© 2018 IJSRSET | Volume 4 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Fingerprint Cryptosystem Based on Delaunay Quadrangle

P. Chandana, T. Sreenivasulu Reddy
Department of Electronics and Communication Engineering, S V U College of Engineering, Sri Venkateswara University, Tirupati, Andhra Pradesh, India

ABSTRACT

Arrangement free unique finger impression cryptosystems perform coordinating utilizing relative data between particulars, e.g., neighborhood details structures, is promising, in light of the fact that it can keep away from the acknowledgment blunders and data spillage caused by layout arrangement/enrollment. Be that as it may be the most nearby details structures just contain relative data of a couple of particulars in a neighborhood area, they are less discriminative than the worldwide details design. In this paper, we propose an arrangement free fluffy vault-based unique mark cryptosystem utilizing quadra angle based structure . The proposed quadrangle-based structure can endure the nearby basic change endured by the triangle-based structure under nonlinear contortion, as described .Generally, the elements extracted from the proposed quadrangle-based structure are more discriminative than those from the triangle based structure. This is an account of a quadrangle has more characteristics (e.g., one more edge and point) than a triangle.

Keywords: Quadrangle, Triangle Based Structure, Cryptosystems, Fluffy-Vault Based Unique Mark Cryptosystems

I. INTRODUCTION

Fingerprint recognition (identification) is one of the oldest methods of identification with biometric traits. Large no. of archeological artifacts and historical items shows the signs of fingerprints of human on stones. The ancient people were aware about the individuality of fingerprint, but they were not aware of scientific methods of finding individuality. The first challenge facing a finger-scan system is to acquire a high-quality image of the fingerprint. Image quality is measured in dots per inch (DPI) - more dots per inch means a higher-resolution image. Today‘s finger-scan peripherals can acquire images of 500 DPI, the standard for forensic-quality fingerprinting. The lowest DPI generally found in the market is in the 250- to 300-DPI range. Example fingerprint with different DPI Image acquisition is a major challenge for finger-scan developers, because fingerprint quality can vary substantially from person to person and from finger to finger. Some populations are more likely than others to have faint or difficult- to-acquire fingerprints, whether due to wear and tear or physiological traits. In addition, environmental factors can impact image acquisition. In very cold weather, the oils normally found on a fingerprint (which make for better imaging) dry up, such that fingerprints can appear faint. Users may need to press more firmly or even rub the finger into their opposite palm to ensure that a quality image is acquired. Once a high-quality image is acquired, it must be converted to a usable format. Image processing subroutines eliminate gray areas from the image by converting the fingerprint image‘s gray pixels to white and black, depending on their pitch. What results is a series of thick black ridges (the raised part of the fingerprint) contrasted to white valleys. The ridges are then thinned from approximately 5 to 8 pixels in width down to a single pixel, for precise location of features The fingerprint comprises ridges and valleys that

form distinctive patterns, such as swirls, loops, and arches. Most fingerprints also have a core, a central point around which swirls, loops, or arches are curved. Deltas are points, normally at the lower left or right corner of the fingerprint, around which ridges are centered in a triangular shape. Fingerprint ridges and valleys are characterized by discontinuities and irregularities known as minutiae—these are the distinctive features on which most finger-scan technologies are based. There are many types of minutiae, the most common being ridge. Endings (the point at which a ridge ends) and bifurcations (the point at which one ridge divides into two). Depending on the size of the platen and the quality of the vendor algorithm, a typical finger-scan image may produce between 15 and 50 minutiae—larger platens will acquire more of the fingerprint image, meaning that a greater number of minutiae can be located. Vendors utilize proprietary algorithms to map fingerprint minutiae. Information used when mapping minutiae can include the location and angle of a minutia point, the type and quality of minutiae, and the distance and position of minutiae relative to the core. A user normally must place his or her enrollment fingerprint more than once during enrollment, so that the system can locate the most consistently generated minutiae. Finger-scan images will normally have distortions and false minutiae that must be filtered out before template creation. For example, anomalies caused by scars, sweat, or dirt can appear as minutiae. Vendor algorithms scan images and eliminate features that simply seem to be in the wrong place, such as adjacent minutiae or a ridge crossing perpendicular to a series of other ridges. A large percentage of false minutiae are discarded in this process, ensuring that the template generated for enrollment or verification is an accurate reflection of the biometric data. The quality of the fingerprint image must be good enough to create template. There are number of methods for scanning fingerprint image. The leading technologies are: Optical, Silicon and Ultrasound. Large volumes of fingerprints are collected and stored everyday in a wide range of applications including forensics, access control, and driver license registration. An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints in a database.

