Multibiometric Template Security using Fuzzy Vault

Smita Mahajan
Symbiosis institute of technology
Symbiosis international university
Pune, India

Asmita Deshpande
Information Technology Department, PctCoE
Mumbai University
Thane (w)

ABSTRACT
The popularity of biometrics and its widespread use introduces privacy risks. Template security is a critical issue in biometric systems because biometric templates cannot be easily revoked and reissued. While multibiometric systems overcome limitations such as non-universality and high error rates that affect unibiometric systems, they require storage of multiple templates for the same user. Securing the different templates of a user separately is not optimal in terms of security. Hence, we propose a scheme for securing multiple templates of a user as a single entity. . We derive a single multibiometric template from the individual templates and secure it using the fuzzy vault framework. We demonstrate that a multibiometric vault provides better recognition performance and higher security compared to a unibiometric vault. One of the main vulnerabilities of a biometric system is the exposure of a user's biometric template information. Access to a user's template can lead to (i) creation of physical spoofs (ii) replay attacks, and (iii) cross-matching across different databases to covertly track a person. Furthermore, unlike passwords or tokens, compromised biometric templates are not revocable. Due to these reasons, template security is essential to protect both the integrity of the biometric system and the privacy of the users. Although a number of approaches have been proposed to secure templates, most of these schemes have been designed primarily to secure a single template.

General Terms
Pattern Recognition, Security, Algorithms, Fuzzy Vault,

Keywords
Keywords are your own designated keywords which can be used for easy location of the manuscript using any search engines.

1. INTRODUCTION
"Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. However, biometric identification has eventually a much broader relevance as computer interface becomes more natural. Knowing the person with whom you are conversing is an important part of human interaction and one expects computers of the future to have the same capabilities. A number of biometric traits have been developed and are used to authenticate the person's identity. The idea is to use the special characteristics of a person to identify him. By using special characteristics we mean the using the features such as face, iris, fingerprint, signature, etc. The method of identification based on biometric characteristics is preferred over traditional passwords and PIN based methods for various reasons such as: The person to be identified is required to be physically present at the time-of-identification. Identification based on biometric techniques obviates the need to remember a password or carry a token. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic". Compared to traditional (uni)biometric authentication, multibiometric Template Security using Fuzzy Vault Systems offer several advantages such as better recognition accuracy, increased population coverage, greater security, and flexibility and user convenience.[1] However, a multibiometric system stores multiple templates for the same user corresponding to the different biometric sources. One of the main vulnerabilities of a biometric system is the exposure of a user's biometric template information. Furthermore, unlike passwords or tokens, compromised biometric templates are not revocable. Protecting the individual templates separately is analogous to having a system that requires multiple smaller passwords, which is less secure than a system that uses a single large password.[9] Hence this paper proposes a unified scheme to secure template.

2. HISTORY
The history of biometrics dates back to a long time. Possibly the most primary known instance of biometrics in practice was a form of finger printing being used in China in the 14th century, as reported by explorer Joao de Barros. Barros wrote that the Chinese merchants were stamping children's palm prints and footprints on paper with ink so as to differentiate the young children from one another. This is one of the most primitive known cases of biometrics in use and is still being today. Bertillon developed a technique of multiple body measurements which later got named after him - Bertillonage. His method was then used by police authorities throughout the world, until it quickly faded when it was discovered that some people shared the same measurements and based on the measurements alone, two people could get treated as one. After the failure of Bertillonage, the police started using finger printing, which was developed by Richard Edward Henry of Scotland Yard, essentially reverting to the same methods used by the Chinese for years. (Which still is going strong!) Biometric history in the recent past (three decades) has seen drastic advancements and the technology has moved from a single method (fingerprinting) to more than ten prudent methods.

3. WHY MULTIBIOMETRICS?
Biometric systems installed in real-world applications must contend with a variety of problems. [2] Among them are: Noise in sensed data. A fingerprint with a scar and a voice altered by a cold are examples of noisy inputs. Noisy data could also result from defective or improperly maintained sensors (for example, accumulation of dirt on a fingerprint sensor) and unfavorable ambient conditions (for example, poor illumination of a user’s face in a face recognition

system). Noisy biometric data may be incorrectly matched with templates in the database resulting in a user being incorrectly rejected.2.Intra-class variations. The biometric data acquired from an individual during authentication may be very different from the data used to generate the template during enrollment, thereby affecting the matching process distinctiveness. While a biometric trait is expected to vary significantly across individuals, there may be large similarities in the feature sets used to represent these traits. Thus, every biometric trait has some theoretical upper bound in terms of its discrimination capability. Non-universality. While every user is expected to possess the biometric trait being acquired, in reality it is possible for a subset of the users to not possess a particular biometric. A fingerprint biometric system, for example, may be unable to extract features from the fingerprints of certain individuals, due to the poor quality of ridges. [3]Multibiometric systems address the problem of non-universality, since multiple traits can ensure sufficient population coverage. Furthermore, multibiometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user. [4]

