ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

Template Protection for Fingerprint Recognition System using Fuzzy Vault

Shubhangi Sapkal, Government College of Engineering, Aurangabad
Dr. R.R. Deshmukh, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad

Abstract – In this paper, fuzzy vault scheme is discussed for protection of templates in fingerprint recognition system. As fingerprint recognition system is most commonly used biometric, where minutiae points are stored as templates. If attacker gets this database, fake finger or artificial image can be created. Once biometric is compromised, it cannot be reused. This shows importance of template security in biometric recognition system. Fuzzy vault scheme is used for template protection as it is more suitable for fingerprint recognition system. Fuzzy vault is used to conceal minutiae points and is order invariant.

***Index terms* – Biometric encryption, Fingerprint recognition system, Fuzzy vault, Template protection.**

I. INTRODUCTION

Biometric recognition is the science of establishing the identity of a person using his/her anatomical and behavioral traits. Among all biometric indicators, fingerprints have one of the highest levels of reliability and have been extensively used by forensic experts in criminal investigations and many other applications like access control. Biometric technologies do not store physical trait, but biometric template gets stored. This enrollment process may require the individual to provide multiple instances of the biometric trait. But, the attackers may reconstruct the original biometric images from these templates and then fake finger or artificial biometric image could be created to spoof the system.

Biometric Encryption (BE) is a group of emerging technologies that securely bind a digital key to a biometric or generate a digital key from the biometric, so that no biometric image or template is stored. What is stored is the BE template otherwise known as a ‘‘bio-metrically encrypted key’’ or ‘‘helper data”. As a result, neither the digital key nor the biometric can be retrieved from the stored BE template [1]. The failure modes of a biometric system can be categorized into two classes: intrinsic failure and failure due to an adversary attack. Intrinsic failures occur due to inherent limitations in the sensing, feature extraction, or matching technologies as well as the limited discriminability of the specific biometric trait. In adversary attacks, a resourceful hacker (or possibly an organized group) attempts to circumvent the biometric system for personal gains. Adversary attacks are further classified into three types based on factors that enable an adversary to compromise the system security. These factors include system administration, no secure infrastructure, and biometric overtness. Biometric cryptosystem is proposed by Peng Li *et. al.* [2], to solve the above problem. The biometric cryptosystems can be constructed by combining several of error correction codes for fingerprint database.

Two main consequences of stolen templates are: Intrusion, which enables to create physical spoof (security vulnerability) and Function creep, by which cross-matching is possible (loss of privacy). In [3], various methods are discussed to bind a cryptographic key with a biometric template. Following are the requirements of biometric template protection methods:

Diversity - Secure template must not allow Cross-matching, ensuring user’s privacy.

Revocability - Revoke a compromised template and reissue a new one using the same biometric.

Security - Difficult to obtain the original. To satisfy all these requirements at the same time in the presence of intra-user variations is a challenging task. Cryptosystem for biometric authentication is different than password as different measurements of the same biometric source are different. In the vein, biometric template security scheme combines traditional cryptography technique with error-correcting codes. Biometric template security is an important issue because, unlike passwords and tokens, compromised biometric templates cannot be revoked and reissued.

The outline of the paper is as follows. Different approaches for template protection are given in section II. Section III discusses about fingerprint recognition system. In section IV, fuzzy vault scheme is discussed. Section V shows conclusion.

II. TEMPLATE PROTECTION APPROACHES

Biometric template protection scheme is used to convert biometric data into a secure form. It is impossible or hard to retrieve templates from secured biometric data, which prevents renewing and revocation of biometric data [4].

To get more flexibility to determine access levels, degree of security is changed in biometric systems. But there is a trade-off between FAR and FRR as security level varies. Increased security in biometric systems increases false rejection rate. If security is set too low, false acceptance rate increases [5].

M.B. Ramalho *et.al.* [6], proposed a protection scheme to the biometric template data to guarantee its revocability, security and diversity among different biometric systems. Anil K. Jain *et. al.* [7], implemented different template security approaches for fingerprint system. Following are four broadly used template security approaches:

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

a) Salting – In salting user specific password or key is used to increase the discriminability between classes. The original biometric template and different keys are transformed to get disciminant values for different classes [8]. Invertible functions are employed in salting schemes, whose security therefore relies on the protection of the defining transformation parameters.

b) Noninvertible transform – In cancelable biometrics, non-invertible transformed biometric data is stored. Thus, even if the storage is compromised, the biometric data is not compromised. The fuzzy fingerprint vault is one of the most popular solutions for fingerprint template protection. Ki Young Moon *et. al.* [9] proposed solutions for fuzzy fingerprint vault.

c) Key binding biometric cryptosystem - Store a secure sketch by binding the template with a cryptographic key. In a key-binding biometric cryptosystem [10], a secret key is linked to the original template which creates helper data. If the query template is sufficiently matches to the stored template, the correct secret key is released. Error correcting code is used to compensate the variation of input query template.

d) Key generation biometric cryptosystem- A key is generated from biometric in key generation cryptosystem. R. Ranjan *et. al.* [11] proposed distance based key generation algorithm for fingerprint recognition system which reduces the complicated sequence of operations to generate the crypto keys in the traditional biometric cryptosystem.