II. EXISTING METHOD

Biometric Cryptosystems Biometric cryptosystems try to combine biometric templates with cryptographic keys. Successful biometric authentication can reveal the keys. Biometric cryptosystems can act in one of the following three modes: 1) key release, 2) key binding, and 3) key generation. In the key-release mode, biometric authentication is completely decoupled from the key release mechanism. The biometric template and the key are stored as separate entities and the key is released only if the biometric matching is successful. Implementing a biometric cryptosystem in the key release mode is easy, however such a system is not appropriate for high security applications because it has two major vulner abilities. First, the biometric template is not secure. Template security is a critical issue in biometric systems because stolen templates cannot be revoked. Second, since authentication and key release are decoupled, it is possible to override the biometric matcher using a Trojan horse program. In the key binding mode, the key and the template are monolithically bound within a cryptographic framework. It is computationally infeasible to decode the key or the template without any knowledge of the user's biometric data. A crypto-biometric matching algorithm is used to perform authentication and key release in a single step. In the key generation mode, the key is derived directly from the biometric data and is not stored in the database. Based on the fuzzy vault scheme, the minutiae positions were used to encode and decode secret codes. However, alignment of fingerprints is crucial for this method to work properly. Many works have been conducted to overcome this problem. Authors proposed more effective implementation of fuzzy fingerprint vault. They also proposed an automatic. alignment method in the encrypted domain. They used the high

curvature points on ridges to do alignment. Authors proposed another effective implementation of fuzzy vault scheme. They used minutiae descriptor to propose their systems. This method made the false accept rate decrease greatly in low polynomial degrees. However, their scheme also needed the alignment. A proposed a new alignment algorithm for fingerprint fuzzy vault. They used ridges associated with the minutiae around the core point of the fingerprint for the alignment. By using this alignment method, developed a new version of fingerprint fuzzy vault. They integrated local ridge information of minutiae, which exclude the possibility of cross-matching among different vaults constructed from the same finger. So they improve the security of fuzzy vault. This developed an alignment-free fingerprint cryptosystem. This method was based on modified Voronoi neighbor structures. In this paper we propose a novel alignment free fingerprint cryptosystem which does not have any alignment procedure. We use minutiae near the reference point to constitute Cartesian systems. Based on these Cartesian systems, we calculate the new positions and orientations of minutiae to use them in encryption and decryption procedures.

A fingerprint minutiae composes of four elements: x-coordinate, y-coordinate, angle, and type. Encoding and decoding phase are two steps of the fuzzy fingerprint vault systems. In order to explain the proposed method ,Encoding and decoding steps are the fuzzy fingerprint vault and is explained in the preceeding sections.

Encoding Stage

To address errors in different feature levels, a two-level secure sketch is used in the encoding procedure, the detailed steps in the encoding procedure are as follows. Given a fingerprint template T_T , we first extract the template minutiae set using the software VeriFinger 6.0 from Neurotechnology , From this set, we choose only 30 well separated genuine minutiae, i.e., the minimum distance between each is greater than a predefined threshold value. The distance between two minutia point is defined as and the weight assigned to the orientation attribute. If the number of well-separated minutiae in the template is less than 30, all will be chosen and we denote the selected minutiae set S^T . The reason we set the upper bound for the number of genuine minutiae is to reduce the processing time required for matching.

Decoding Stage

The decoding procedure is shown in precious section we first extract the query minutiae set . From that set, we choose only 30 well-separated minutiae (if the number of well separated minutiae in the query is less than 30, all will be chosen and denote the selected minutiae set For each minutiae, we construct its P-P structure by connecting it to all the other minutiae and denote it. In terms of template/key protection, the system fuses cancelable biometrics and biocryptography. Transforming the P-P minutiae structures before encoding destroys the correlations between them,and can provide privacy-enhancing features, such as revocability and protection against cross-matching by setting distinct transformations for different applications. This method does not produce the satisfactory results ,In order to overcome the above drawback.Quadraangle based structure is used for the finger print recognition because it can tolerate the local structural change suffered by triangle based structure under non linear distortion .