4. MULTIBIOMETRIC SYSTEM

4.1.1 Description, Vulnerabilities and Security

Let us see how a typical biometric system works. A generic biometric system consists of five components: Sensor, feature extractor, template database, matcher, and decision module. Fig. 1 shows a basic block diagram of a biometric system.

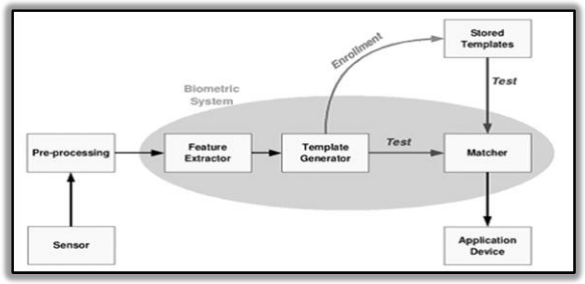

Fig. 1: Basic Block Diagram of a Biometric System

In general, these systems run as follows: In the enrollment phase, the biometric templates are processed and stored in the database. Then, in the verification phase, the biometric query template extracted from the user in this moment is compared with the one already stored in the database. If this comparison succeeds the user identity is verified, otherwise she is rejected. In most cases, the applications in which biometric systems are used are unimodal, i.e., they rely on the evidence of a single source of information for authentication. But these systems suffer from some problems, among them the most important are the intra and inter-user variability. The intra-user variability measures the differences of two biometric templates extracted from the same user, while the inter-user variability measures the similarities between two biometric templates extracted from different users. These two measurements can cause not to recognize a known user or to recognize an attacker as a known user, respectively. The most straightforward way to secure a biometric system, including the template, is to put all the system modules and the interfaces between them on a smart card. These systems are known as match-on-card and their advantage is that the biometric information never leaves the card. The drawback is that these systems are not appropriate for large-scale applications and it is possible to get the template from a stolen card. So, both the system and the template must be protected. Several approaches, known as cancelable biometrics, fuzzy vault scheme, fuzzy vault extractor have been proposed to secure biometric templates.

4.1.2 Template protection schemes

There are mainly two categories of template protection schemes

1. Feature transformation approach
2. Biometric cryptosystem

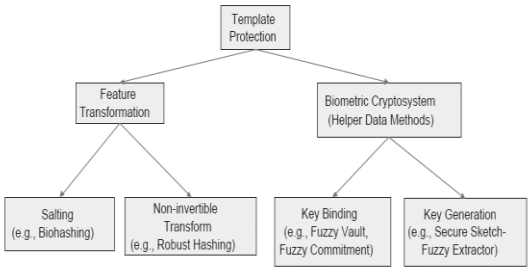

Fig. 2: template protection schemes

In the feature transform approach, the biometric features are modified using a transformation function, whose parameters are typically derived from a random key [6-7]. Only the transformed template is stored and matching takes place directly in the transformed domain. The feature transform approach can be further categorized as (i) salting - the transform is invertible, so the security is based on the secrecy of the key, and (ii) non-invertible transform - a one way function where it is computationally hard to invert a transformed template even if the key is known. In a biometric cryptosystem some public information about the biometric template (referred to as helper data) is stored. The helper data is usually obtained by binding a key K (that is independent of the biometric features) with the template T. Hence, such schemes are known as key- binding biometric cryptosystems. Matching is performed indirectly by recovering the key from the helper data using the query biometric features.[8] The issue of biometric template security is gaining importance due to concerns about the potential misuse of stolen templates. There are two major concerns regarding a stolen biometric template: (i) spoofing and (ii) privacy intrusion. If an adversary is able to access the stored templates, he can create a spoof biometric from the template and present it to the system. Due to limited live ness detection capability of current biometric systems, spoofing is major security vulnerability. Further, an adversary can cross-link the stolen templates with other biometric databases, allowing him to track the activities of a person covertly. We focus here on improving the security and performance of fuzzy vault which is a popular biometric cryptosystem. Fuzzy vault can effectively utilize the natural representation of fingerprint minutiae i.e. an unordered set. In addition to minutiae position and orientation, we utilize additional attributes extracted from a minutia's neighborhood to improve the vault. In particular, we show that minutiae descriptors, which contain local ridge orientation and ridge frequency information, have sufficient saliency to reduce the FAR of a fingerprint fuzzy vault. Moreover, we also show that "encrypting" the polynomial evaluations in the vault using the minutiae descriptors increases the vault security.