Such schemes include fuzzy commitment [12],[13], fuzzy vault, helper data, and secure sketch[14]. Yagiz Sutcu *et. al.* [14] used secure sketch, a recently proposed error-tolerant cryptographic primitive, can be applied to protect the template.

III. FINGERPRINT RECOGNITION SYSTEM

A fingerprint appears as a series of dark lines called ridges and white space between these ridges called valleys. They smoothly flow in parallel and sometimes terminate and bifurcate. The pattern of the ridges and valleys is unique for each individual. Location and direction of ridge endings and bifurcations (splits) are called minutiae points. The minutiae feature is a widely used and standardized fingerprint feature in existing fingerprint recognition systems [15]. The minutiae points are ridge endings and ridge bifurcations as shown in figure 1.

Ridge ending – The abrupt end of the ridge
Ridge bifurcation – A point where ridge divides into two ridges.

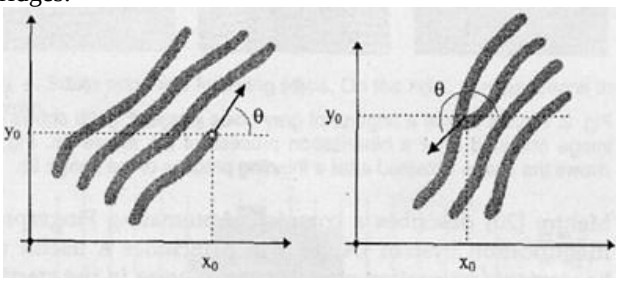

Fig 1: Ridge ending and Ridge bifurcation

This feature extraction method requires image enhancement and image preprocessing. The minutiae feature called template is stored in database, which makes attacker easy to create fake finger or artificial image to spoof the system. Template protection is important issue now a days as biometric systems are widely used for identification. Template protection algorithm like fuzzy vault is applied to fingerprint template.

IV. FUZZY VAULT

Fuzzy vault is used for hiding a key and unlock it with biometric data. Ari Juels *et. al.* [16] described a fuzzy vault scheme which gives a provable security against a computationally unbounded attacker. Fuzzy vault scheme is used to encrypt some cryptographic key using locking elements from set A. This locked data is called vault. If another set B sufficiently matches to set A, vault is decrypted successfully [17].

Enrollment process is done on random polynomial p(x) over a finite field with degree less than k. The minutiae points (encoded as field elements x_1, x_2,….,x_t) are evaluated on the polynomial. These are the genuine points lying on the polynomial. Random chaff points which do not lay on polynomial are added along with genuine points and all these points together is called vault. Vault is stored along with hash value of the concatenated coefficients of the polynomial. For verification, query attributes are encoded as field elements and compared with the stored fuzzy vault [18]. Two procedures which are required for encryption and decryption are LOCK and UNLOCK.

LOCK:

Represent the secret k as a polynomial p. Fingerprint template i.e. minutiae points are given as input A={a1, a2, …a_t}. (R-t) chaff points which are not lying on polynomial p are added to conceal the template. The set R and the parameter triple (k, t, r) together form a fuzzy vault called V_A.

PROCEDURE LOCK

$X, R \leftarrow \phi;$

$p \leftarrow k;$

$for\ i = 1\ to\ t\ do$

$(x_i, y_i) = (a_i, p(a_i));$

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

$X \leftarrow X$ bigcup x_i;
$R \leftarrow R \bigcup (x_i, y_i)$;
for $i = t+1$ *to* r *do*
$x_i \in_U F - X$;
$y_i \in_U F - \{p(x_i)\}$;
$R \leftarrow R \bigcup (x_i, y_i)$;
output R;

UNLOCK:

Unlock a vault V_A and determine the codeword that encodes the secret k. Set A specifies template points in R. If B contains template of input query, B is compared with A, and if it closely matches to A, B will allow to decode with correct codeword. remove the difference between A and B by means of a Reed-Solomon decoding algorithm. the reverse of the procedure employed in Lock. Let $(x_i, y_i) \xleftarrow{(b_i, 0)} R$ denote projection of R onto the x-coordinate b_i. If there is a pair $(b_i, y) \in R$ for any y, then $(x_i, y_i) = (b_i, y)$, otherwise null element is assigned to the (x_i, y_i).