III. PROPOSED METHOD

Delaunay Quadrangle Generation

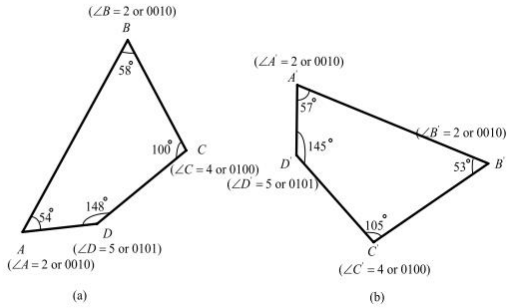
The construction of the Delaunay quadrangle-based structure motivated by the observation that even if the triangles that constitute a Delaunay quadrangle are changed, the minutiae from this Delaunay quadrangle do not change This shows some real examples from the publicly available database that the Delaunay quadrangles do not alter but the Delaunay triangles which comprise are changed under distortion, even if the fingerprint images in the same row are from the same finger. Delaunay quadrangles are built upon the construction

of the Delaunay triangulation net. The algorithm for producing the Delaunay triangulation net is detailed in . Here we give a brief description. A Voronoi diagram is generated first, which partitions the entire fingerprint region into small cells centering on each minutia. All the points in the cell around are closer to than to any other minutiae. Then the Delaunay triangulation net is produced by linking the centers of every pair of neighbor cells as shown For a Delaunay triangulation net formed by the minutiae Delaunay triangles, where K is the number of minutiae on the convex hull of the Delaunay triangulation net. Once the Delaunay triangulation net is generated, a Delaunay quadrangle can be formed by joining any two Delaunay triangles that share a common side.

The proposed Delaunay quadrangle-based structure can tolerate the local structural change suffered by the Delaunay triangle-based structure under nonlinear distortion, as discussed in Generally speaking, the features extracted from the proposed Delaunay quadrangle-based structure are more discriminative than those from the Delaunay triangle based structure. This is because a quadrangle has more attributes (e.g., one more edge and angle) than a triangle.

Local Registration Using Topology Code

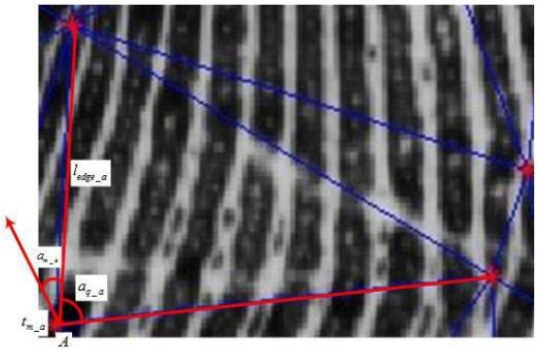
Fingerprint image registration or alignment is a critical process in fingerprint matching. But unfortunately, fingerprint registration usually takes place in the unencrypted domain rather than the encrypted domain. This is because for a fingerprint authentication system with template protection, the original template data are unavailable 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 exposure of the reference points 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 quadrangle-based structure can avoid this global image registration process because only local registration is needed by using local minutiae information, there is a pair of corresponding Delaunay quadrangles, Q(ABC D) and Q(ABCD) from the template and query images, respectively. The key to matching Q(ABC D) with Q(ABC D) is that Q(ABCD) has to be correctly aligned with Q(ABC D). Assume that the points A, B, C and D in Q(ABC D) are corresponding to points A, B, C and D in Q(A BC D), respectively, and that the feature extraction procedure starts from point A, the vertex of the smallest angle, in Q(ABC D) 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 Q(A BC D). A straightforward method is to search the vertex of the smallest angle from Q(ABC D) and considering as a starting point.



Invariant Features Extracted From the Delaunay Quadrangle

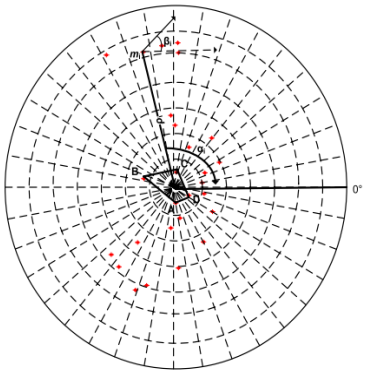
Several invariant features extracted from the Delaunay quadrangle can be used for matching. Below we define some rotation and translation invariant local features of a Delaunay quadrangle:- the length of edges, ledge; - the angles between the each minutia orientation and its neighbour edge in the clock-wise direction, am;- angles between two edges, aq;- the type of each minutia.

All the above invariant features can be easily computed by the given minutia information this also gives an example of the four invariant features for point A in a Delaunay quadrangle.



