Proceedings of 2014 RAECS UIET Panjab University Chandigarh, 06-08
March, 2014

Methods of Automatic Alignment of Fingerprint in Fuzzy Vault :A Review

Parul Sood
Department of Computer Science and Engineering
PEC University of Technology
Chandigarh, India
Kapoornaisha2011@gmail.com

Manvjeet Kaur
Department of Computer Science and Engineering
PEC University of Technology
Chandigarh, India
manvjeet@pec.ac.in

***Abstract*—Security of cryptographic keys is an important issue in today's unprotected world. Most reliable solution of this problem is state of art fuzzy vault which is an application of bio-cryptosystems. These systems use biometric trait for locking and unlocking the keys. During unlocking, it is necessary to do alignment of query biometric data with enrolled biometric data because of large variation in two samples of a biometric trait of a user taken over the short span of time. Complexity of alignment is increased due to absence of original fingerprint template during alignment. That's why helper data or additional information is required for alignment. There are number of techniques developed for automatic alignment of fingerprints till now. This paper gives the review of most of those methods.**

Keywords*— fuzzy vault; helper data; reference points; minutia structure; automatic alignment; fingerprint alignment; alignment free; minutia orientation.

I. INTRODUCTION

Exchange of information through internet has increased in this era. But keeping this information secure is major challenge. Couple of cryptographic algorithms (e.g. AES, DES) is developed to encrypt and decrypt the data to be protected. These algorithms are successful in maintaining the safety of data but it is difficult to handle their keys due to their large size (generally more than 128-bit) [1]. Earlier, passwords were used to protect these keys. But use of passwords for securing the keys is not reliable solution. Because passwords can be easily lost stolen, forgotten or guessed using social engineering and dictionary attacks [2].

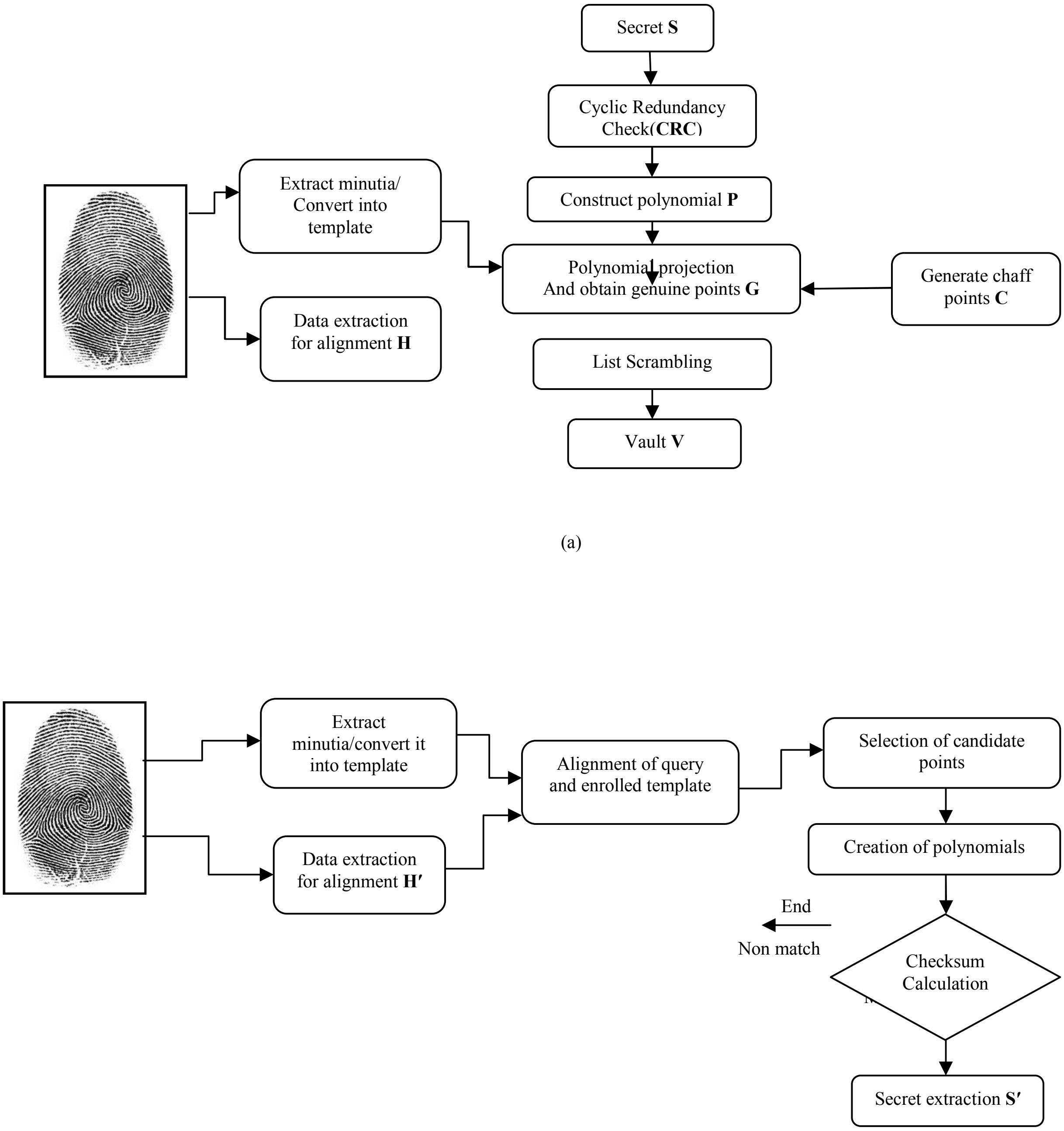
Passwords based authentication is replaced by more secure authentication known as biometric authentication [3] which allows user to access the secret only after matching of live biometric sample with stored sample in database. But in this scheme templates are compromised by various attacks (like -override the biometric matcher, by stealing template database) moreover it is difficult to reissue template because these are unique for every individual [4]. Further this issue is resolved by merging cryptography and biometrics in a single unit and these combined security systems are called as biometric cryptosystems. These systems work mainly in three modes: (1) Key release: (2) Key binding: and (3) Key generation. In key release mode, secret (key) is delivered only if query template matches with stored template. Here key and template is independently stored in separate databases. In key binding mode, secret (key) and template is encoded in such a way it is computationally infeasible to separate secret and template without having user's biometric data. In key generation mode key is randomly generated from biometric data [5].

