quality as shown in table 2. Three databases composed 80 fingerprint images from 10 different fingers, i.e. eight impression per finger. Performance of the proposed system lower in database FVC2002 DB3 compare to other two biometrics used in our proposed system such as, FVC2002 DB1, FVC2002 DB2. Proposed system recognition performance degraded in three proposed databases because of poor image quality.

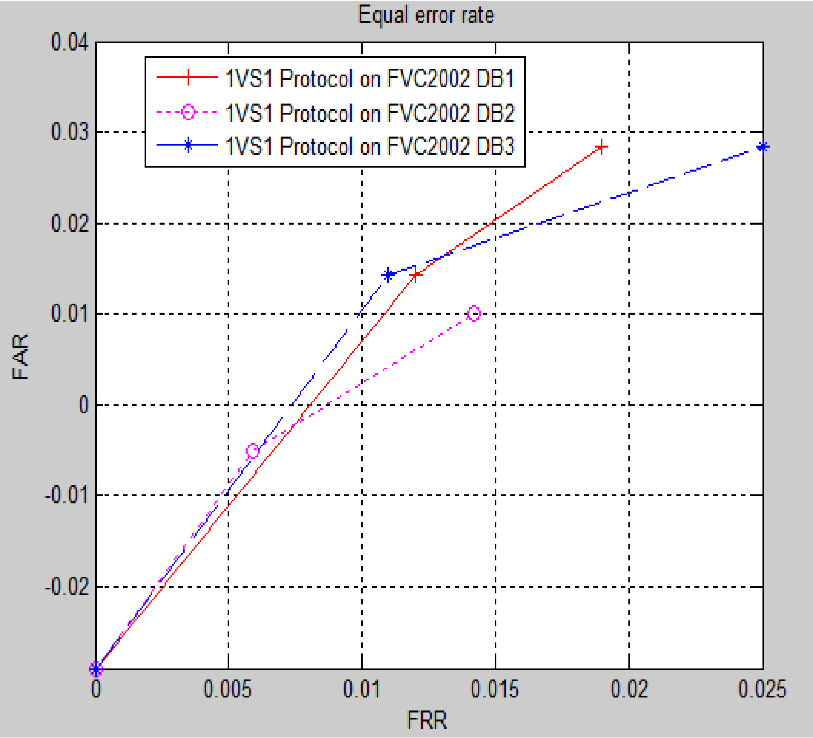


Figure 8: Performance of the three different of 1VS1protocol used in proposed method.

The proposed system perform best on FVC2002 DB2 (FAR=0%, FRR=0.71%); with the 1VS1 protocol, FVC2002 DB1 (FAR=0% FRR=2.8%) and FVC2002 DB3 (FAR=1.1% FRR=2.8%) as shown in table 3. The performance of this proposed system is mainly degraded because of lower image quality. Security of the proposed system is provided by double layer of protection, topology code and pinsketch.

Table 3: Performance Analysis Of 1VS1 Protocol Used In Proposed Method (Values In Percentage).

Method	**2002DB1 EER (FRR/FAR)**	**2002DB2 EER (FRR/FAR)**	**2002DB3 EER (FRR/FAR)**
Li et al.	-	(7/0)	-
Kai et al.	-	4.5	-
Wencheng yang et al.[1]	(4/0)	1.02	8.63
Proposed method incorporating Topology code for local registration.	(2.8/0) 1.42	0.71	1.95

Conclusion

In this paper, we propose a Delaunay pentangle based fingerprint authentication system to withstand local structural change under non linear distortion. We have extract three feature set from Delaunay pentangle based structures are: (1) Auxiliary feature to increase discriminative ability of the proposed system; (2) Extract secrete key from Delaunay Pentangle that needs protection, by using pinsketch for providing security protection to template data; and (3) Extract five topology code to provide security production for template protection another benefit of the topology code to achieve accurate local registration in presence distortion. We conclude that our proposed system assurance double layer of secure protection to template data and also Delaunay pentangle can assist in accomplishing best local registration under non linear distortion because Delaunay pentangle has more stable and robust than Delaunay quadrangle based method. Experimental results report that proposed system EER = 0.71% FAR = 0% FRR = 1.42% than other biometric methods. Future work, the proposed method will be tested with other biometric templates especially palm print. Since palm print has less intrusive and more social acceptability and high accuracy than other biometrics.

