A Hybrid Template Security Technique using Multimodal Biometric Features

Srujan Satyavarapu[1], Farida Khurshid[1], Shoaib Amin Banday[1]

Department Of Electronics and Communication Engineering,
National Institute Of Technology, Hazratbal Srinagar
J&K, India-190006
srujansatyavarapu@gmail.com; fklone@rediffmail.com; shoaibee.a@gmail.com

Abstract—— **Biometrics has taken over as the mainstream security in almost every type of infrastructure ranging from the college libraries to the critical infrastructures like banks and airports. Despite the dramatic impetus that has taken biometrics from one level to the higher levels of security, there are still some open voids in terms of security that need to be filled. Among all such issues and threats, template security is of the most concern. The reason being that we don't want to make an identity compromise of a person. If a biometric template of a person is compromised that unfortunately means theft of identity of that person. This paper proposes a novel method that uses two different biometric data from the same person for making a biometric template against each person. The two biometrics modalities that have been used in our work are fingerprint and iris. The features and verification of the proposed system has been done using MATLAB.**

Keywords-— Biometrics, template security, cryptography, biometric security issues.

I. INTRODUCTION

Biometrics is a science of using physiological behavioral characteristics for identifying and verifying an individual. The main function of biometric system is to verify an individual biometric data to the enrolled data and authenticate the user. In this paper we are about to discuss various types of recognitions, various attacks occurring to the template database (template security) and how to keep an barricade between attackers and template data. In biometrics we can use two characteristics like physical and behavioral. In physical characteristics, every individual will be different to each other like fingerprint, face, palm print, earlobe etc. The physical characteristics become an interface to the system. In behavioral characteristics we take into account of persons behavioral characteristics like voice, keystroke, signature, gait and because of this the behavioral characteristics will be varying for each every individual and cannot be imitated easily.

The importance of biometric systems have increased in our day to day life. They are being used many ways like enrolment and verification purposes. The enrolment is used to enrollment the students in colleges, employees in a company, hospitals and many other places. In addition to these places, the biometric security systems are used in almost every critical infrastructure like airports and banks. The verification is process where the person will be authenticated. This authentication is done based on enrolled data. We will compare the live data with enrolled data and authenticate. This helps us to control access to some restricted areas and make a keen look on people enter in that area. The figure 1 below shows various physical and behavioral characteristics of humans that can be used for the purpose of authentication.

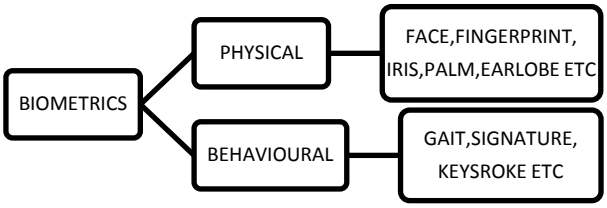

Figure 1

The usage of biometrics has been increased because being a human being we always forget keys, passwords and security questions. But now the physical characteristics are only key for accessing the system. Even now the Indian government is planning to use biometric ATM's to give labor their daily wages directly via the ATM, thus eliminating the use of the salary registers (under the project 100days labor work). The biometric technology has become of less costly and more effective. This is a major factor for improvisation of this field. By using biometrics a company or organization can mostly avoid unauthorized access.

1.1 Limitations of Biometric systems

Though there have been a tremendous growth in the advancement of this field, there is still a lot to think about regarding the performance of such systems. The recognition rates for most of the biometric systems is yet to reach 100% and there is also a primary concern over the security of the templates which are stored in the database.

Biometric Type	Accuracy	Ease of Use	User Acceptance
Fingerprint	High	Medium	Low
Hand Geometry	Medium	High	Medium
Voice	Medium	High	High
Retina	High	Low	Low
Iris	Medium	Medium	Medium
Signature	Medium	Medium	High
Face	Low	High	High

Table.1

The rest of the paper is divided into five sections. Cloud computing basic model and its related aspects including security are discussed in section II. The feature extraction from iris is discussed in section III followed by the proposed access control model for cloud in section IV. Section V and section VI are results and the conclusion respectively of this work.

