IJITKM 0973-4414 Volume-9, Number-2 Jan-Jun 2016 pp. 9-13 **Impact Factor 2.8** available online at www.csjournalss.com

# Different Protection Schemes for Biometric Templates

Ramesh Kumar, Naveen Monga
Department of Computer Science, SUS Govt. College, Matak Majri, Indri, Karnal
ramesh_aurora@yahoo.com, navmong@yahoo.co.in

**Abstract:** Biometrics access control system offer some significant over standard method of access control. Biometrics recognition provides a strong link between an individual and a claimed identity. Biometrics template security system evaluates an individual's physiological and behavioral traits data, it is the strongest and most reliable physical privacy and security technique used for authentication. biometrics measurable features ensures the security of information of E-commerce, such as on-line banking and shopping malls. In Particular, here discuss security of biometrics template which is significant concern because, unlike keys and password, compromised biometrics template cannot be invalidate or release. To improve template security in biometrics authentication using efficient data encryption technology. In biometric template protection schemes their advantages and limitations in terms of accuracy and privacy.

**Keywords:** Introduction, templates vulnerability, template protection scheme.

## I. Introduction

Biometrics system identifies a person by using his/her physiological and behavioral traits. In traditional system people identification done with their scar, color or by choosing password and any token key etc. Now the current biometric extracts with hand geometry, veins, voice and finger print. Biometrics takes once step high in security level. For secure identification and personal verification. In future even the on line banking transaction can be done with highly secure ,to avoid vulnerable attacks.

A Biometric can be either Identification (who am I) 1: n or Verification (am I who I claim I am?)1:1..

## *II. How Templates are vulnerable?*

At the level of security, the failure modes of a biometric system can be classified 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 distinguishable of the specific biometric trait. In adversary attacks, hacker (or possibly an organized group) attempts to circumvent the biometric system for personal gains. We further classify the adversary attacks into three types based on factors that enable an adversary to compromise the system security. These factors include system administration, non secure infrastructure, and biometric overtones.

### *A. Intrinsic Failure*

Intrinsic failure is the security error due to an inaccurate decision made by the biometric system. A biometric verification system can make two types of errors in decision making, namely, false accept and false reject. A genuine (legitimate) user may be falsely rejected by the biometric system due to the large differences in the user's stored template and query biometric feature sets. These intrauser variations may be due to incorrect interaction by the user with the biometric system (e.g., changes in pose and expression in a face image) or due to the noise introduced at the sensor (e.g., residual prints left on a fingerprint sensor). False accepts are usually caused by lack of individuality or uniqueness in the biometric trait which can lead to large similarity between feature sets of different users (e.g., similarity in the face images of twins or siblings). Both intruder variations and intruder similarity may also be caused by the use of obscure features and delicate matchers. Sometimes, a sensor may fail to acquire the biometric trait of a user due to limits of the sensing technology or adverse environmental conditions.

### *B. Adversary attacks*

An adversary intentionally stages an attack on the biometric system whose solution depends on the evasiveness in the system design .We classified the adversary attacks into three main classes: administration attack, vulnerable infrastructure, and biometric overtness.

*1) Administration attack*

This attack, also known as the insider attack, refers to all vulnerabilities introduced due to inappropriate administration of the biometric system. These include the integrity of the enrollment process (e.g., validity of certificate presented during enrollment), collusion (or coercion) between the opposition and the system administrator or a authenticated user.

*2) Vulnerable infrastructure*

The infrastructure of a biometric system consists of hardware, software, and the communication channels between the various modules. There are a number of ways in which an adversary can manipulate the biometric infrastructure that can lead to security breaches.

*3) Biometric overtness*

It is possible for an adversary to covertly acquire the biometric characteristics of a genuine user (e.g., fingerprint impressions lifted from a surface) and use them to create physical artifacts (gummy fingers) of the biometric trait.

*c. Attacks at the interface between modules*

An adversary can intrude on the communication interfaces between different modules. For instance, he can place an interfering source near the communication channel .If the channel is not secured physically or cryptographically, an adversary may also intercept and/or modify the data being transferred. A common way to secure a channel is by cryptographically encoding all the data sent through the interface, say using public key infrastructure. But even then, an adversary can stage a replay attack by first intercepting the encrypted data passing through the interface when a genuine user is interacting with the system and then sending this captured data to the desired module whenever he wants to break into the system. A countermeasure for this attack is to use time-stamps (Lam and D. Gollmann, 1992), (K. Lam and T. Beth, 1992) or a challenge/response]. mechanism (R. M. Bolle).

