Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Enhancing Template Security by a Biometric key Generating Cryptosystem: A Review

Sumeet Kaur

Department of Computer Science and Engineering

Punjabi University Regional Centre of Information Technology and Management, India

Abstract: The major catalyst to the rise of biometric methods is its eminence as an identity handling technique. This paper epitomizes the concept of biometric identification system, security, fuzzy vault and pros and cons of fuzzy vault. It also points out the subsequent research that is needed to circumvent the attacks and vulnerabilities.

Keywords: Biometrics, template protection, identification management, fuzzy vault, security.

I. INTRODUCTION

A stable and firm identity management system is essentially needed in order to affray the rampant growth in identity theft and to meet the constantly accelerating security requirements. With the pronounced necessitate for robust human recognition techniques in critical applications such as secure access control, law enforcement and international border crossing, biometrics has positioned itself as a viable technology that can be integrated into large-scale identity management systems.

Biometric recognition is the science of identification of individuals based on their biological and behavioral traits [1]. A biometric system consists of modules which work perpetually to authenticate and verify users. Widespread application of biometric based authentication leads to new problem of security and privacy. Security is a significant aspect of any authentication system and there are various ways to secure the system. The most potentially damaging attack on a biometric system is against the biometric templates that are stored in the system database. Biometric templates are actually compared in a biometric recognition system. So, special attention is given to Template Security which is achieved by Feature Transformations or Biometric Cryptosystems. A cryptographic construction that operates in the key binding mode proposed by Ari Juels and Madhu Sudan[5] is Fuzzy vault i.e. state of the art technique. . Fuzzy vault can handle intra-class variations in the biometric data. In this scheme, real minutiae points are evaluated using single polynomial and chaff points are added to vault for concealing real minutiae points.In this paper, we focus on biometrics security and a biometric cryptosystem(Fuzzy Vault) for securing fingerprint template. Fuzzy vault gives robustness to system as it stores templates in transform domain which aids in securing the template database.

II. BACKGROUND

Identification for the control of access and other scopes can be achieved by utilizing three factors: 1) what you know (e.g. passwords), 2) what you have (e.g. smartcards), and 3) what you are (biometric data identifying a person) [3].These factors can be used individually or amalgam of these three can be used to increase security and compensate the cons of one factor. We might forget the passwords and theft of smartcards is common; a biometric is inseparable from any being and always accessible resulting in comparatively high level of security.

There are two categories of biometrics:

- *Physiological* – also known as static biometrics: Biometrics based on data derived from the measurement of a part of a person's anatomy. For example, fingerprints and iris patterns, as well as facial features, hand geometry and retinal blood vessels.
- *Behavioral* – biometrics based on data derived from measurement of an action performed by a person, and distinctively incorporating time as a metric, that is, the measured action. For example, voice (speaker verification), signature, gait and DNA.

Any human physiological/behavioral characteristic could be a biometrics provided it has the following desirable properties [3].

- *Universality:* This means that every person should have the characteristic.
- *Uniqueness:* This indicates that no two persons should be the same in terms of the characteristic.
- *Permanence:* This means that the characteristic should be invariant with time.

- *Collectability*: This indicates that the characteristic can be measured quantitatively.
- *Acceptability:* This indicates to what extent people are willing to accept the biometric system, and
- *Circumvention:* This refers to how easy it is to fool the system by fraudulent techniques.

The most Common biometric traits include fingerprint, face, iris, hand geometry, voice, palm print, handwritten signatures and gait. There are five major elements in a generic biometric authentication system, namely, sensor, feature extractor, template database, matcher and decision module (see Figure 1).

A. *Biometric Sensor:* A biometric sensor is the interface between the user and the biometric system and its function is to acquire identifiable information from the users.

B. *Preprocessing unit*: This unit enhances the raw biometric (say by removing false minutiae points, removing spur and H-bridge from fingerprint image) to ensure that the acquired biometric can be reliably processed by a feature extractor.

C. *Feature extractor*: Feature extractor processes the scanned biometric data to extract the salient information (feature set) that is useful in distinguishing between different users.

D. *Template Generator:* The extracted feature set is stored in a database as a template indexed by the user's identity information. A template is a small file derived from the distinctive features of a user's biometric data, used to perform biometric matches. Biometric systems store and compare biometric templates, not biometric data.

E. *Matcher Module:* The matcher module is usually an executable program, which accepts two biometric feature sets (from template and query respectively) as inputs, and outputs a match score (S) indicating the similarity between the two sets. This module compares query or test biometric data with the pre-stored template.

F. *Decision module*: Finally the decision module makes the identity decision and initiates a response to the query.

G. *Stored template*: Since the template database could be geographically distributed and contain millions of records, maintaining its security is a trivial task.