Biometric cryptosystems in key release mode are easy to implement but not secure [1]. In contrast, biometric cryptosystems in key binding mode are more secure and difficult to implement because biometric data having large intraclass variation.

Fuzzy vault proposed by juels and sudan [6] is an application of biometric cryptosystems in key binding mode. Most approaches divide fuzzy vault broadly into two steps: (1) State of art fuzzy vault construct: and (2) automatic alignment [7]. Fuzzy vault is mainly used to hide a secret **S** generally of length 128-bit using unordered set **U** (e.g. when fingerprint is used as a biometric trait then unordered set contains minutiae extracted from fingerprint sample). Extra features to do alignment are also extracted from biometric trait and sometimes this information is known as helper data **H**. Generally 16-bit checksum is calculated on secret and append it in the end of secret. After that secret **S** is divided into coefficient of polynomial **P** and then polynomial is evaluated on all elements of set **U** and resultant points are called genuine points **G**. Then chaff points **C** are selected randomly and added with genuine points **G** to provide mask to genuine points **G.** Collection of chaff points **C** and genuine points **G** is called vault **V**. During decoding user gives biometric sample (query). Extract unordered set $\mathbf{U}'$ and $\mathbf{H}'$. Then alignment of query and enrolled template is performed through helper data. By matching $\mathbf{U}'$ with vault **V** then user can find some points that lie on polynomial and using these points number of polynomials are constructed. After that error correction techniques are applied on every polynomial and then error free polynomial is selected. At last coefficient of polynomial is

978-1-4799-2291-8/14/$31.00@2014 IEEE

converted to $\mathbf{S}'$ which is same as **S** [5]. Fuzzy vault encoding-decoding is described in Fig.1. Automatic alignment methods for fingerprint are described in section II. Section III presents the alignment free fuzzy vault. Conclusion is contained in section IV.