*III. Template Protection scheme*

An ideal biometric template protection scheme should possess the following four properties (D. Maltoni).

1) Diversity: the secure template must not allow cross matching across databases, thereby ensuring the user's privacy.

2) Revocability: it should be straightforward to revoke a compromised template and reissue a new one based on the same biometric data

(3) Security: it must be computationally hard to obtain the original biometric template from the secure template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template.

(4) Performance: the biometric template protection scheme should not degrade the recognition performance (FAR and FRR) of the biometric system.

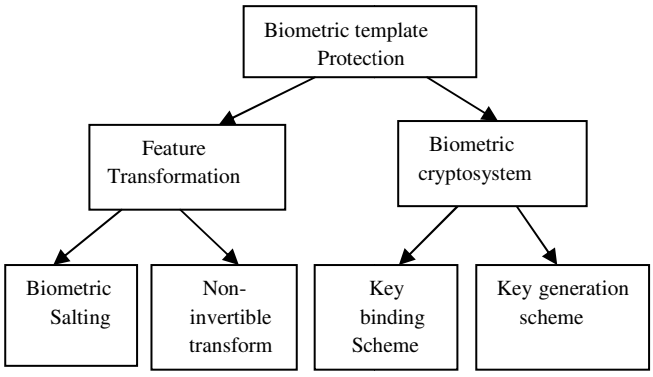


Figure1. Different Biometric template Protection

Table: Template Protection Schemes

| **Approach** | **Template security depends on** | **Entities to be stored** | **Limitation** |
|---|---|---|---|
| Feature Trans-formation | Secrecy of User Specific key. | Transformed Template | Once the key is stolen template is no longer secure |
| Non invertible Transform | Non-invertibility Of Transformed Function | Transformed Template key. | Non-invertibility |
| Key binding cryptosystem | Security depend On Information revealed by helper data. | Transformed Template, helper data. | Helper data carefully Design. |
| Key generating cryptosystem | Security depends on the info revealed by helper data. | Transformed Template, Helper data | Non revocable in nature Key stability and key entropy. |

*A. Salting*

Salting or Biohashing is a template protection approach in which the biometric features are transformed using a function defined by a user-specific key or password. Since the transformation is invertible to a large extent, the key needs to be securely stored or remembered by the user and presented during authentication. This need for additional information in the form of a key increases the entropy of the b iometric template and hence makes it difficult for the opposition to guess the template.

*B Noninvertible transform*

In this approach, the biometric template is secured by applying a noninvertible transformation function to it. Noninvertible transform refers to a one-way function, F , that is "easy to compute" (in polynomial time) but "hard to invert" (given F (x), the probability of finding x in polynomial time is small). The parameters of the transformation function are defined by a key which must be available at the time of authentication to transform the query feature set. The main characteristic of this approach is that even if the key and/or the transformed template are known, it is computationally hard (in terms of brute force complexity) for an adversary to recover the original biometric template.

*C Key-binding biometric cryptosystem*

In a key-binding cryptosystem, the biometric template is secured by monolithically binding it with a key within a cryptographic framework. A single entity that embeds both the key and the template is stored in the database as helper data. This helper data does not reveal much information about the key or
the biometric template, that is, it is computationally hard to decode the key or the template without any knowledge of the user's biometric data. Usually the helper data is an association of an error correcting code (selected using the key) and the biometric template. When a biometric query differs from the template within certain error tolerance, the associated codeword with similar amount of error can be recovered, which can be decoded to obtain the exact codeword, and hence recover the embedded key. Recovery of the correct key implies a successful match.

**Advantages**

This approach is tolerant to intrauser variations in biometric data and this tolerance is determined by the error correcting capability of the associated codeword.

