International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

A Security-Enhanced Fuzzy Based Fingerprint Cryptosystem Using Pair-Polar Minutiae Structures

SirishaBeela & Prof. M. Sampath Kumar
Department of CSSE, A.U.College of Engineering (A) Andhra University, Visakhapatnam

Abstract:*The popularity of biometrics and its widespread use introduces privacy risks. To mitigate these risks, solutions such as the helper-data system, Pair-Polar Minutiae Structures, fuzzy vault, fuzzy extractors, and cancelable biometrics were introduced, also known as the field of template protection. Fuzzy vault is a practical and promising scheme, which can protect biometric templates and perform secure key management simultaneously. Alignment of the template biometric sample and the query one in the encrypted domain remains a challenging task. In this thesis, we propose an alignment-free cryptosystem based on Pair-Polar Minutiae Structures with multiple fuzzy vaults and minutia local structures. In proposed method, in registration phase, multiple vaults construct for one fingerprint or iris and in verification phase, if at least one of the vaults with respect to its minutiae local structures decoded successfully by the query fingerprint or iris, the secret will be recovered. we propose an alignment-free fuzzy vault-based fingerprint cryptosystem using highly discriminative pair-polar (P-P) minutiae structures. The fine quantization used in our system can largely retain information about a fingerprint template and enables the direct use of a traditional, well-established minutiae matcher. In terms of template/key protection, the proposed system fuses cancelable biometrics and biocryptography. Transforming the P-P minutiae structures before encodingdestroys the correlations between them, and can provide privacy-enhancing features, such as revocability and protection against cross-matching by setting distinct transformation seeds for different applications. The comparison with other minutiaebased fingerprint cryptosystems shows that the proposed systemperforms favorably on selected publicly available databases and has strong security.*

Keywords: — fuzzy vault, local minutiae structure, alignment-free, pair-polar minutiae structure.

1. INTRODUCTION

When biometric templates are compromised, privacy violations may occur. Therefore, biometric template protection has become a critical issue in the current biometric community. Several researchers have shown that an unknown original biometric image can be reconstructed from a fingerprint. Authors showed that three levels of information about the original fingerprint could be obtained from minutiae templates: the orientation field, the class or type of information, and the friction ridge structure[1]. The local ridge orientation was estimated using the minutiae triplets. This was then used to predict the class of the fingerprint. Finally, the ridge structure of the original fingerprint was generated using streamlines that were based on the estimated orientation field. Recently, authors experimentally showed that minutiae based matcher could be faked using reconstructed minutiae but image based matcher could not be faked. Furthermore, traditional methods for identifying persons, for example, ID and personal identification numbers (PINs), can be cancelled and re-issued if the above privacy issues are compromised. But this is not possible with biometric data because biometric data do not vary much over time and are very rarely shared by two people [2]. Therefore, when the same biometric data are used in multiple security applications, biometric data can be shared between commercial companies and law enforcement or government agencies[3]. This may lead to the possibility of tracking personal biometric data stored in one security application by getting access to another security applications through cross matching.

In general biometric systems, templates are stored fairly insecurely in databases[3]. To protect them better, many alternate solutions have been proposed by both biometric and cryptographic researchers. These solutions can be roughly divided into two categories: cancellable biometrics and biometric cryptosystems.

