www.ijaret.org

Vol. 1, Issue III, April 2013
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

Enhancement of Biometric Template Security in MultiBiometric Systems

Asra Nisar Bhat[1], Supreet Kaur[2]

[1]Student of Lovely School of Technology and Sciences
Lovely Professional University
er .asrabhat@gmail.com

[2] Faculty of Lovely Professional University
Phagwara, Punjab
supreet.16843@lpu.co.in

Abstract: *Security is a very important aspect in the biometric systems. Templates are the very important parts of biometric systems and attacker mostly attack on template and database of biometric system so securing them is a very crucial issue these days. In this research paper our focus is on template security in biometrics system and we develop a system to encrypt and decrypt the biometric images. In this work, multi-modal biometric template security for palmprint and fingerprint is proposed. At first, the preprocessing steps are applied and subsequently, the features are extracted and combined. Then different cryptographic techniques are used to encrypt it to make it secure so that even if someone gains access to the encrypted image stored in the database he will not able to reproduce the original image from it and it will be useless for him.*

Keywords: *Multi-modal biometrics; Template protection, Fingerprint, Palmprint, Encryption, Decryption, Cryptography, Security.*

1. INTRODUCTION

A biometric is a measurement of a biological characteristic of a person .It is a science of determining a person's identity (ID) by measuring his/her physiological characteristics. It is well known that humans use some body characteristics such as face, gait or voice to recognize each other. Thus it is a method of physical access control. Biometrics is attractive for its uniqueness. It cannot be forgotten, shared, lost or guess easily hence it is necessary to ensure that it remains private and is used properly without being abused. Basically it is a collection of methods for identification based on measuring the physiological characteristics that are unique to each and every individual. Some examples of such characteristics are:

- Voice
- Fingerprints
- Body Contours
- Retina
- Iris
- Handwriting Style / Handwritten Signature
- Gait
- DNA

Typically, a biometric authentication scheme consists of two phases:

i Enrolment phase

ii Authentication phase

Enrollment: Individuals must first register their form of identity with the system by means of capturing a raw biometric to be used in the system. This process is called Enrolment and is composed of three distinct phases:

Capture: A raw biometric is captured.

Process: Characteristics that are unique to individuals and distinguish individuals from one another are extracted from the raw Biometric and transformed into a biometric "template".

Enrol: The processed template is stored in a suitable storage medium such as a database on a disk storage device or on a portable device such as a Smart Card, whereby later comparisons can be made easily.

Authenticate Phase: Once Enrolment is complete, the system can authenticate individuals by means of using the stored template. Authentication is the process whereby a new biometric sample is captured by the individual who is authenticating with the system and compared to the registered (enrolled) biometric template. Since a biometric trait is an everlasting link between a person and his identity, it can be easily prone to abuse in such a way that a person's right to privacy and secrecy is compromised. Hence, strategies to protect biometric template and to ensure an individual's privacy are urgently needed. Stolen biometric templates can be used to compromise the security of the system in the following ways .The stolen template can be replayed to the matcher to gain unauthorized access, and A physical spoof can be created from the template to gain unauthorized access to the system (as well as other systems which use the same biometric trait). Hence, spoof attacks are possible even when the attacker does not have access to the biometric template.When biometric templates are compromised.

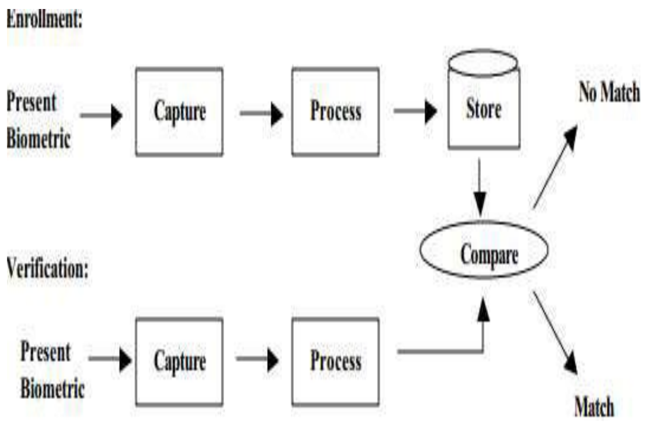

Figure 1: The Biometric Authentication System

It is not possible for a genuine user to revoke his biometric identifiers and switch to another set of uncompromised identifiers.

[1]In 1985 Berggren, L. described that the combinatorial complexity of the phase information across different persons spans about 249 degrees of freedom and generates discrimination entropy of about 3.2 bits/mm2 over the iris, enabling real-time decisions about personal identity with extremely high confidence [1].