II. SECURITY ISSUES

2.1 Biometric Security Outline

We have many security issues in biometric system .The security is the major factor that should be taken care by a security system developer. The heart of whole biometric system is its "template data". Securing the biometric templates has become a major task. Once an intruder breaks through the system we expect what type of threats may happen. He can use template data in wrong ways. If an individual biometric template is compromised it cannot be revoked easily because these biometric data cannot be changed in life time. The template protection became a big hurdle for the security developers.

2.2 Accountability of biometric systems

The biometric systems have two kinds of failures:
1) Intrinsic failure.
2) Failure due to an adversary attack.
The biometric system vulnerability is mostly because lack of proper secured infrastructure:

2.2.1 Intrinsic failure:-

Because of incorrect decisions made by biometric system the intrinsic failure occurs. Biometric system verification generally makes two types decision errors namely

1) *False accept*
2) *False reject*

False acceptance usually occurs because lack of uniqueness and individuality of biometric trait because of this we will be having more similar feature sets of different individuals. In false reject a genuine legitimate user may be rejected by the system due to more difference in users stored data. These intrauser variations may happen due to improper interaction with sensor.(eg.,change in position, change of expression).This also happens because of non robust systems and due to improper data acquisition from individual by a sensor. The fingerprint sensor may not catch proper impression because of wet fingers or dirty fingers. This leads to (FTE) Failure-to-enroll (FTA) Failure-to-acquire errors. It will be a serious threat if we accept a wrong person. The rejection of a genuine person cannot be that fatal [2].

2.2.2 Adversary attack

Here an attacker intentionally stages an attack on the biometric system. The success of attacker depends on the loopholes of the system. We categorize these in three sub classes.

2.2.2.1Administration attacks

This attack is also called as insider attack, which refer to all accountabilities introduced due to improper administration of biometric systems.

2.2.2.2 Non-secure infrastructure

The infrastructure means the hardware and software and the communication channels of biometric system. There are many ways an intruder can manipulate the infrastructure which leads to system attacks.

2.2.2.3 Biometric overtness

It is possible for an attacker to obtain biometric characteristics of a genuine user and use to create gummy fingers of the biometric trait. If the biometric system should be capable to differentiate between live and spoofed fingerprints. An attacker can circumvent the biometric system by presenting spoofed traits.

2.3 Countering adversary attacks

Attacker generally attacks the system at one or more modules or interfaces. We differentiate these attacks into four categories

a) Attacks at the user interface
b) Attacks at the interfaces between modules
c) Attacks on the modules
d) Attacks on the template database.

2.3.1 Attacks at the user interface

Attacks at the user interface may take place by presenting a spoofed trait. If the sensor is unable to differ between spoofed and original trait, the attacker can easily enters the system with false identity. Until now many software and hardware solutions for this lively detection have been developed [3][4].

2.3.2 Attacks at the interface between modules

An attacker generally attacks at communication interfaces between different modules, for instance he can keep a jammer near a communication channel. If a channel is not protected physically or cryptographically an attacker can obtain the data and he can make changes to the data and resend it. An insecure channel can allow an attacker to perform a replay or hill-climbing attacks. A common and mostly performed way is by sending the data cryptographically encoding using some public key in this we can also use time stamp to improve the security of the data.

2.3.2 Attacks on the software module

The program can be modified in a way that to obtain values that are desired by attacker these attacks are known as Trojan-horse attack. These attacks can be avoided by practicing secure code execution practices. If the attacker finds the loophole he will enter silently without being noticed.

2.3.3 Attacks on template database

The most potentially and powerfully damaging attack on biometric system is attack on template database. Attacks on template database leads to three vulnerabilities:
-A template can be replaced by a duplicate template to gain access.
-a spoof can be created to gain access to the system.
-The stolen template can be used to relay to the matcher to gain access to the system
These are attacks generally happen on the template database these can be avoided by providing secure infrastructure in such way that there should not be any loopholes like unsafe communication channels. we should also be able to revoke the stolen templates of an individual (for example a criminal can change his template data base and keep some other individuals templates).