A. Cancelable biometrics

Cancelable biometrics uses transformed or intentionally-distorted biometric data instead of original biometric data for identification. Because the transformation is noninvertible, the original biometric templates cannot be recovered from the transformed templates. When a set of biometric templates is found to be compromised, it can be discarded and a new set of biometric templates can be regenerated. Authors proposed a key-based transformation method for fingerprint minutiae. A core point of an input fingerprint image was detected and then a line through the core point was specified. The angle of the line depended on the key, where 0 ≤ Key ≤ Pi. The transformed fingerprint templates were generated by reflecting the minutiae under the line into those above the line[3]. The new transformed fingerprint template was then generated by changing the key (angle). A disadvantage of this method is that it required core point detection as well as the alignment of the input fingerprint image into a canonical position[10]. Also, since the minutiae above the line were not transformed, the transformed template still retained some information from the original fingerprint. Authors described three transformation methods such as Cartesian, polar, and functional transformation. The Cartesian and polar transformation methods divided a fingerprint into sub-blocks and then scrambled those sub-blocks. In the functional transformation method, transformation was based on a Gaussian function. However, all three methods required alignment before transformation. To align the fingerprints, these methods used singular points. Authors proposed a cancelable fingerprint template using fingerprint minutiae. Translation and rotation invariant values were extracted using orientation information around each minutia. The obtained invariant value was input into two changing functions (which output translational and rotational movement) to transform each minutia. Final cancelable templates were generated by moving each minutia according to the calculated movements[9]. When the cancelable templates were compromised, new templates were regenerated by replacing the changing functions.

B. Biometric cryptosystems

Biometric cryptosystems combine cryptographic keys with biometric templates so that the keys cannot be revealed without successful biometric authentication. One of the most popular approached is fuzzy vault scheme proposed by Juels and Sundan. Based on the fuzzy vault scheme, the minutiae positions were used to encode and decode secret codes. However, this method inherently assumed that the fingerprints were aligned. Several works have been proposed to overcome this issue. proposed more robust and effective implementation of fuzzy fingerprint vault (FFV). They also developed an automatic alignment method in the encrypted domain, using the high curvature points on ridges (i.e., so-called helper data)[4]. Authors developed another effective implementation which took the minutia descriptor into consideration and made the FAR decrease greatly in low polynomial degrees. However, their scheme also aligns the corresponding fingerprints using high curvature points on ridges. Authors developed a novel alignment algorithm for FFV, by tracing the ridges associated with the minutiae around the core point of the fingerprint and storing the location and orientation of the sampling points. By using this alignment method, authors proposed a security-enhanced version of FFV integrating local ridge information of minutiae, which excluded the possibility of cross-matching between different vaults constructed with the same finger[10].

2. LITERATURESURVEY

A fingerprint matching algorithm based on relative topological relationship among minutiae[1]

The relative topological relationship among minutiae was used in fingerprint matching for its changeless characteristics in distorted fingerprints. Each minutia was defined by a characteristic record in which the minutia type and the relative topological relationship among the minutia and its 5 nearest neighbors are included. The fingerprints matched or not depend on the number of minutiae matched. The results show that the algorithm presented in this paper is insensitive to both linear and nonlinear distortions in fingerprint.

Core-based structure matching algorithm of fingerprint verification [2]

The fingerprint matching algorithm is a key issue of fingerprint recognition, and there already exist many fingerprint matching algorithms. According to the dependence of the core point, fingerprint matching algorithms are divided into two groups: core-based match algorithms and noncore-based match algorithms. Most of the noncore-based matching algorithms are time consuming, therefore, they are not suitable for online application; while the core-based matching algorithm is more efficient than the noncore-based matching algorithm, but it highly depends on the core detection precision. In this paper, we present a new core-based structure matching algorithm which considers both efficient and precision. First, we use a core detection algorithm to obtain the core position, then define some local structures of the core area. Using these local structures, we can find some of the correspondent points of the two fingerprint image. Next, we use the correspondent points in the first stage to match the global feature of the fingerprint.

Fingerprint minutiae matching based on the local and global structures [3]

Proposedss a fingerprint minutia matching technique, which matches the fingerprint minutiae by using both the local and global structures of minutiae. The local structure of a minutia describes a rotation and translation invariant feature of the minutia in its neighbourhood. It is used to find the correspondence of two minutiae sets and increase the reliability of the global matching. The global structure of minutiae reliably determines the uniqueness of fingerprint. Therefore, the local and global structures of minutiae together provide a solid basis for reliable and robust minutiae matching. The proposed minutiae matching scheme is suitable for an online processing due to its high processing speed.

3. ALGORITHMSTECHNIQUES

A. GENERATION OF STRUCTURE

A fingerprint F is always represented by a set of minutiae, i.e. ,$F = \{Mi \}Ni{=}1$, $Mi = (xi , yi, \theta i)$, where (xi,yi) are the Cartesian coordinates of Mi , and N *is* the number of minutiae in F *and*θi its orientation.