Acknowledgement

I would like to thank my guide Dr. G. Mary Amirtha Sagayee, Professor, Department of Electronics and Communication Engineering, Parisutham Institute of Technology and Science, Thanjavur for her help and guidance to enable me to propose this system.

References

[1] W.Yang, J. Hu, and s.wang, “Delaunay quadrangle based fingerprint authentication system with template protection using topology code for local registration and security enhancement” Inform. forensics and security, vol. 9, no. 7, pp.1556-6013, July 2014.

[2] R.Cappelli, D. Maio, and D. Maltoni, “Modelling plastic distortion in fingerprint images,” in Proc. ICAPR, 2001, pp. 369-379.

[3] F. Farooq, R. M. Bolle, T. Y. Jea, and N. Ratha, “Anonymous and revocable fingerprint recognition,” in Proc. IEEE CVPR Conf., Jun. 2007, pp. 1–7.

[4] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” SIAM J. Comput., vol. 38, no. 1, pp. 97–139, Sep. 2008.

[5] W. Yang, J. Hu, S. Wang, and J. Yang, “Cancelable fingerprint templates with Delaunay triangle-based local structures,” in Cyberspace Safety and Security. New York, NY, USA: Springer-Verlag, 2013, pp. 81–91.

[6] W. Yang, J. Hu, and S. Wang, “A Delaunay triangle-based fuzzy extractor for fingerprint authentication,” in Proc. 11th Int. Conf. Trust, Security Privacy Comput. Commun., 2012, pp. 66–70.

[7] G. Parziale and A. Niel, “A fingerprint matching using minutiae triangulation,” in Proc. Biom. Authenticat., 2004, pp. 241–248.

[8] R.Soleymani and M.C. Amirani, “A hybrid fingerprint matching algorithm using Delaunay triangulation and Voronoi diagram,” in Proc.20th ICEE, 2012, pp. 752–757.

[9] A. A. Khanban and A. Edalat, “Computing Delaunay triangulation with imprecise input data,” in Proc. 15th Can. Conf. Comput. Geometry, 2003, pp. 94–97.

[10] G. Bebis, T. Deaconu, and M. Georgiopoulos, “Fingerprint identification using Delaunay triangulation,” in Proc. Int. Conf. Inform. Intell. Syst., 1999, pp. 452–459.

[11] M. Abellanas, F. Hurtado, and P. A. Ramos, “Structural tolerance and Delaunay triangulation,” Inform. Process. Lett., vol. 71, nos. 5–6, pp. 221–227, Sep. 1999.

[12] J. P. Berrut and L. N. Trefethen, “Barycentric lagrange interpolation,” SIAM Rev., vol. 46, no. 3, pp. 501–517, 2004.

[13] K. Nandakumar, A. Nagar, and A. Jain, “Hardening fingerprint fuzzy vault using password,” in Proc. Int. Adv. Biometrics Conf., 2007, pp. 927–937.

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

[15] A. Juels and M. Wattenberg, “A fuzzy commitment scheme,” in Proc. 6th ACM Conf. Comput. Commun. Security, 1999, pp. 28–36.

[16] A. Juels and M. Sudan, “A fuzzy vault scheme,” Des., Codes Cryptogr., vol. 38, no. 2, pp. 237–257, 2006.

[17] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” SIAM J. Comput., vol. 38, no. 1, pp. 97–139, Sep. 2008.

[18] D.-T. Lee and B. J. Schachter, “Two algorithms for constructing a Delaunay triangulation,” Int. J. Comput. Inform. Sci., vol. 9, no. 3, pp. 219–242, 1980.

[19] A. A. Khanban and A. Edalat, “Computing Delaunay triangulation with imprecise input data,” in Proc. 15th Can. Conf. Comput. Geometry, 2003, pp. 94–97.

[20] H. Chen, “A novel algorithm of fingerprint encryption using minutiae-based transformation,” Pattern Recognit. Lett., vol. 32, no. 2,pp. 305–309, Jun. 2011.