[2]A method of rapid visual recognition of person identity is described by Daugman, J in 1993, based on the failure of statistical test of independence. the most unique phenotypic feature visible in the persons face is the detailed texture of each eye's iris. An estimate of its statistical complexity in a sample of human population reveals variation corresponding to several hundred independent degrees of freedom [2].

[4] In March 2007, A. Cavoukian and A. Stoianov, described in their work about privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of Biometric Encryption (BE) over other uses of biometrics. The work is intended to engage a broad audience to consider the merits of the Biometric Encryption approach to verifying identity, protecting privacy, and ensuring security. Our central message is that BE technology can help to overcome the prevailing "zero-sum" mentality, namely, that adding privacy to identification and information systems will necessarily weaken security and functionality. The work explains how and why BE technology promises a "positive-sum," winwin scenario for all stakeholders involved [4].

[3]In 2006 U. Uludag and A. K. Jain given the idea about biometrics based personal authentication systems that use physiological (e.g., fingerprint, face, iris) or behavioral (e.g., speech, handwriting) traits are being increasingly utilized in many applications to enhance the security of physical and logical access systems. Even though biometric systems offer several advantages over traditional token (e.g., key) or knowledge (e.g., password) based authentication schemes (e.g., increased user convenience and robustness against imposter users), they are still vulnerable to attacks.

[5]Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Salil Prabhakar, Member, IEEE, in 2004 have given a brief overview of the field of biometrics and summarized some of its advantages, disadvantages, strengths, limitations, and related privacy concerns [5].The main aim of biometrics is that the rendered services are accessed only by a legitimate user and no one else. Examples of such applications include secure access to buildings, computer systems, laptops and ATM's.

[7]D.Shanmugapriya and Dr. G. Padmavathi, in 2009, analyzed keystroke dynamics since they provide more reliable and efficient means of authentication and verification. Keystroke Dynamics is one of the famous biometric technologies, which will try to identify the authenticity of a user when the user is working via a keyboard. The authentication process is done by observing the change in the typing pattern of the user.

[8]Hisham Al-Assam, Harin Sellahewa, Sabah Jassim in 2011, have evaluated the security and accuracy of Multi-Factor Biometric Authentication (MFBA) schemes.These are based on applying User-Based Transformations (UBTs) on biometric features. The UBTs work on the transformation keys which are generated from passwords/PINs.The work includes the proposed mechanisms to enhance the security as well as the accuracy of MFBA schemes. The transformation keys can be compromised and that scenario has been described in the paper briefly along with the misevaluation of this scenario as the results can be easily misinterpreted [8].

In this research work the two biometric characteristics i.e. fingerprint and palm print has been used which are the commonly used traits for the authentication purpose.Fingerprints have been used for over a century. Fingerprint is the pattern of ridges and valley on the inner surface of a finger or a thumb [6]. The lines that flow in various patterns across fingerprints are called ridges and the spaces between ridges are valleys. It is these ridges that are compared between one fingerprint and another when matching.[6]Palm print refers to an image acquired of the palm region of the hand.Palm print inherently implements many of the same matching characteristics that have allowed fingerprint recognition. The main advantage of palm print is the availability of large space for extracting biometric features [6].Usually palm print images should be normalized and oriented before feature extraction. It contains more information than fingerprints, so they are more distinctive. By combining all features of palm and fingerprint such as ridge and valley features, principal lines and wrinkles, it is possible to build a highly accurate biometric system.

2. BIOMETRIC CHARACTERISTICS

[9]A number of biometric characteristics are being used in various applications. Each biometric has its pros and cons and, therefore, the choice of a biometric trait for a particular application depends on a variety of issues as follows:

Universality: Every individual accessing the application should possess the trait.

Uniqueness: The given trait should be sufficiently different across individuals comprising the population.

Permanence: The biometric trait of an individual should be sufficiently invariant over a period of time with respect to the matching algorithm. A trait that changes significantly over time is not a useful biometric.

Measurability: It should be possible to acquire and digitize the biometric trait using suitable devices that do not cause undue inconvenience to the individual. Furthermore, the acquired raw data should be amenable to processing in order to extract representative feature sets.

Performance: The recognition accuracy and the resources required to achieve that accuracy should meet the constraints imposed by the application.

Acceptability: Individuals in the target population that will utilize the application should be willing to present their biometric trait to the system.

Circumvention: This refers to the ease with which the trait of an individual can be imitated using artifacts (e.g., fake fingers), in the case of physical traits, and mimicry, in the case of behavioural traits [9].