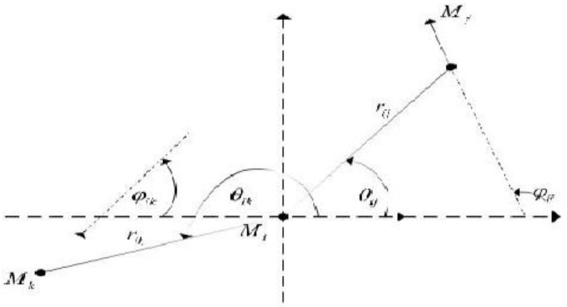


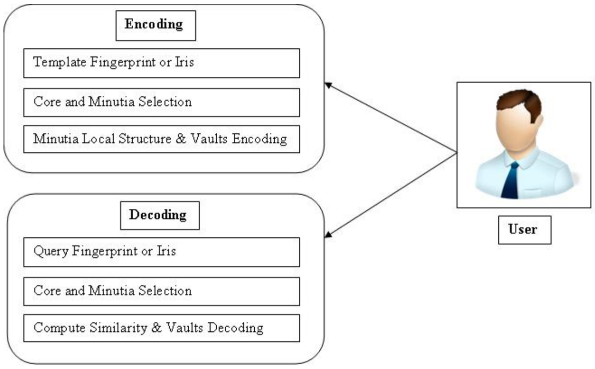
Fig1. Generation of Structure

When Mi is selected as a reference minutia, we denote the relative position of a minutia Mj ,j _= i to Mi by a P-P coordinate vector $vi\ j = (rij\ ,\phi i\ j,\theta i\ j\ )$.Here Mi *is* serves as the center of a polar coordinate space, the orientation of which acts as the 0° axis, $ri j$ is the radial distance between Mi and Mj , $\phi i\ j$ the counter-clockwise angle between the orientation of Mi and direction of $MiMj$, and $\theta ij$the orientation difference between Mi and Mj . In this case, the P-P structure of Mi can be represented by Vi , show Figure and F by $F = \{Vi\}Ni$=1[8].

B. MINUTIAE MATCHER

In global minutia matching algorithms are aligned after two fingerprints first is a template and second is a queryand, their corresponding minutiae are paired. Mj=(xj ,yj, θj) from the template and Mj= (xj , yj, θj) from the query are regarded as a pair of matched simultaneously. where d and θ are predefined distance and angle thresholds, respectively. 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[4]. 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[4]. However, we can seamlessly transform it into a transformation-invariant feature-applicable version as below. Let vij = (rij, ϕij ,θij) is the relative position of minutia Mj to Mi and vkl = (rkl, ϕkl, θkl) is the relative position of minutia Ml to Mk) be two P-P coordinate vectors for comparison.

4. SYSTEM ARCHITECTUR


Encoding
Template Fingerprint or Iris
Core and Minutia Selection
Minutia Local Structure & Vaults Encoding
Decoding
Query Fingerprint or Iris
Core and Minutia Selection
Compute Similarity & Vaults Decoding
User

1. Load Fingerprint or iris templates:

• In this module, we load the fingerprint or iris templates.

•Given the template fingerprint or iris image T, the encoding procedure is starts.

2. Encoding process:

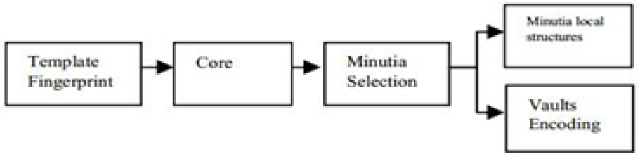


Fig 3 .Encoding process

Extracting core: At this stage, fingerprint image T is preprocessed and the orientation field is estimated. Afterwards, we calculate all of the possible singular points using Poincare and select the most reliable singular point as the core according to the changing of the orientation field and the ridges around the core.