5. FUZZY VAULT FRAMEWORK

A well-known example of biometric cryptosystem is the fuzzy vault framework, which is designed to secure biometric features that are represented as an unordered set. In this paper, we propose a unified scheme to secure multiple templates of a user in a multibiometric system by following steps.

1. Encoding: transforming features from different biometric sources into a common representation,
2. Performing feature-level fusion to derive a single multibiometric template.
3. Securing the multibiometric template using a single fuzzy vault construct. [5]

6. FINGERPRINT MINUTIAE ENCODING

Fingerprints are the ridge and furrow patterns on the tip of the finger and are used for personal identification of people .An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints in a database. A fingerprint is the pattern of ridges and valleys (also called furrows) on the surface of a fingertip. Each individual has unique fingerprints. The uniqueness of a fingerprint is exclusively determined by the local ridge characteristics and their relationships. These local ridge characteristics are not evenly distributed. Most of them depend heavily on the impression conditions and quality of fingerprints. The two most prominent local ridge characteristics, called minutiae are ridge ending and ridge bifurcation. A ridge ending is defined as the point where a ridge ends abruptly. A ridge bifurcation is defined as the point where a ridge forks or diverges into branch ridges. A good quality fingerprint typically contains about 40–100 minutiae .Automatic fingerprint matching depends on the comparison of these local ridge characteristics and their relationships to make a personal identification. A critical step in fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images, which is a difficult task.

Examples of minutiae are shown in figure 3.

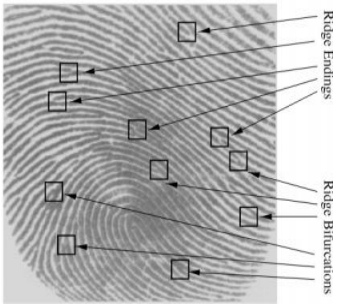

Fig 3: Fingerprint minutiae

6.1.1 *Encoding* steps

1. to obtain a 16-bit number which is then considered as an element in GF.
2. Only a fixed number (denoted by r) of minutiae are selected for vault construction based on their quality.
3. Set of high curvature points are extracted from the template image and stored along with the vault. The high curvature points do not reveal any information about the minutiae.
4. Let X 1 is the generated template by this way.
5. Now in the same way we can encode other biometric traits such as iris, palm prints, face to transform the features extracted from these different traits into a common representation.
6. Let X2 is another generated template by different trait. say Iris modality.
7. But securing the different templates of a user separately is not optimal in terms of security.
8. Hence we have to secure multiple templates of a user as a single entity

6.1.2 *Feature-level Fusion*

1. Let X1 and X2 be the set of feature points generated by the fingerprint and iris modalities.
2. The union, X, of the two sets X1 and X2 is formed such that the Hamming distance between any two elements in the union is greater than or equal to 2.
3. The high curvature points from the fingerprint and the transformed iris code template are stored along with the vault as helper data.
4. During authentication, the query biometric (iris code) is used to recover the transformation key from the transformed template.
5. During authentication, the query iris code is used to recover the transformation key from the transformed iris code template.
6. The union of the two unlocking sets (l1',l2') is considered as the final unlocking set that is used for polynomial reconstruction

6.1.3 *Designing a fuzzy vault construct*

1. Let X denotes a biometric template with r elements.
2. The user selects a key K, encodes it in the form of a polynomial P of degree n and evaluates the polynomial P on all the elements in X.
3. The points lying on P are hidden among a large number (denoted by s) of random chaff points that do not lie on P and the union of genuine and chaff point sets constitutes the helper data or vault V.
4. In the absence of user's biometric data, it is computationally hard to identify the genuine points in V, and hence the template is secure.
5. During authentication, the user provides a biometric query denoted by X'
6. If X' overlaps substantially with X, the user can identify many points in V that lie on the polynomial.
7. If the number of discrepancies between X and X' is less than (r -n)/2, Reed-Solomon decoding can be applied to reconstruct P and the authentication is successful.
8. On the other hand, if X and X' do not have sufficient overlap, it is infeasible to reconstruct P and the authentication is unsuccessful.