3. ATTACKS ON BIOMETRIC SYSTEMS

[10]Any system (including biometric systems) is susceptible to various types of threats. These threats are discussed below:

i. Denial of Service: An adversary overwhelms computer and network resources to the point that legitimate users can no longer access the resources.

ii. Circumvention: An adversary gains access to data or computer resources that he may not be authorized to access.

iii. Repudiation: A legitimate user accesses the resources offered by an application and then claim that an intruder had circumvented the system.

iv. Covert acquisition: An adversary compromises and abuses the means of identification without the knowledge of a legitimate user.

v. Collusion: In any system, there are different user privileges. Users with super-user privileges have access to all of the system's resources. Collusion occurs when a user with super-user privileges abuses his privileges and modifies the system's parameters to permit incursions by an intruder.

vi. Coercion: A legitimate user is forced to give an intruder access to the system. For example, an ATM user could be forced to give away her ATM card and PIN at gunpoint [10].

4. TEMPLATE PROTECTION SCHEME

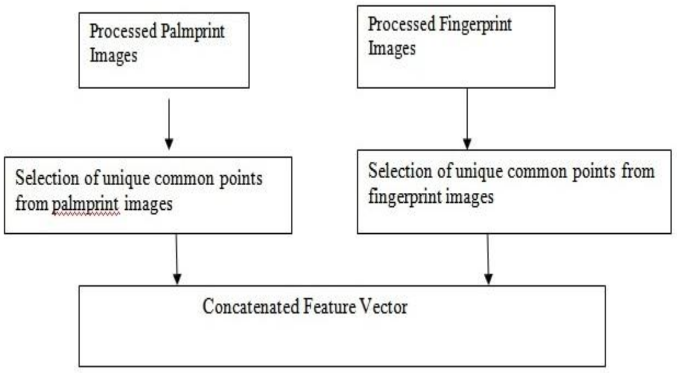
Processed Palmprint Images
Processed Fingerprint Images
Selection of unique common points from palmprint images
Selection of unique common points from fingerprint images
Concatenated Feature Vector

Figure 2: Template Protection scheme in Biometric Systems

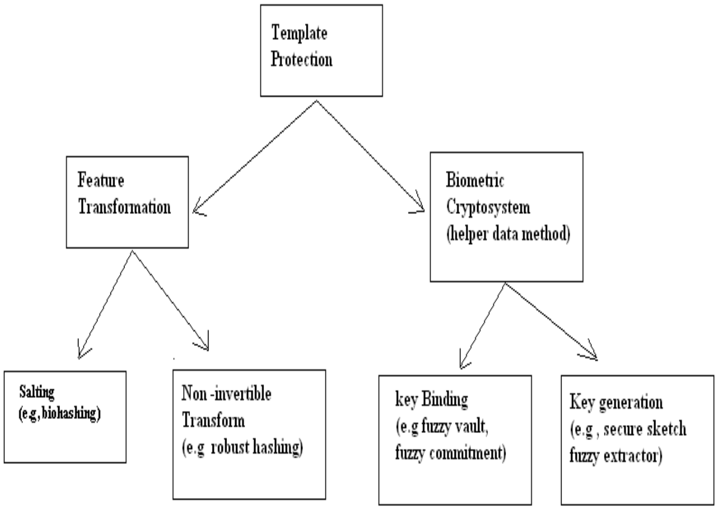
Template Protection
Feature Transformation
Biometric Cryptosystem (helper data method)
Salting (e.g, biohashing)
Non -invertible Transform (e.g robust hashing)
key Binding (e.g fuzzy vault, fuzzy commitment)
Key generation (e.g , secure sketch fuzzy extractor)

