International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Biometric Template Security Scheme using Fuzzy Vault

Purva Gabhane[1], Anisa Anjum[2]

[1]RTMNU University, Kavi kulguru Institute of Technology and Science, Ramtek, India

[2]Assistant Professor, RTMNU University, Kavi kulguru Institute of Technology and Science, Ramtek, India

Abstract: ***To protect the biometric templates and secret key simultaneously fuzzy vault is one of the most popular algorithms. In fuzzy vault generation at first, the preprocessing steps are applied and subsequently, the features are extracted and combined. For recognition, we match the feature vectors of images. The biometric template along with the input key are used to generate the fuzzy vault. In the decoding process, the template is given as input and is combined with the stored fuzzy vault to generate the corresponding final key. In this fuzzy vault scheme the biometric features are used to lock and unlock the secret key which is encoded in the coefficient of polynomial equation. The security of fuzzy vault system is depend on the infeasibility of polynomial reconstruction problem. By adding more noise points that are the chaff points to the vault enhance the performance of vault.***

Keywords: Biometric, fuzzy vault, chaff point, template protection, key generation

1. Introduction

Now a days we need to verify our identities and identify someone else. Biometrics deals with human's physical as well as behavioral characteristics, Using biometrics for authentication human is user-friendly, demands less cost, and offers better safety measures to avoid information theft and safety harassment. Biometric template are the nothing but the digital references of distinct characteristics that has been extracted from a biometric sample. During the enrollment phase the biometric template is captured and stored in the smartcards and system database. These templates are used at the time of authentication as the encryption as well as decryption key. It is important that biometric templates used in biometric application should be constructed and stored in a secure way because, if the biometric data once replaced or stolen that cannot be get back easily. Biometric template need to secure in the way that the adversaries would not be able to forge biometric data easily even when the templates are compromised. If the template is compromised then the adversaries will imitate the legitimate users. This leads to serious problem in privacy and security such that information leakage, imitation and tracking/tracing threats of biometric system. Biometric cryptosystem which is the template protection scheme serve for the purpose of either securing the cryptographic key using the biometric features or directly generating the cryptographic key from the biometric features. Key binding and key generation are the two subcategories of biometric encryption. If the helper data is derived from binding the secret key and biometric template, it is called key binding. Examples include the fuzzy commitment and fuzzy vault. If the helper data are generated from the biometric template only, and the secret key comes from the helper data and the biometric features, it is called key generation.

2. Preprocessing Steps

Fuzzy vault is a template security scheme which is used for protecting the biometric template. In the proposed paper fingerprint is used as a biometric trait, initially the enrolled image is preprocessed, the following are the steps involved in pre-processing

1) Binarization
2) Thinning
3) Minutiae extraction
    i. Bifurcation
    ii. Termination
4) Region of interest (ROI)

Binarization: The ridges in the fingerprint image are highlighted with black color while furrows are white. It transform the 8-bit Gray image into a 1-bit image with 0-value for ridges and 1-value for furrows.

Thinning: Ridge thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide.

Minutiae extraction: Here both bifurcation and termination of ridges the fingerprint is taken.

• Bifurcation
The ridge pixels with three ridge pixel neighbors are identified as ridge bifurcations.

• Termination
The ridge pixels with two ridge pixel neighbors are identified as ridge terminations.

Orientation field is generated which not only shows the angle formed by ridge. It also represents the directionality of ridges in the fingerprint image.

Region of Interest (ROI): Region of Interest (ROI) is useful for the recognition of each fingerprint image. The image area without effective ridges and furrows is first discarded because it only holds background information. It depends on the locations of minutiae and the directions of ridges at the minutiae location. False minutiae are affecting the accuracy

of matching. So, removing false minutiae are essential to keep the system effective.

Feature extraction
After the pre-processing step, features are extracted from fingerprint image. Along with this, some random points (chaff points) are added for an individual to constitute the feature vector elements.