Secret **S**
Cyclic Redundancy Check(**CRC**)
Construct polynomial **P**
Extract minutia/ Convert into template
Polynomial projection And obtain genuine points **G**
Generate chaff points **C**
Data extraction for alignment **H**
List Scrambling
Vault **V**
Extract minutia/convert it into template
Alignment of query and enrolled template
Selection of candidate points
Creation of polynomials
Data extraction for alignment **H′**
End
Non match
Checksum Calculation
Secret extraction **S′**

(a)

(b)

Fig.1. Fuzzy vault: (a) encoding, (b) decoding

II. Methods of automatic alignment of fingerprint

This section describes the different methods of automatic alignment. These are categorized in five major categories based on reference points, helper data, geometric hashing minutia structure and minutia orientation histograms. All these are described below.

A. *Fingerprint alignment based on reference points*

Shenglin Yang and Ingrid Verbauwhede [8] alignment method finds a new set of feature in polar co-ordinate system and this feature set do not have effect of rotation on them. Main task of this method is to select the origin and here, each feature is represented by three parameters **r, ø, φ**. Here **r** is a distance between two minutia, **ø** is position angle, **φ** is difference of direction between origin and minutia after that similarity level between two minutia is calculated on the basis of some threshold and pair having maximum similarity is reference pair moreover this pair is chosen as base to align one template and also store the local structure of this pair to find the corresponding reference points in query template. If similar reference points are found in query then alignment is performed. But this assumption is not true in general [9]. Reference points based alignment method is simple to compute but task of finding reference point is crucial. Mistakenly chosen reference point could lead to false reject [5].

B. *Fingerprint alignment based on helper data*

Karthik NandaKumar, Anil K. Jain and Sharath Pankanti [5] proposed helper data based alignment method. Helper data is basically additional information extracted from fingerprints and stored publicly. Helper data should not reveal any information and also have sufficient data to do alignment. Here helper data is high curvature points and these points does not leak any kind of information. After extracting high curvature points, a trimmed iterative closest point (ICP) algorithm [12] is applied to align query and enrolled template.

Li et al. [7] define a method based on helper data to calculate translation and rotation parameters and also constructs topological structure around the core points. Helper data of query and enrolled template is compared to get matching parameters then translation and rotation is applied to query. On the basis of result of matching decision of decoding is taken.

C. *Fingerprint alignment based on geometric hash tables*

Chung et al. [10] proposed alignment method is based on geometric hash tables which can be large in size. These hash tables encode transformation of valid and dummy points on the basis of single reference minutia and performance and experimental results did not discussed in this paper [9].

Moon et al. [11] Proposed improvement over original geometric hashing method. Original geometric hashing is used for 1:N identification and 1:1 verification. But 1:N identification is excluded in this new method. Moreover experimental results are also given in this paper. Authors did experiment by taking less than 10 minutia and then achieved False Reject Rate (FRR) is .081. Overall experimental False Accept Rate(FAR)is 0%.

D. *Fingerprint alignment based on minutia structure*

Jason Jeffers and Arathi Arakala[13] describe three minutia based structure for alignment :(1) Five nearest neighbor based structure: (2) voronoi neighbor based structure: and (3) triangle based structure. Five nearest neighbor structure is based on local ridge orientation and this contains five minutia neighbors to it. Match between two local structures occur only if matching of number of neighbor is greater than local match threshold. Voronoi neighbor structure is similar to five neighbor but only difference in selection of neighbors which is selected from voronoi diagram. These two algorithms are local. Triangle based structure uses three minutia which collectively form the triangle. Here match between two instances exists only if Cartesian distance between each displacement lie within edge threshold and ridge orientation ranges within direction threshold. Experiment proved triangle based structure is better than other methods.

E. *Fingerprint alignment based on minutia orientation histograms*

Vedrana Krivokuca and Waleed Abdulla [14] alignment method is mainly divided into three steps: (1) make minutia orientation histograms for query and enrolled templates: (2) aligning these two histograms through circular correlation: (3) again align query and enrolled template using rotation parameter which are the result of circular correlation. Experimental results of this method have shown that proposed method is more accurate and fast.

III. Alingment free fuzzy vault for fingerprints

All above methods are using some additional information for alignment. But this section contains alignment free method. That means this method is based on only those feature which do not need any type of alignment.