6.1.4 Actual implementation of multibiometric vault

There are two phases of implementation.

1. Locking Phase
2. Unlocking Phase

6.1.4.1 Locking Phase

1. The key of 128 bits provided by user is encoded using Cyclic Redundancy Check (CRC) and the K(crc) of 144 bits is obtained
2. K (crc) is truncated into 9 non-overlap segments (c0, c1, c2…c8) of 16 bits, from which a 8-order polynomial can be obtained.
3. The polynomial obtained is as
   a. $f(x)\ c0 + c1x + c2x^2 + \ldots.. + c8x^8$
4. From all components of transformed feature vector R, we can obtain the set G (of pairs
   a. $G=\{(r_i, f(r_i)),\ i=1,2,3\ldots.M\}$
5. Then the chaff points $C=\{(s_j, w_j), j=1,2,3\ldots.Nc\}$ }
6. (Nc>>M) are generated by the following rules
   a. $s_j \neq r_i$
   b. $w_j \neq f(s_j)$
7. The fuzzy vault is obtained by taking the union of two sets *C and G*
   a. *V= C Union G*
8. $=\{(a_k, b_k)\ ,k=1,2,3\ldots..,M + Nc)\}$

The diagrammatic representation of Locking phase in given in the figure 4.

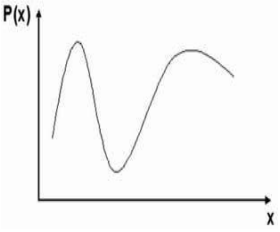

Fig. 4: Create a Polynomial

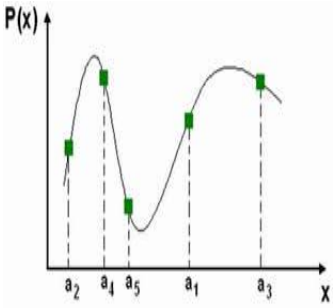

Fig. 5 Project locking elements on to the polynomial

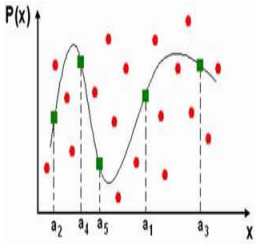

Fig.6: Randomly create & add chaff points

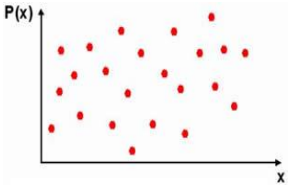

Fig.7: Final appearance of the Vault

6.1.4.2 Unlocking Phase

During authentication, the query biometric features are used to filter out the chaff points(C) in the vault V resulting in an unlocking set L'

1. Several candidate sets of size (n + 1) are generated from L' and polynomials are reconstructed using Lagrange interpolation. From this reconstructed polynomial we can get K*(crc) of 144 bits
2. CRC based error detection is used to identify the correct polynomial and hence, decode the correct key
3. K*(crc) is divided by CRC (16 bits) , if the remainder is zero, recovered key is correct.
4. Furthermore, if the recovered key is equal to the key provided by user, the authentication is successful. Otherwise, it is failed. The diagrammatic representation of Unlocking phase is given in following figures.The

location and orientation attributes of a minutia point are quantized and concatenated in order.