PROCEDURE UNLOCK
$Q \leftarrow \phi$;
for $i = 1$ *to* t *do*
$(x_i, y_i) \xleftarrow{(b_i, 0)} R$;
$Q \leftarrow Q \bigcup (x_i, y_i)$;
$k' \leftarrow RSdecode(k, Q)$;
output k';

V. CONCLUSION

Traditional cryptographic methods cannot be applied for biometric systems because of fuzzy nature of biometric signals. Hence, fuzzy vault scheme is useful for template protection in biometric system such as fingerprint recognition system. Also fuzzy vault is order invariant, which is useful for minutiae points. But, fuzzy vault scheme is vulnerable to correlation attacks. Degradation in biometric performance occurs due to biometric template protection as compared to unprotected biometric systems. One of the way to improve performance is biometric fusion in template protected systems. We argued that the proposed scheme enhances security.

REFERENCES

[1] Ann Cavoukian and Alex Stoianov, "Encyclopedia of Biometrics".

[2] Peng Li , Xin Yang, Hua Qiao, Kai Cao, Eryun Liu, Jie Tian, "An effective biometric cryptosystem combining fingerprints with error correction codes", Expert Systems with Applications 39 (2012) 6562–6574, Elsevier.

[3] Umutuludag, Sharath Pankanti, Salil Prabhakar and Anil K. Jain, "Biometric Cryptosystems: Issues and Challenges", Proceedings of the IEEE, Vol. 92, No. 6, June 2004, pp. 948-960.

[4] Xuebing Zhou, Arjan Kuijperl, Raymond Veldhuis, and Christoph Busch, "Quantifying Privacy and Security of Biometric Fuzzy Commitment", 2011 IEEE, pp.1-8.

[5] Kirk L. Kroeker, "Graphics and Security: Exploring Visual Biometrics", IEEE 2002, pp. 16-21.

[6] M.B. Ramalho, P.L. Correia, L.D. Soares, "Hand-based multimodal identification system with secure biometric template storage", IET Comput. Vis., 2012, Vol. 6, Iss. 3, pp. 165–173.

[7] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, "Biometric Template Security", Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing Volume 2008, pp. 1-17.

[8] Yi C. Feng, Pong C. Yuen, and Anil K. Jain, "A Hybrid Approach for Generating Secure and Discriminating Face Template", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 1, March 2010, pp.103-116.

[9] Ki Young Moon, Daesung Moon, Jang-Hee Yoo, Hyun-Suk Cho, "Biometrics Information Protection using Fuzzy Vault Scheme", 2012 Eighth International Conference on Signal Image Technology and Internet Based Systems, pp.124-128.

[10] Hisham Al-Assam and Sabah Jassim, "Robust Biometric Based Key Agreement and Remote Mutual Authentication", 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012 IEEE, pp. 59-65.

[11] R Ranjan, Sanjay Kumar Singh," Improved and Innovative Key Generation Algorithms for Biometric Cryptosystems", 2012 IEEE, pp. 943-946.

[12] Alawi A. Al-Saggaf, and Lahouari Ghouti, Haridas S. Acharya, "Biometric Cryptosystem with Renewable Templates", WIAR 2012, King Saud University.

[13] Seira Hidano, Tetsushi Ohki and Kenta Takahashi, "Evaluation of Security for Biometric Guessing Attacks in Biometric Cryptosystem using Fuzzy Commitment Scheme", 2012 International Conference of the Biometrics Special Interest Group (BIOSIG).

[14] Yagiz Sutcu, Qiming Li, and Nasir Memon, "Protecting Biometric Templates with Sketch: Theory and Practice", IEEE Transactions on Information Forensics and Security, Vol. 2, No. 3, September 2007, pp. 503-512.

[15] Bian Yang and Christoph Busch, Koen de Groot, Haiyun Xu and Raymond N.J., "Decision Level Fusion of Fingerprint Minutiae Based Pseudonymous Identifiers", 2011 IEEE.

[16] Ari Juels and Madhu Sudan, "A Fuzzy Vault Scheme".

[17] Hailun Liu, Dongmei Sun, Ke Xiong, Zhengding Qiu, "Is Fuzzy Vault Scheme very Effective for Key Binding in Biometric Cryptosystems?", 2011 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2011 IEEE, pp. 279-284.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

[18] Johannes Merkle, Tom Kevenaar, Ulrike Korte, "Multi-Modal and Multi-Instance Fusion for Biometric Cryptosystems", 2012 International Conference of the Biometrics Special Interest Group (BIOSIG).