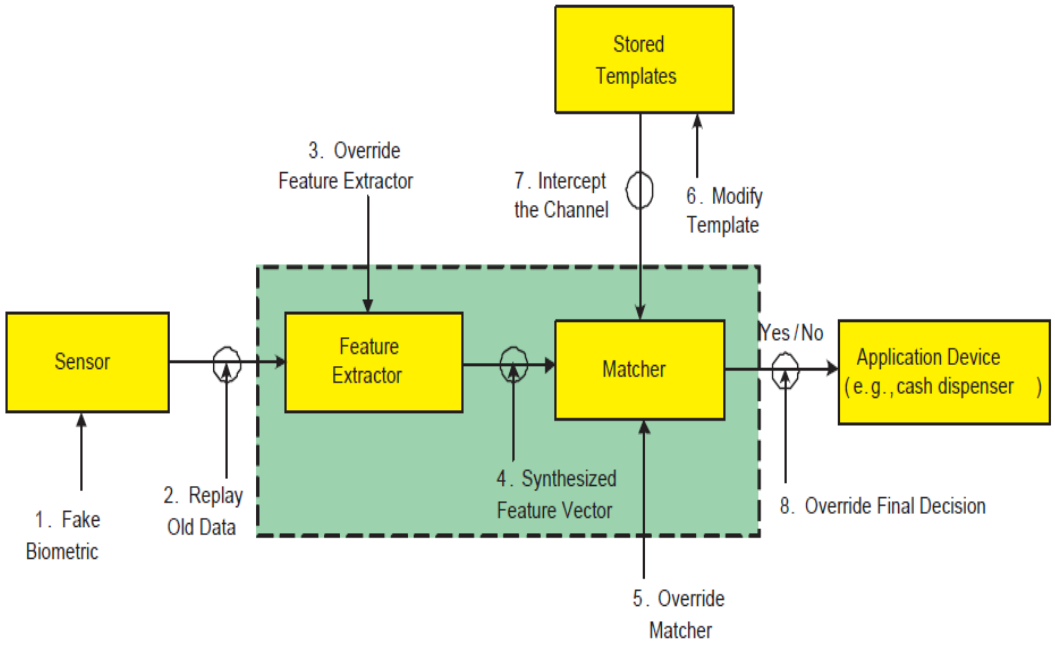

Fig. 1 Biometrics Security Model [2]

III. SECURITY

Template security is one of the most important factor in designing a secure biometric system and it needs timely and severe attention. Most of the available template protection techniques fail to meet all the desired requirements of a practical biometric system like revocability, security, privacy, and high matching accuracy.

ATTACKS	HAZARDS	EFFECTS	REMEDIES
Template database compromise	Privacy Loss (template theft, database cross-matching)	Gain access to the template database	Encrypt the templates
Fake enrollments	Denial of service (system's template database overflow) e.g. multiple email accounts	i) Generating fake biometric features ii)Enrolling fake biometrics	Controlled enrollment procedure
Hill Climbing	Privacy Loss (template theft)	i) Injecting biometric features ii) Obtaining match score	Avoid outputting the match scores
Biometric Spoof	Intrusion (multiple systems)	i) Acquiring biometric features ii) Creating reliable spoof	Liveness detection techniques

Fig. 2 Characterization of different outbreaks (attacks) on a biometric recognition system.

IV. FUZZY VAULT AND RELATED WORK DONE

Fuzzy vault was brought up by Juels and Sudan [5], that aims to secure vital data with the biometric template in a way that exclusively the authorized user can access the secret by providing the genuine biometric. Fuzzy vault is a cryptographic construction that operates in the key binding mode and, in principle, can compensate for intra-class variations in the biometric data [6]. Ari Juels et al. presented the fuzzy vault scheme. Fuzzy vault aims to secure vital data with the biometric template in a way that exclusively the authorized user can access the secret by providing the genuine biometric. A fuzzy commitment scheme can be understood with the help of simple example of Alice and bob, where Alice can lock her telephone number tel_a using the set A, yielding a vault denoted by V_a. If Bob tries to unlock the vault V_a using his own set B, he will succeed provided that B overlaps largely with A. On the other hand, anyone who tries to unlock V_a with a set of favorite movies differing substantially from Alice's will fail, helping to ensure that Alice's set of favorites remains private. Thus, a fuzzy vault may be thought of as a form of error-tolerant encryption operation where keys consist of sets [8].

Now we discuss literature survey about the biometric system, vulnerabilities in biometric system and various techniques to secure the biometric system among which fuzzy vault is extended for research work. Various research papers related to fuzzy vault and its implementation which is a template protection scheme are discussed in this section Hisham Al-Assam et al. proposed a technique for biometric template security. A novel and an efficient approach to biometric template protection that meets the four properties diversity, security, performance and revocability are discussed. This scheme can be incorporated into any biometric verification scheme while maintaining, if not improving, the accuracy of the original biometric system [7].Clancy et al. proposed a fingerprint vault based on fuzzy vault of Juels and Sudan. He used multiple minutiae locations as elements of locking set. This paper describes the use of random points known as chaff points which do not lie on polynomial. Chaff points are simple dummy points that are randomly generated, that aim to hide and protect real minutiae points [9]. Uludag et.al proposed a method using simple translation and rotation for alignment because reference minutiae cannot be same at enrolment and verification [14].Karthik Nandakumar et.al proposed improved fuzzy vault by using minutiae matcher during decoding to compensate for non-linear distortion in fingerprints [13].Anil K. Jain et.al analyzed how two challenges of fuzzy vault are being addressed in practice and how the design choices affect the trade-off between the security and matching accuracy. Though much progress has been made over the last decade, they mentioned that fingerprint template protection algorithms are still not sufficiently robust to be incorporated into practical fingerprint recognition systems [12]

BENEFITS OF FUZZY VAULT:

a. This technique generates the secret data from the registered template and query biometric data. Therefore, it excels not only in template security but also in secret data conceal ability.
b. The fuzzy vault scheme stores only a transformed version of the template, which makes it applicable to various modalities besides fingerprints.
c. It can handle intra-class variation such as variation in placing finger on scanner.
d. Fuzzy vault is also applicable to other biometrics say iris, face.