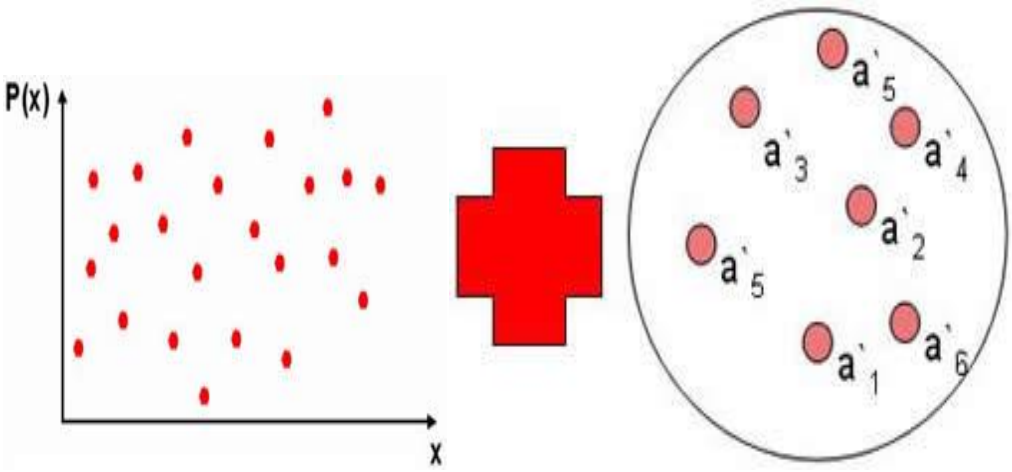

Fig 8: Fuzzy Vault of claimed ID (left) and test unlocking set (right)

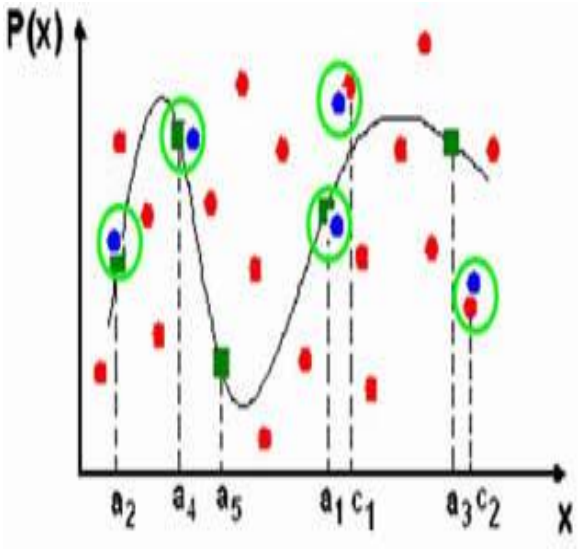

Fig 9: Test unlocking set matched against the vault.

7. CONCLUSION

We have proposed a framework for securing multiple biometric templates of a user in a multibiometric system as a single entity. This is achieved by generating a single multibiometric template using feature level fusion and securing the multibiometric template using the fuzzy vault construct. We have also implemented a fully automatic fuzzy vault system for securing the fingerprint minutiae and iris code templates. While we use an existing fingerprint fuzzy vault implementation to secure fingerprint minutiae, we propose a new vault implementation for securing iris codes. A salting transformation based on a transformation key is used to indirectly convert the fixed-length binary vector representation of iris code into an unordered set representation that can be secured using the fuzzy vault. We have shown that the multibiometric vault can secure templates from different biometric sources such as multiple fingerprint impressions, multiple fingers and multiple modalities such as fingerprint and iris. We have also demonstrated that the multibiometric vault provides better recognition performance as well as higher security compared to the unibiometric vaults.

8. REFERENCES

[1] A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics. Springer, 2006.Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[2]] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint Image Reconstruction From Standard Templates," IEEE Trans. on PAMI,vol. 29, no. 9, pp. 1489-1503, 2007.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[3] A. Vetro and N. Memon, "Biometric System Security," Tutorial presented at Second International Conference on Biometrics, Seoul, South Korea, August 2007.Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[4] Y Sutcu, Q. Li, and N. Memon, "Secure Biometric Templates from Fingerprint-Face Features," in Proceedings of CVPR Workshop on Biometrics, Minneapolis, USA, June 2007.Y.T. Yu, M.F. Lau, "A

comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

[5] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," in Proc. of IEEE Intl. Symp. on Info. Theory, Lausanne, Switzerland, 2002, p. 408.

[6] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis, "Practical Biometric Authentication with Template Protection," in Proceedings of Fifth Intl. Conf on AVBPA, Rye Town, USA, July 2005, pp. 436-446.

[7] S. C. Draper, A. Khisti, E. Martinian, A. Vetro, and J. S. Yedidia, "Using Distributed Source Coding to Secure Fingerprint Biometrics,"in Proceedings of ICASSP, vol. 2, Hawaii, April 2007, pp. 129-132.

[8] S. C. Draper, A. Khisti, E. Martinian, A. Vetro, and J. S. Yedidia, "Using Distributed Source Coding to Secure Fingerprint Biometrics,"in Proceedings of ICASSP, vol. 2, Hawaii, April 2007, pp. 129-132.

[9] Y. Sutcu, Q. Li, and N. Memon, "Protecting Biometric Templates with Sketch: Theory and Practice," EEE Transactions on Information Forensics and Security, vol. 2, no. 3, pp. 503-512, September2007-2008.