3. Fuzzy Encoding

User's secret key and fingerprint template is protected in encoding phase. In the encoding process of fuzzy vault scheme first the secret key K= {ki}n i=1 of length q*n bits is encoded using CRC that is cyclic redundancy check because the coefficients were q-bit value is that all the arithmetic operation of proposed fuzzy vault system were based on finite field F=GF(2q). To form the new q(n+1) bit code K' the q-bit CRC is concatenated at end of secret. For constructing the polynomial the secret K' is used. The secret K' is encoded into a polynomial P of degree n in F by partitioning it into (n+1) qbit values (c0, c1, …, cn) and they are as the coefficients of P (i.e., P(x)=cnxn+…+c0). The fingerprint minutiae of each user protect the secret such that the secret K' just can be reconstructed from the fuzzy vault as long as (n+1) number of minutiae are found. Second, generating a genuine point set G. A={ai}r i=1, where ai∈F, is the fingerprint template that has r minutiae. r minutiae is well-separated minutiae (i.e., the minimum distance between any two selected minutiae is larger than a threshold δ, if the selection algorithm fails to find r well-separated ridge features, it will be considered as a failure to capture (FTC) error and the algorithm stops or says "it terminates". Treating the elements of A as distinct x-coordinate values, she computes evaluations of the polynomial P on the elements of A to obtain a genuine point set G, where G={ai, P(ai)}r i=1. Third, generating a chaff point set C. Randomly generate s chaff points which are not on P(x), s and these points construct a chaff point set C to secure the fingerprint template. These chaff points are C={cj, zj}s j=1, where zj ≠ P(cj), j ∈ [0, ..., s]. Finally, constructing the vault template, get a new set, V'={xi, yi}r+s i=1, by combining G and C sets together. The scrambled V', denoted as V, is the final fuzzy vault set.

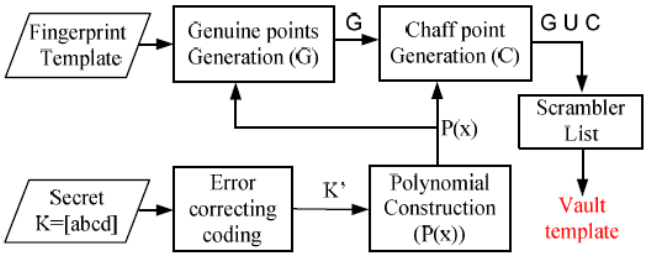

Figure 1: Fuzzy Encoding

4. Fuzzy Decoding

User tries to unlock the vault V using query fingerprint in decoding phase. If the query fingerprint template is similar to the fingerprint template stored in the database then the coefficient and the secret key can be obtained. Detail of decoding process is given in the above figure. From the query fingerprint the query minutiae is obtained and it is represented as the field element, B= {bj}t j=1, where bj€F. if the well separated query minutiae is less than r, it is consider as Failure to Capture (FTC) at that time algorithm stops or say "it terminates". For every bj the vault set V is searched for matching field elements (bj=xi) and the corresponding projection point on the polynomial P(x), Q= {bl, P (bl)} t' l=1. In order to reconstruct an n-order polynomial P, Q set should have at least (n -1) elements. Third, Lagrange interpolation can be used to reconstruct the polynomial. Then, the coefficients are obtained and the secret K is retrieved. The security strength of the fuzzy vault scheme is based on the infeasibility of the polynomial reconstruction problem. The vault performance can be improved by adding more number of chaff points to the vault.

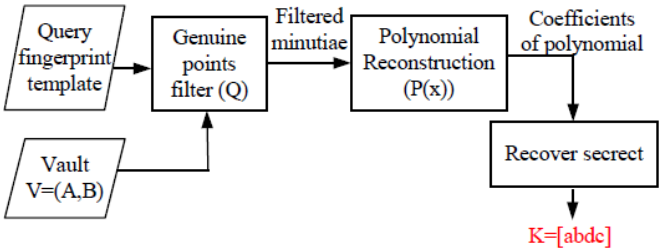

Figure 2: Fuzzy decoding

5. Chaff point generation

The main goal of the adding chaff points in the fuzzy vault is to hide the genuine fingerprint minutiae, so that the chaff points could be chosen in a way that they must be indistinguishable from genuine points. In proposed system, the fingerprint image will split into the segments, called image cells, and the chaff point generation randomly and unique in the image cells. Each image cell has eight adjacent image cells. In an arbitrary image cell, system randomly generated a unique chaff point. If the image cell contains a genuine point or chaff point, this image cell will be ignored.