III. TEMPLATE PROTECTION SCHEMES

An ideal biometric template protection should be able to possess through the fallowing properties.
1) Diversity: the cross matching of the template in data base must not be allowed there by ensuring users privacy
2) Revocability: the compromised biometric template should be revoked straight forward and reissue new one based on the same biometric data.
3) Security:- it should be potentially very hard to obtain the original template from the secured one. this property prevents attacker to create physical biometric template spoof from the stolen template[5][6].
4) Performance:- the recognition performance(FAR and FRR) of a biometric system should not be degraded by the template protection scheme.

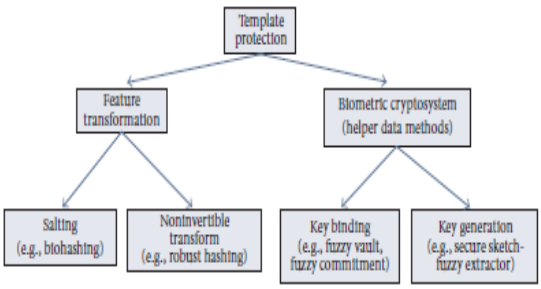

Figure. 3

Going back in the literature survey, following are the template security techniques that have been proposed and implemented. The following techniques along with their respective merits and demerits are explored:

3.1 Salting

In salting or bio-hashing template protection approach using a specific key or password, the biometric features are transformed. Because of invertible transformation to large extent, the key which is used must be secured safely or remembered by the user and should present during authentication process if the additional information the entropy of biometric template increases and hence make adversary hard to guess the template.

Advantages

1) Low false accept rates can be obtained by introducing a key.
2) We can generate multiple templates from same biometric data because the key is user specific.

Limitations

The main drawback is once the key is compromised the template is no longer secure because the transformation is usually invertible. If the attacker gains the access he easily owns the original template [7] [8].

3.2 Noninvertible transform

By applying the noninvertible transform the template can be secured because noninvertible transform is a one way function. This function is EASY TO COMPUTE and HARD TO INVERT. The key is defined by parameters and transformation function it must be provided during the authentication time. The main feature of

this approach is though the attackers know the key or transformed template it is hard to recover the original template.

Advantages

1) This approach is better than salting because it is hard recover original template even when the key is compromised.
2) By using the application-specific and user-specific transform function we can achieve diversity and revocability.

Limitations

The main drawback of this approach is tradeoff between discriminability and non invertbility of the transform function [11] [12].

3.3 Key-binding biometric cryptosystem

In a key-binding cryptography system, the biometric template is kept safe by binding monolithically with the key in cryptographic framework. Both the key and the template are embedded in a single entity in the database as helper data. The helper data does not reveal any information about the key or template it is very hard to decode without any known edge of key. Usually the error correcting code is associated with the helper data.

Advantages

To intrauser variations in biometric data this approach is very good tolerant. The tolerance can be determined by checking the error correcting capability of associated codeword.

Shortfalls

In this we have a problem of leaking key because matching must be done using error correcting code to match it with original template because of this we have possibilities of leaking a key [9] [10].

3.4 Key generating biometric cryptosystems

In the key generation the key is derived from the data itself. The cryptographic approaches play a major role in this scheme. These are applied on biometric template data to obtain a key.

Advantages

In this the key is directly generated from the biometric data only. It invokes the cancellable biometrics.

Shortfalls

It is very hard to generate a key with more stability and entropy. In this we have chances to derive dissimilar key because of improper features of the template data which may lead to mismatch of template (FRR) [12] [14].

IV. PROPOSED METHOD

In this method we are going to use two biometric templates of fingerprint and iris we will collect the data from the fingerprint (as shown in flow diag.) we will generate the key from iris data then we will encrypt the data using the key which is generated from iris data then we use encrypted data for template and store in data base(e.g, if person A comes and keep his finger print and his iris then only he will be authenticated. If an impostor comes thought he fake the fingerprint or by knowing the algorithm he can obtain the finger print data but he cannot be authenticated because the finger print is related to the iris because it is the key the major advantage of iris is is it cannot be spoofed because of its sophisticated structure. As a result the intruder cannot enter the system.)