Auxiliary Features Extracted From the Delaunay Quadrangle-Centered Polar Coordinate Space

To increase the discriminative ability of each Delaunay quadrangle, we further explore an auxiliary featurefromthe local region around each Delaunay quadrangle. firstly, the center of each Delaunay quadrangle is found .



Further considered as the reference point of a polar coordinate space. Secondly, all minutiae covered by the circle of radius R centered at CABC D are translatedandrotatedinto polar coordinates . In this way, each minutiae in this circle range can be represented by a feature set (ρi,αi,βi), where ρi , αi and βi are respectively the radial distance, radial angle and orientation relative to CABC D in the polar coordinate.

IV. RESULTS

Figure 1 .(a) Input image ,(b)Binarization

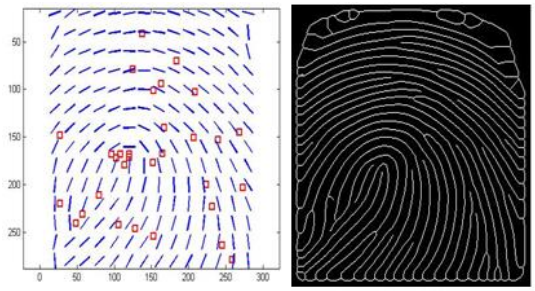


Figure 2. (a) Orientation Image,(b) Thinning Image.