Figure 3: Block Diagram of Feature Extraction Process

5. PROPOSED METHODOLOGY

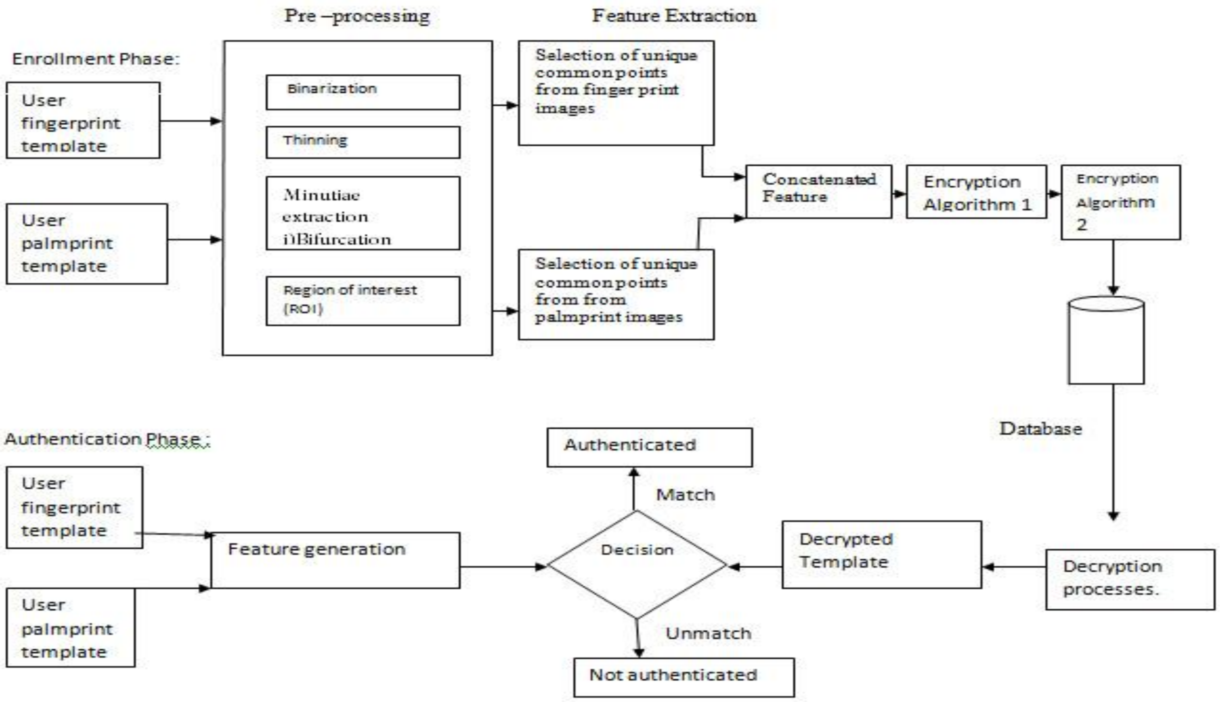

Figure 4: Block Diagram of the methodology proposed

6. CONCLUSION

In this paper, Security of Biometric Template has been discussed. The Biometric Template has been encrypted. This paper presents a method of securing templates in the database, in which the inputs are the fingerprint and the palmprint images which are initially processed in order to smoothen the image and make it fit for feature extraction. Subsequently, feature extraction is carried to have the feature vector. Then the cryptographic algorithms are used to encrypt the concatenated feature in the database. Even if the intruder gets access to database he will not be able to use the actual templates as it will be in encrypted form, and hence will be of no use to the attacker. In the Future, we will present how we will apply cryptographic algorithms to further secure the extracted feature to secure it in the database.

REFERENCES

[1] Berggren, L. "Iridology: A critical review", Acta Ophthalmological 63(1): 1-8 , 1985.

[2] Daugman, J. "High confidence visual recognition of persons by a test of statistical independence" IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15(11), pp. 1148-1161, 1993.

[3] U. Uludag and A. K. Jain, "Attacks on biometric systems: a case study in fingerprints," In Proc. SPIE, Security, Steganography and Watermarking of Multimedia Contents VI, vol. 5306, pp. 622–633, (San Jose, CA), January 2004.

[4] A. Cavoukian and A. Stoianov, "Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy," Office of the Information and Privacy, Commissioner of Ontario, Technical Report, March 2007

[5] Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Salil Prabhakar, Member, IEEE, January 2004,"An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1.

[6]F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," IEEE Transactions on Computers, vol. 55, pp. 1081-1088, 2006.

[7] Mrs. D. Shanmugapriya , Dept. of Information Technology and Dr. G. Padmavathi , Dept. of Computer Science(IJCSIS) ," A Survey of Biometric keystroke Dynamics Approaches, Security and Challenges" International Journal of Computer Science and Information Security,Vol. 5, No. 1, 2009. Evaluation of Multi-Factor Biometric Authentication", International Journal for Information Security Research (IJISR), Volume 1, Issues 1/2.

[8] Hisham Al-Assam, Harin Sellahewa, Sabah Jassim, March/June 2011, "Accuracy and Security

[9] Manvjeet Kaur, Dr. Sanjeev Sofat and Deepak Saraswat,"Template and Database Security in Biometrics Systems: A Challenging Task", International Journal of Computer Applications, July 2010.

[10] Kocher Niinuma, Unsang Park, and Anil K. Jain, "Soft Biometric Traits for Continuous User Authentication", IEEE 2010.