*C. cryptographic key generation*

biometrics is an attractive proposition because intrauser variability is difficult problem. Early biometric key generation schemes such as those by Chang et al. (Y.-J. Chang, 2004) and Veilhauer et al. (C. Vielhauer, 2002) employed user-specific quantization schemes. Information on quantization boundaries is stored as helper data which is used during authentication to account for intrauser variations. Dodis et al. (Y.Dodis, 2006), (Y. Dodis, 2002)introduced the concepts of secure sketch and fuzzy extractor in the context of key generation from biometrics. The secure sketch can be considered as helper data that leaks only limited information about the template..The fuzzy extractor is a cryptographic primitive that generates a cryptographic key from the biometric features. Secure sketch and multimodal systems (face and fingerprint) (Y. Sutcu, 2007)has also been proposed.

Key generating biometric cryptosystems usually suffer from low distinguishable which can be assessed in terms of key stability and key entropy. Key stability refers to the extent to which the key generated from the biometric data is repeatable. Key entropy relates to the number of possible keys that can be generated.

*IV Various Security Enhancement Technique*

*A. Biometrics Steganography*

Steganography principles to hide biometric data (e.g., fingerprint minutiae) in host images (e.g., faces).

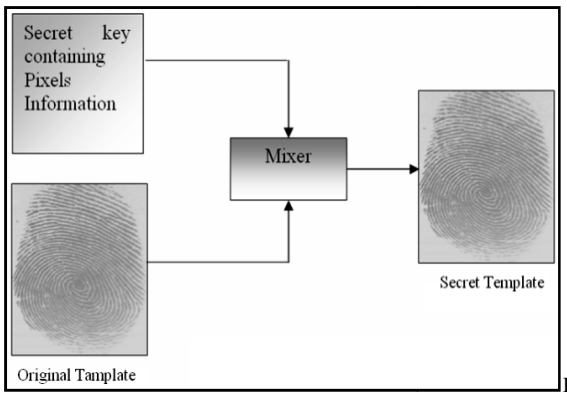


Fig: biometric steganography (16)

This is particularly useful in distributed systems where the raw biometric data may have to be transmitted over a non-secure communication channel. Embedding biometric data in an insipid host image secure or safe an snoop from accessing sensitive or secured template data. The authors also discuss a novel application wherein the facial features of a user (i.e., eigen-coefficients) are embedded in a host fingerprint image (of the user).

*B. Biometrics Watermarking*

watermarking technique to disclose regions in a fingerprint image that have been intrude by an intruder. In the proposed scheme, a turbulent mixing procedure is employed to transform a visually detectable watermark to a random-looking textured image in order to make it volatile against attacks.This "mixed" image is then included in a fingerprint image.The authors show that the presence of the watermark does not affect the feature extraction process. The use of a watermark also transmit copyright capability by identifying the origin of the raw fingerprint image

.

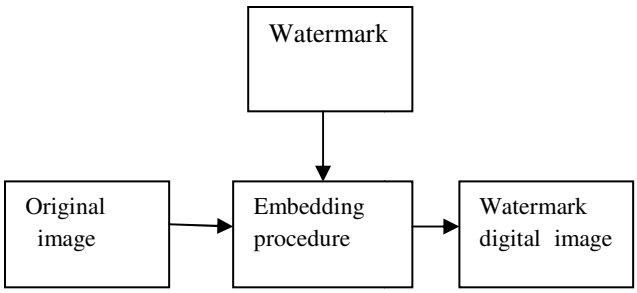


*Fig Biometrics watermarking*

*C. Biometrics cryptography*

cryptography defined an approach to create a distinctive and more secure cryptographic key from biometrics template. captured images are processed to generate template or code to be utilized for the encryption and decryption tasks. The international standard cryptography algorithm – AES has been adopted in their work to produce a high cryptographic strength security protection on the information. Their proposed approach comprises of two processes. They are encryption and decryption process. Template matching is the process used for pattern recognition. The utilization of biometric as a key is to improve security in a more efficient way, decrease human mistakes during identification, increase user relief and automation of security function. Their experimental results inform that their proposed approach out performed some of the conventional techniques in providing authentication for the user.

