IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 12, December 2016

Alignment-Free Fingerprint with iris Cryptosystem Based on Pair-Polar Minutiae Structures with Multiple Fuzzy Vault and Minutia Local Structures

Prof. Archana Lomte [1], Priyanka Vethekar [2]

Assistant Professor, Computer, JSPM's, BSIOTR, Wagholi, Pune [1]

Student, Computer, JSPM's, BSIOTR, Wagholi, Pune [2]

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. Experiments on FVC2002-DB2a and FVC2002-DB1a are conducted to show the promising performance of the proposed fingerprint or iris cryptosystem.

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

I. 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 canceled 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 agencie s[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.

Previous ways of protecting biometric templates

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: cancelable 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 $0 \leq \text{Key} \leq \text{Pi}$. 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

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 12, December 2016

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. 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.

II. SYSTEM WORKFLOW AND COMPONENT

A. Generation of Structure

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

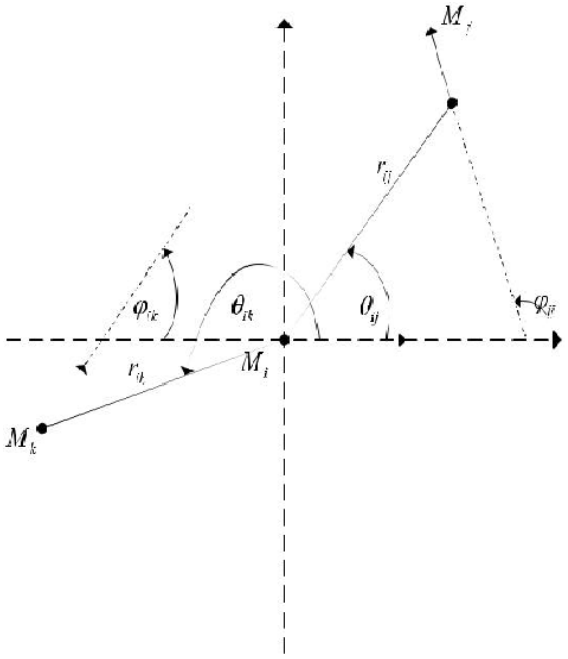

Fig1. Generation of Structure

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 , ϕi j ,θi 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 , ϕi j the counter-clockwise angle between the orientation of Mi and direction of MiMj, and θi jthe 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 query and, 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. 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.After Mi and Mk are aligned, Mj and Ml in the new coordinatespace can be expressed as (ri j cos ϕi j , ri j sin ϕi j , θi j)and (rkl cos ϕkl , rkl sin ϕkl, θkl), respectively. Assuming that vi j matches vkl when Mj matches Ml .

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 12, December 2016

C. System Architecture

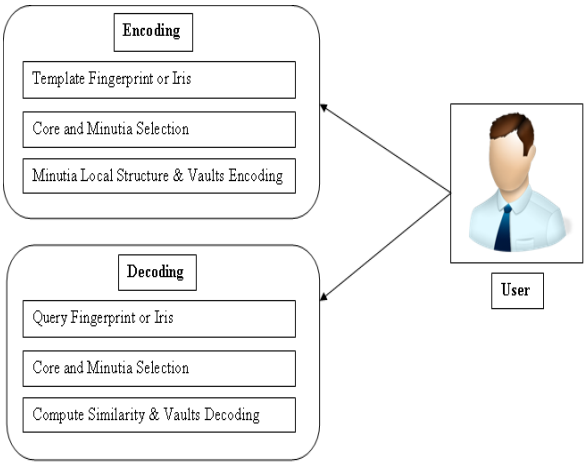

Fig2.System Architecture

Encoding stage

To address errors in different feature levels, a two-level secure sketch (a fuzzy vault and Shamir's secret sharing scheme) is used in the encoding procedure[2].

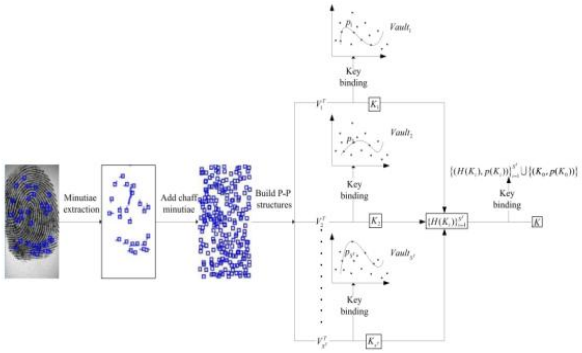

Fig3.Encoding stage

(1) Extracting core. At this stage, fingerprint image T is pre-processed 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.

(2) 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 minutiae MiT, the minutia local structures MD0 3are extracted using the method.

(3) Constructing fuzzy vaults. Let L= {(xi,yi, θi, ti) | i= 1,...,n} be a set of real minutia. Minutiae in the ring is selected as the reference minutiae, other minutiae in the set L are rotated and translated.

With a set of transformed minutiae, a fuzzy vault vi is encoded with the method. Another minutiae in the ring is selected as the reference minutia, and a new fuzzy vault Vj is encoded. Encoding of fuzzy vaults is repeating.

Decoding Stage

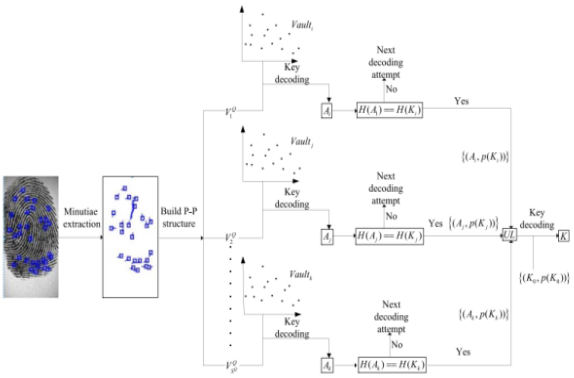

Fig4.Decoding stage

(1) 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.

(2) Selecting minutia. We draw a ring around the reference point by radiuses R1 and R2 and mark all minutiae' in the ring (radiuses R1 and R2 are the same as the ring radiuses at the encoding procedure). For each minutia . ', the minutia local structures MD@ 0 are extracted based on the method described in section 3 to obtain the set of pairs MV@ = {(. ', MD0 @)} ># ?′ .

(3) Decoding fuzzy vaults. For the ith minutia, inside the set MV@,its corresponding minutia local structures are MD0 @. The similarity measure {-)})># ?A?′ between MD @ 0 and the first elements in MV3 (i.e. MDB 3, $1 \leq j \leq r$) is computed by equation 20. If -) satisfy the following condition:-) ≥ FG, **(20)** Where FG is threshold, thus we can say . ' has a reliable counterpart .) (in the template fingerprint. So with minutiae. ' as the reference minutia, other minutiae are rotated and translated with equation 19. Decoding of vault VB in MV3) is checked by using method which described in 2-2. If VB is not decoded, another minutia inside the set MV@ is selected as the reference minutiae and this step repeats until whole minutia inside the set MV@ are selected. If at least one of the vaults decoded successfully, the secret will be recovered.

III.CONCLUSION

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 neighbor, Voronoi neighbor, 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.

ACKNOWLEDGMENT

I thank my project guide and ME. Coordinator **Prof. Archana lomte** for the guidelines in completion of this paper. I also wish to record my thanks to our Head of Department **Prof. G. M. Bhandari** for consistent encouragement and ideas.

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 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.