Li et al. [1] provided an alignment free fuzzy vault. For this they need to choose features robust to translation and rotation. So they decided to use minutia descriptors and minutia local structure. Minutia descriptors are selected by method proposed by Tico and Kuosmanen [15] and minutia local structure is proposed by Jiang and Yau [16]. Three fusion strategies are use to combine two local features and to decrease the size of minutia descriptor Huffman encoding is used. Moreover Cyclic Redundancy Check (CRC) is replaced by SHA-2 to provide more accuracy. This method is providing accuracy but takes more space to store vault. So there is need to reduce the storage space.

IV. Conclusion

Fuzzy Vault is secure and growing bio-cryptography construct. Alignment is one crucial part of fuzzy vault. Initially alignment is done using reference points but reference points are not easily found in every fingerprint. At same time alignment based on geometric hashing came in existence but problem of hashing is huge hash tables. After that it started performing with the help of helper data but in some cases helper data reveal information about fingerprint. Recently alignment is done through use of histograms but there is need to improve its speed. There is also one alignment free technique but it needs to store large templates. Concluding, there is still need of more promising, secure and efficient scheme for alignment.

References

[1] P. Li, X. Yang, K. Cao, X. Tao, R. Wang, and J. Tian, " An alignment free fingerprint cryptosystem based on fuzzy vault scheme " journal of networks and computer application, vol. 3, pp. 207-220, May 2010.

[2] J. Apelbaum, "User authentication principals theory and practice", Technology Press, 2004.

[3] A. K. Jain, "An introduction to biometric recoginitation," in Proc. IEEE Trans1. circuits and systems on video technology , vol. 14, pp. 4-20 ,Jan. 2004.

[4] P. Ambalakat, "Security of biometric authentication systems", in Computer Science Seminar, Rensselaer at Hartford, 2005.

[5] A. K. Jain and S. Pankanti "Fingerprint based fuzzy vault:implementation and performance," in Proc. IEEE Trasns4. information forensics and security, vol. 2, pp. 744-757, 2007.

[6] A. Juels, and M. Sudan, "A fuzzy vault scheme," in Proc. IEEE Int.Symp. Inform. Theory, Lausanne, Switzerland, 2002, p. 408.

[7] J. Jeffers, and A. Arakala, " Fingerprint alignment for a minutiae-based fuzzy vault", in Proc. IEEE biometrics symposium ,2007.

[8] S. Yang, and I. Verbauwhede, "Automatic secure fingerprint verification system based on fuzzy vault sceheme ," in Proc. IEEE ICASSP, pp. 609-612, 2005.

[9] U. Uludag, and A. jain, "Securing fingerprint template :Fuzzy vault with helper data," in Proc. IEEE CVPRW, 2006.

[10] Y. Chung, D. Moon, S. Lee, S. Jung, T. Kim, and D. Ahn, " Automatic alignment of fingerprint featuresfor fuzzy fingerprint vault," In Proc.CISC, SKLOIS conference on information Security and Cryptology, pp. 358–369, 2005.

[11] D. Moon, S. Lee, Y. Chung, S.B.Pan, and K.Moon, " Implementation of automatic fuzzy fingerprint vault," in Proc. IEEE 7th Int. Conf. machine learning and cybernetics, pp. 3781-3786, July 2008.

[12] D. Chetverikov, D. Svirko, D. Stepanov, and P. Krsek, " The trimmed iterative closest point algorithm," in Proc. IEEE Int. Conf. Pattern Recognition, pp. 545–548 Aug. 2002.

[13] J. Li, X.Yang, J. Tain, P. Shi, and P.Li, "Topological structure-based alignment for fingerprint fuzzy vault," IEEE, 2008.

[14] V. Krivokuca, and W. Abdulla, " Fast fingerprint alignment method based on minutia orientation histograms," in Proc 27th Conf. Img. Vis. Comp.,pp. 486-491,2012.

[15] M. Tico, and P. Kuosmanen, " Fingerprint matching using an orientation based minutia descriptors ," IEEE Trans. pattern analysis and machine intelligence, vol. 25, pp. 1009-1014, Aug. 2003.

[16] X. Jiang, and W. Y. Yau, " Fingerprint minutia matching on local and global structures," in Proc. IEEE, pp. 1038-1041,2000