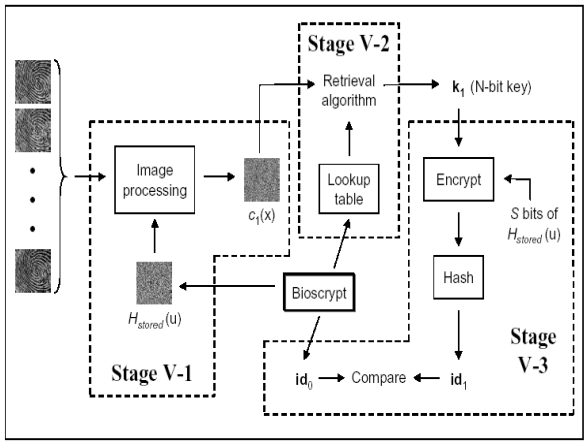


*Fig :Biometrics cryptography*

## V Conclusion

Biometric authentication is becoming a Very famous and most reliable user authentication system. The interest in biometric approaches for authentication is increasing for their advantages such as security, accuracy, reliability, service, and warmth. The Biometric Recognition system uses physical characteristics such as fingerprint, face, voice recognition, iris scanning. Biometric Recognition system replaces the existing security system which are used in some places like e-commerce application such as on-line banking and shopping mall. These systems overcomes the drawbacks of the traditional computer based security systems which are used at the places like money transaction, passport, credit cards, access control, smart cards, token key, government offices and network security. The biometric security systems have been proved to be accurate and very effective in various applications. Hence these systems are proved highly confidential computer based security systems.

## *References*

[1] A.K. Jain, L. Hong, R. Bolle, "On-line Fingerprint verification" , IEEE Trans. Pattern Anal. Mach. Intel. 1997.

[2] Steve Lawrence C. Lee Giles Ah Chung Tsoi, Andrew D.Back, "Face Recognition: A Convolutional Neural Network Approach", IEEE Transactions on Neural Network s, Special.

[3] A. K. Jain and U. Uludag, "Hiding biometric data,"*IEEE Trans. Pattern Anal. Mach. Intelligence*, vol. 25,no. 11, pp. 1493–1498, 2003.

[4] M. Yeung and S. Pankanti, "Verification watermarks on fingerprint recognition and retrieval," in *Proc. SPIE,Security and Watermarking of Multimedia Contents*, vol. 3657, pp. 66–78, (San Jose, USA), January 1999.

[5] Sim Hiew Moi, Nazeema Binti Abdul Rahim, Puteh Saad, Pang Li Sim, Zalmiyah Zakaria, and Subariah Ibrahim, 2009, "Iris Biometric Cryptography for Identity Document", IEEE Computer Society, International Conference of Soft Computing and Pattern Recognition: pp. 736-741.

[6] Anil K. Jain, Arun Ross, Sharath Pankanti "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security, Vol 1, No. 2, June 2006

[7] K. Lam and D. Gollmann, "Freshness assurance of authentication protocols," in Proceedings of the European Symposium on Research in Computer Security (ESORICS '92), pp. 261–272, Toulouse, France, 1992

[8] K. Lam and T. Beth, "Timely authentication in distributed systems," in Proceedings of the European Symposium on Research in Computer Security (ESORICS '92), vol. 648, pp. 293–303, Toulouse, France, 1992.

[9] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," Pattern Recognition, vol. 35, no. 12, pp. 2727–2738, 2002.

[10] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, Berlin, Germany, 2003.

[11] Y.-J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation" in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '04)*, vol. 3,pp. 2203–2206, Taipei, Taiwan, June 2004.

[12] C. Vielhauer, R. Steinmetz, and A. Mayerh¨ofer, "Biometric hash based on statistical features of online signatures," in *Proceedings of the International Conference on PatternRecognition*, vol. 1, pp. 123–126, Quebec, QC, Canada, August 2002.

[13] Y.Dodis, R. Ostrovsky, L. Reyzin, andA. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," Tech. Rep. 235, Cryptology ePrint Archive, February 2006.

[14] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data,"in *Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT '04)*, vol. 3027 of *Lecture Notes in Computer Science*, pp. 523–540, Interlaken, Switzerland, May 2002

[15] Y. Sutcu, Q. Li, and N. Memon, "Secure biometric templates from fingerprint-face features," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR '07)*, Minneapolis, Minn, USA, June 2007.

[16] chander kant, rajender nath,sheetal chaudhary"biometrics security using stegnogarphy," in *Proceedings of the International journal of security,volume (2): issue (1)*,february 2008.