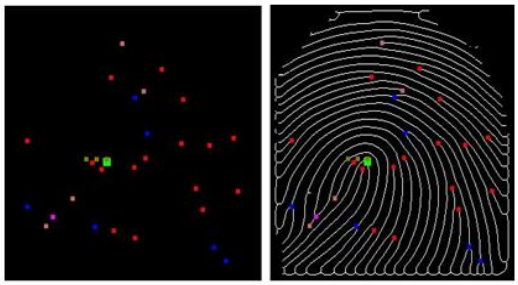


Figure 3. (A) Minutiae Points ,(B) Thinned Minutiae Points

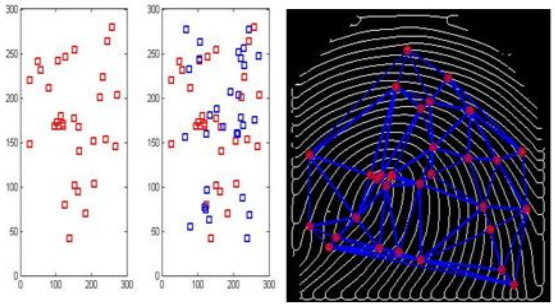


Figure 4. (A) Real Minutiae And Feature With Chaff Minutiae ,(B) Minutiae Points

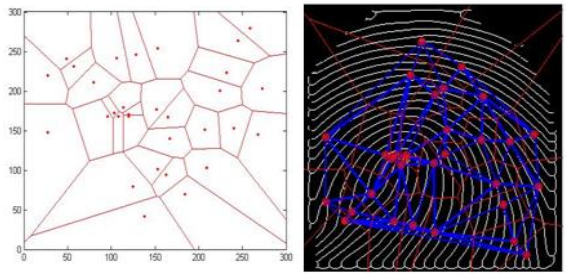


Figure 5. (a) Varoni diagram, (b) Minutiae points

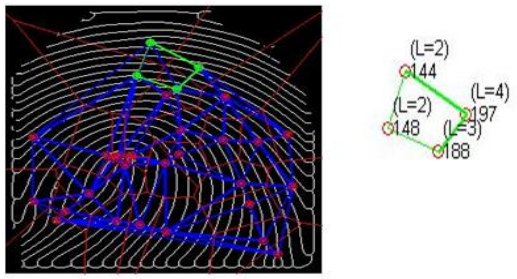


Figure 6. (a) Quadrangle Points ,(b) Region Of Interest

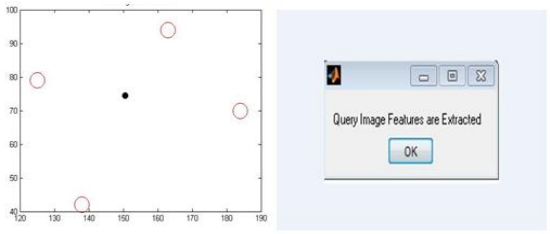


Figure 7. (a) Quadracentre Points ,(b) Query Image Features Extracted

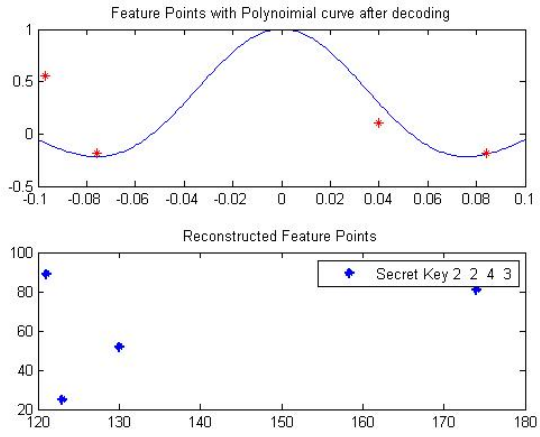


Figure 8. Feature Points With Polynomial Curve After Decoding ,Reconstructed Feature Points

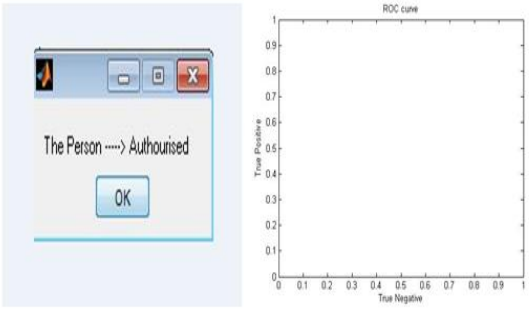


Figure 9. (a) Person Authorized , (a) Roc Curve

V. CONCLUSION

In spite of the fact that arrangement free unique mark cryptosystems give a promising answer for format/key security without enlistment, the acknowledgment exactness of past work is deficiently fulfilling because of poor discriminative energy of the elements utilized and dishonorable treatment of nonlinear twists in the quantized/scrambled area. To address this issue, an arrangement free fuzzy vault utilizing quadra angle based structures is proposed in this paper. The trial comes about on a wide determination of openly accessible databases demonstrate that the proposed framework beats other comparable frameworks while giving solid security. So far, breaking down the trouble of leading a beast constrain assault is most generally utilized as a part of looking at the quality of the fluffy vault plot as far as layout assurance since it is basic and instinctive.A

VI. REFERENCES

[1]. W.-B. Zhong, X.-B. Ning, and C.-J. Wei, "A fingerprint matching algorithm based on relative topological relationship among minutiae,"in Proc. ICNNSP, Jun. 2008, pp. 225–228.

[2]. W. Zhang and Y. Wang, "Core-based structure matching algorithm of fingerprint verification," in Proc. 16th ICPR, 2002, pp. 70–74.

[3]. K. Xi and J. Hu, "Dual layer structure check (DLSC) fingerprint verification scheme designed for biometric mobile template protection," in Proc. 4th ICIEA, May 2009, pp. 630–635.

[4]. X. Jiang and W.-Y. Yau, "Fingerprint minutiae matching based on the local and global structures," in Proc. 15th ICPR, 2000, pp. 1038–1041.

[5]. N. K. Ratha, V. D. Pandit, R. M. Bolle, and V. Vaish, "Robust fingerprint authentication using

local structural similarity," in Proc. 5th IEEE WACV, 2000, pp. 29–34.

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

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

[8]. T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate-based cancelable fingerprint templates," Pattern Recognit., vol. 44, nos. 10–11, pp. 2555–2564, 2011.

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

[10]. Galbally J, Cappelli R, Lumini A, Maltoni D, Fierrez J. "Fake fingertip generation from a minutiae template". Pattern recognition, 2008. ICPR 2008. 19th international conference on digital object identifier. 2008.

[11]. Sutcu Y, Sencar H T, Memon N. "A geometric transformation to protect minutiaebased fingerprint templates". Published in DSP'09 proceedings of the 16th international conference on digital signal processing. 2009.

[12]. Lee C, Kim J. "Cancelable fingerprint templates using minutiae based bit-strings". Journal of network and computer applications 33, 2010, pp.236-246.

[13]. Ahmad T, Hu J, Wang S. "Pair-polar coordinate based cancelable fingerprint templates". Pattern recognition 44, 2011, pp.2555-2564.

[14]. Matteo Ferrara, Davide Maltoni, and Raffaele Cappelli, "Noninvertible minutia cylinder-code representation," Information Forensics and Security, IEEE Transactions on, vol. 7, no. 6, pp. 1727–1737, 2012."Verifinger,"

[15]. "verifinger",http://www.neurotechnology.com/verifinger.html, Accessed: 2013-10-30.

[16]. "Mcyt100database,"http://atvs.ii.uam.es/index, Accessed: 2014-10-01.