- Selecting minutia: We draw a ring around the reference point by radius R1 and R2, and mark all minutiae MiT in the ring. Each MiT will define a coordinate system C0. For each minutiaeMiT, the minutia local structures MDiT are extracted.

- Finally we Constructing & Encoding fuzzy vaults.

3. Decoding process:

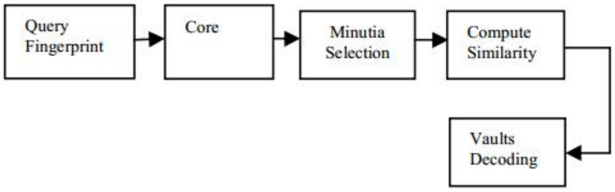


Fig 4. Decoding process

- Extracting core: Similar to the first step at encoding procedure, the same core detection algorithm is applied to detect the core of fingerprint image Q.

- Selecting minutia: We draw a ring around the reference point by radiuses R1 and R2 and mark all minutiae MiQ in the ring (radiuses R1 and R2 are the same as the ring radiuses at the encoding procedure). For each minutia MiQ, the minutia local structures MDiQ are extracted.

- Finally we Decoding the fuzzy vaults.

5. RESULT

Our proposed system solves the problem of low accuracy for matching the Minutiae structure of submitted fingerprint/iris with template provided by user Ui at the time of registration. For performance measure we compare the success ratio of match algorithm by both systems using existing and proposed. The success ratio of predicted values defines the precision / accuracy in matching Minutiae structure of submitted fingerprint/iris with template provided by user Ui at the time of registration .It is calculated by simple formula total number of right match attempt /total attempt done by system. For existing system it is recorded that the success ratio is ranging between low to high 50% to 85% and it largely depend on orientation and the also fingers should be in right condition for matching like no moisture and also only one reference point is considered thus produces low accuracy results which degrade the performance of system.It is expected that for proposed system the success ratio will always be high and will scale easily if N users enroll to system and it predicts accurate values on basis of multiple reference point data collected hence more accurate and also fast.

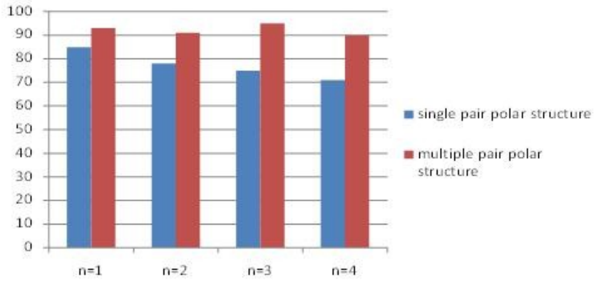


Fig6. Percentage matched of single pair polar and multiple pair polar

6. CONCLUSION AND FUTURE WORK

Although alignment-free fingerprint or iris 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 in this paper. Our system improves recognition accuracy in two respects. Firstly, the P-P minutiae structure is more discriminative than other local minutiae structures, such as the five-nearest neighbour ,Voronoi neighbour , and triangle structures. Secondly, compared with the trivial or coarse quantization used in other work, the fine quantization used in our system can retain more information about a fingerprint or iris template to a greater extent and enable the direct use of a well - established minutiae matcher, which is specially designed to deal with intra-class variations. In terms of security, the proposed system combines the advantages of cancelable biometrics as well as biocryptography. Firstly, transforming P-P minutiae structures before encoding destroys the correlations between them and also provides privacy enhancing features, such as revocability and protection against cross-matching attacks. Secondly, adding enormous numbers of chaff points in the vault provides extra protection for transformed genuine features, which increases the complexity of deriving the original template from the transformed one. The experimental results on a wide selection of publicly available databases show that the proposed system outperforms other similar systems while providing strong security.

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, June. 2008, pp. 225–228 W. Zhang and Y. Wang, "Core-based structure matching algorithm of fingerprint verification," in Proc. 16th ICPR, 2002, pp. 70–74

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. 5thIEEE 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 Recognit., 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. C. Lee, J.-Y. Choi, K.-A.Toh, S. Lee, and J. Kim, "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