RISKS IN FUZZY VAULT

a. Positioning of the query with transformed version of biometric is perquisite.

b. The chaff points that are generated later are likely to have smaller free area. There are more neighboring points near the point with small free area and it becomes relatively simple to detect them. [10]

c. If there is generation of 2 or more fuzzy vaults from the same point but keys and random chaff are different, the minutiae are credibly recoverable by matching two templates.[11]

d. In forensics (crime scenes) or labor class due to bruises and rough texture, only few minutiae (fingerprints) are encountered. So, FRR is high in these cases. A fuzzy vault for this platform is needed that can reduce FRR.

IV. DISCUSSION AND CONCLUSION

From the previous work it is concluded that the combination of biometric with cryptography has both features of biometric system and cryptography. Fuzzy vault is reliable and effective method for biometric template security. It stores templates in transform domain which secures the template database and is applicable to modalities other than fingerprints. It is a system that can provide required concealment of template. The existing fuzzy vault system has some unaddressed issues in its implementations. The alignment between template and query is a serious issue in its implementation.FRR is high in case of bruised or rough texture of fingerprints. These issues if handled can make system applicable more practically and efficiently.
For future work, one can try to implement fuzzy vault using more than two polynomials. One can also work on automatic alignment of query fingerprint image in order to enhance the proposed scheme. The implementation of fuzzy vault is difficult at higher level and reduces its accuracy.FRR can be reduced for special cases of query matching(for usage in forensic and labor class).Most of the available template protection techniques fail to meet all the desired requirements of a practical biometric system like revocability, security, privacy, and high matching accuracy. In particular, protecting the fingerprint templates has been a difficult problem due to large intra-user variations (e.g., rotation, translation, nonlinear deformation, and partial prints. The need is to reduce the computation time and improve its efficiency. The proposed research work is to find and remove some of the discrepancies in implementation of fuzzy vault.

References

1) ANSI. Harmonized Biometrics Vocabulary. standing document 2, version 8, 2007.
2) Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, "Biometric Template Security", in Journal on Advances in Signal Processing, Michigan State University, pp. 1-17, 2007.
3) Abhishek Nagar, "Biometric Template Security", Ph.D. Thesis, 2012.
4) NTSC. Biometrics in Government post 9/11. http://www.ostp.gov/galleries/NSTCReports/BiometricsinGovernmentPost9-11.pdf.
5) Ari Juels and Madhu Sudan, "A Fuzzy Vault Scheme" , in IEEE International Symposium Information Theory, Lausanne, Switzerland, pp. 408, 2002.
6) Anthony Vetro, Stark Draper, Shantanu Rane, Jonathan Yedidia, " Securing Biometric data", preprint of a chapter in distributed source coding, p. l. dragotti and m. gastpar eds., academic press, Feb. 2009.
7) Hisham Al-Assam, Harin Sellahewa, & Sabah Jassim, "A Lightweight approach for biometric template protection", to appear in the proceedings of SPIE Mobile multimedia/image processing, security, and applications, Florida, USA March 2009.
8) Vani Perumal, Dr. Jagannathan Ramaswamy, "An Innovative Scheme For Effectual Fingerprint Data compression using Bezier Curve Representation", in International Journal of Computer Science and Information Security, Vol. 6, No. 1, pp. 149-157, Oct 2009.
9) Ruifang Wang, "A Novel Fingerprint Template Protection Scheme Based on Distance Projection Coding", in International Conference of Pattern Recognition, pp. 886-889, Sep 2010.
10) Hoi Ting Poon and Ali Miri, "A Collusion Attack on the Fuzzy Vault Scheme", University of Ottawa, ISC, pp. 27-34, 2009.
11) Mohammad Khalil-Hani, Rabia Bakhteri, "Securing Cryptographic Key with Fuzzy Vault based on a new Chaff Generation Method", in proceedings of IEEE, pp. 259-265, 2010.
12) Anil K. Jain, Karthik Nandakumar and Abhishek Nagar, "Fingerprint Template Protection : From theory to practice " to be appear in P.Camisi (ed), Springer, 2012.
13) Karthik Nandakumar, *Anil K. Jain and* Sharath Pankanti, "Fingerprint-Based Fuzzy Vault:Implementation and Performance", IEEE, 2007.
14) Umut Uludag,Sharath Pankanti and Anil K . Jain, "Fuzzy vault for fingerprints" , in Proceedings of Audio and Video based biometric Person Authentication, Rye Town, NY, 2005