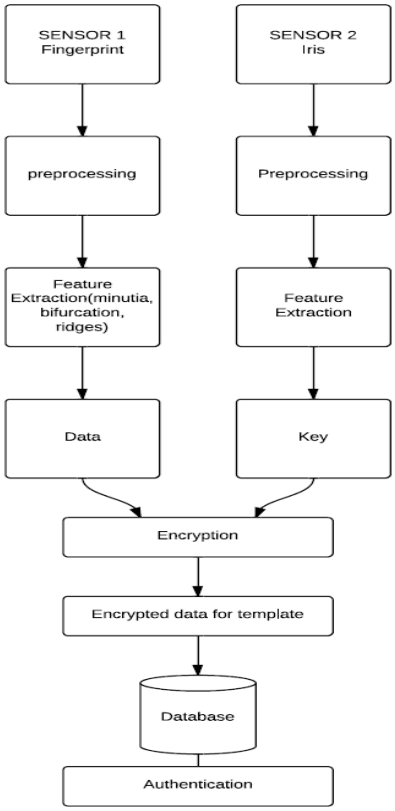

Figure.3

V. CONCLUSION

The proposed method is potentially sound to eliminate most demerits that other template security techniques have. The issues like keys being stolen and illegally used can be very much overcome and reduced. If a key is stolen, the intruder can get the access to the template and can actually make an identity theft, i.e., the intruder can access the most important credentials of the person who template has been stolen. So the uniqueness and randomness of the key plays an important role in the template security. If one key is developed from one biometric and data is obtained from the other biometric of the same person than it is really difficult for an intruder to get into the template database. The main reason behind this is that the intruder cannot spoof both the biometrics of the same person and other reason being that the intruder is unaware of the fact that how the features of a particular biometrics are computed. The third reason being that even if he gets data of the both biometrics, he is still unaware how to bind the biometric key to the biometric data.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, 2006.
[2]A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*,Springer, Berlin, Germany, 2006
[3] D. R. Setlak, "Fingerprint sensor having spoof reduction features
and related methods," US patent no. 5953441, 1999.
[4] K. A. Nixon and R. K. Rowe, "Multispectral fingerprint imaging for spoof detection," in *Biometric Technology for Human Identification II*, vol. 5779 of *Proceedings of SPIE*, pp. 214–225, Orlando, Fla, USA, March 2005
[5] 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.
[6] 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
[7] C. S. Chin, A. T. B. Jin, and D. N. C. Ling, "High security iris verification systembased on random secret integration," *Computer Vision and Image Understanding*, vol. 102, no. 2, pp. 169– 177, 2006.
[8] T. Connie, A. B. J. Teoh, M. Goh, and D. C. L. Ngo, "PalmHashing: a novel approach for cancelable biometrics,"

Information Processing Letters, vol. 93, no. 1, pp. 1–5, 2005.
[9] T. Clancy, D. Lin, and N. Kiyavash, "Secure smartcard-based fingerprint authentication," in *Proceedings of the ACMSIGMMWorkshop on Biometric Methods and Applications*, pp. 45–52,Berkley, Mich, USA, November 2003.
[10] S. Yang and I. Verbauwhede, "Automatic secure fingerprint verification system based on fuzzy vault scheme," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '05)*, vol. 5, pp. 609–612, Philadelphia, Pa, USA, March 2005.
[11] M. Savvides and B. V. K. Vijaya Kumar, "Cancellable biometric filters for face recognition," in *Proceedings of the IEEE International Conference Pattern Recognition (ICPR '94)*, vol. 3, pp. 922–925, Cambridge, UK, August 2004.
[12] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, 2007
[12] Q. Li and E.-C. Chang, "Robust, short and sensitive authentication tags using secure sketch," in *Proceedings of the 8th Multimedia and Security Workshop (MM and Sec '06)*, pp. 56–61, Geneva, Switzerland, September 2006.
[13] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: theory and practice," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 503–512, 2007.
[14] E. C. Chang and S. Roy, "Robust extraction of secret bits from minutiae," in *Proceedings of 2nd International Conference on Biometrics*, pp. 750–759, Seoul, South Korea, August 2007
[15]Review Article Biometric Template Security Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar] Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing Volume 2008, Article ID 579416.