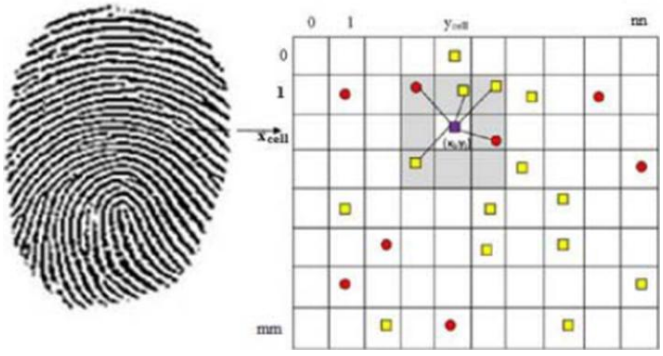

Figure 3: chaff point generation

References

[1] Rubal Jain and Dr. Chander Kant, "A Novel Approach for Securing Fingerprint Template using Steganography", International Journal of Innovations & Advancement in Computer Science, ISSN 2347 – 8616, Volume 4, Issue 6, pp. 503–512, June 2015.

[2] S.Usha and M.Karthik, "A Robust Digital Image Watermarking for Biometric Template Protection Applications", International Journal of Advanced Research in Electrical, Electronics, and Instrumentation Engineering, ISSN 2320-3765, Volume 4, Issue 4, pp. 2067-2072, 2015.
[3] V.Wagh and S.Sonvane, "Minutiae Point Extraction using Biometric Fingerprint Enhancement", Journal on International Research in Engineering and Advance Technology, ISSN 2320-8791 Volume 2, Issue 1, pp. 777-789 March 2014.
[4] N.Hajare, A.Borage, N.Kamble, and S.Shinde, "Biometric Template Security using Visual Cryptography", International Journal of Engineering Research and Application, ISSN 2248-9622, Volume 3, Issue 2, pp. 1320-1323, March 2013
[5] S.Sowakarthika and N.Radha, "Securing Iris and Fingerprint Templates using Fuzzy Vault and Symmetric Algorithm", International Conference on Intelligent System and Control (ISCO), pp. 189-193, 2013.
[6] Thi Hanh Nguyen, Yi Wang, "A Fingerprint Fuzzy Vault Scheme using a Fast ChaffPoint Generation Algorithm", Signal Processing, Communication and Coming(ICSPCC), IEEE International Conference, pp. 1-6, 2013.
[7] S. Ponnarasi and M.Rajaram, "Impact of Algorithm for Extraction of Minutiae Points in Fingerprint Image", Journal of Computer Science, Volume 8, Issue 9, pp. 1467-1672, 2012.
[8] R. Verma, A. Gole, " Wavelet Application in Fingerprint Recognition", International Journal of Soft Computing and Engineering, Volume 1, Issue 4, pp. 129-134, 2011.
[9] A. Nagar, K. Nandakumar, and A. Jain, "Securing Fingerprint Template: Fuzzy Vault with Minutiae Descriptor," International Conference on Pattern Recognition, Volume 6, pp. 822-825, 2008.
[10] K. Nandakumar, A. Jain, S. Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation and Performance", IEEE Transaction on Information Forensics and Security, Volume 2, Issue 4, pp. 744-754, 2007.
[11] N. Raha, S. Chikkerur, and J. Connell, "Generating Cancelable Fingerprint Template", IEEE Transaction on Pattern Analysis and Machine Intelligence, Volume 29, Issue 4, pp. 561-572, 2007.
[12] Geetika, & Kaur, M. (2013, April). Fuzzy Vault with Iris and Retina: A Review. International Journal of Advanced Research in Computer Science and Software Engineering, 3(4).
[13] Jain, A., Nandakumar, K., & Nagar, A. (2008). Biometric Template Security. EURASIP Journal on Advances in Signal Processing (2008).