A Survey of Multi-Biometric Cryptographic Security System

Vaibhavkumar S. Gaikawad[1], S. N. Kini[2]

[1]M.E (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007

[2]Prof (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007

Abstract: ***Over the past few years biometric technologies are used to security purposes by analyzing human characteristics. Unimodal biometric has some limitations which overcome with multibiometric. Multibiometric system also inherits some problems related to the template security. Now a days in network goes on different types of attacks which can handle by biometrics. In paper present different types of biometrics attacks and types of multi-model biometric system. Various techniques proposed in developing an authentication system for promising to individual's information security to come together biometric characteristics of that individual and the feature transformations as well as cryptographic techniques. It also provides fundamental idea for future research that may help in removing the difficulty associated with the current authentication systems. Biometrics technologies are gaining popularity today since they provide more safe and capable of authentication and verification.***

Keywords: Multi-Biometric, Cryptographic, Security, authentication accuracy, template protection

1. Introduction

With increasing use of IT technology and need to protect data, in our daily lives, we have multiple accounts/passwords. We can only remember so many passwords, so we end up using things we know to create them. It is easy to crack passwords, because most of our passwords are related to self and those are weak! If the user create strong passwords, that should be combinations of different keys, we will forget them! Because is very difficult to remember such passwords. The best solution for this problem is to use bio metrics to protect your devices or accounts. A biometric is a physiologic or behavioural characteristic of a human being that can distinguish between person to person and that can be used for identification or verification of same person identity. When we decide the use of biometrics then it can be difficult to choose which type is the best for particular work. This is because every biometric has some limitations and benefits. It is not difficult to purloin a biometric of user, create a copy and use the fake trait to attack on biometric systems. This types of problems realizes a requirement of biometric security in network.

There are different types of Biometrics,
1) Biological traces (DNA, blood, saliva)
2) Physiological characteristics (fingerprints, eye irises and retinas, hand palms and geometry, and facial geometry),
3) Behavioural characteristics (signature, keystroke dynamics, lip motion, gait and voice).

Compared with old and traditional authentication techniques such as token cards, token number, picture-based passwords and passwords, biometric-based techniques offer a non-ordinary, more universal and reliable option for personal or group authentication [1]. The system to verify biometric templates consists of the standard universal input-input – match process. The first stage of the above mentioned process is called as the enrolment process. Enrolment process consists of 3 sub processes 1- Scanning of the biometric images or input by the system with the help of devices and 2) where in the biometric features are understood and measured by the system and 3) based on which the templates created for the system storage for the verification purpose and stored in database.

The Second stage is the stage where the new set of data or biometric samples collected again to authenticate the identity of the end user. The biometric security system that is the person whose identity is authenticated for the purpose system will collect the data with fresh samples of the same person in the same manner again and match it with existing data of biometric template of the person stored in the system. If system is able find match whether exact or in percentage enough to establish the identity of the user based on pre-defined parameters it would give the output as match. In the opposite scenario the system may clear indicate that two user are different or it may raise some concerns or queries or even may ask for more qualitative and or quantitative sample of the data in order to arrive to the conclusion. (Figure 1).

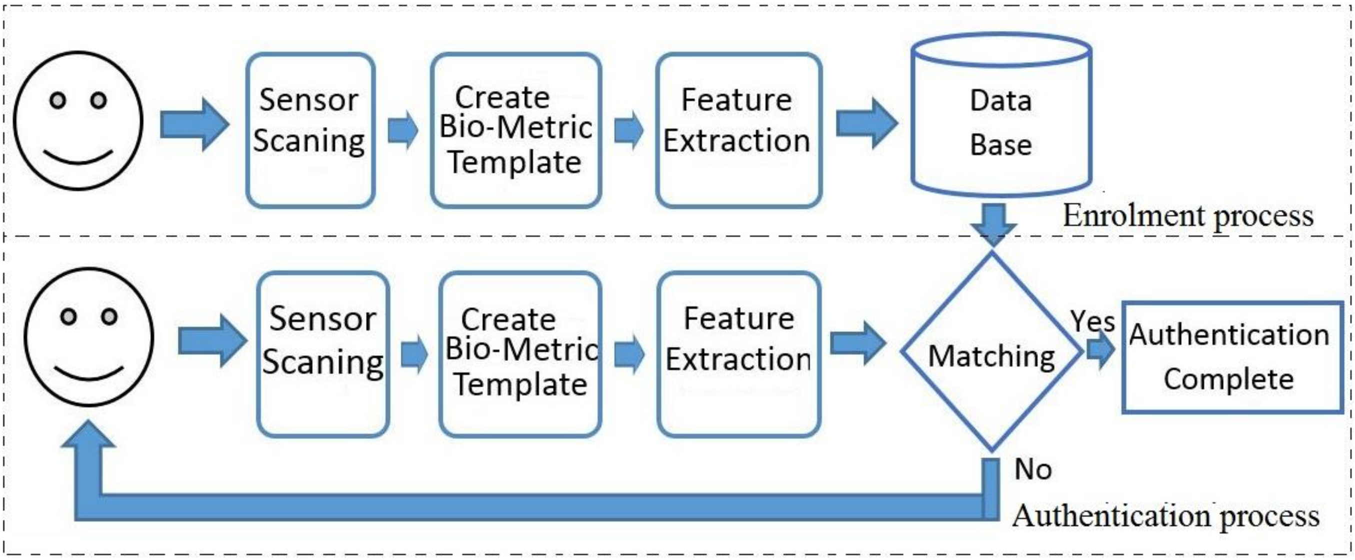

Figure 1: Biometric based authentication system.

Only biometric is not sufficient to provide a security but integrating biometric with the cryptography is provide a well security. Biometric cryptosystems apply on single biometric (such as face, fingerprint, iris etc.), the accuracy and security of single biometric (unimodal) cryptosystems are limited [1], which leads to the theoretical work and practical applications of multibiometric cryptosystems.

The rest of the paper is organized as follows: - Section 2 discusses Literature Survey. Section 3 includes types of multimodal systems. Section 4 concentrate on different classes of attacks on biometric security. A security and protection of biometric system is understand in section 5. And conclusion are given in section 6.

2. Literature Survey and Related Work

The scarcity and unique traits of biometric combined with the fact that these signature and traits are part and parcel of the person they represent are left all over the places wherever a person goes or work or visit. Can easily get the samples of fingerprints of the person from the hotel he eats or the books he reads or vehicle he drives. Voice sample of any prominent personality can easily be recorded even at public gatherings or your retina samples can be stoles from your eye specialist. There have been published instances of fake fingerprints created out of gelatin, and of face recognition software being bypassed [6]. Indeed, many research findings have proven that biometric information stored in a database may leak biometric features which can be used to reconstruct a biometric image.

Biometric applications have expanded their reach right from complex scientific R &D premises to widespread use in BFSI, Manufacturing, Gov. Organizations, etc. across the world But along with the qualitative and quantitative rise in the use and scale and scope of biometric systems we are facing increase in the number of challenges coming up and certain inherent drawback of the system [9]. The major threat is posed by attackers wherein they can access biometric templates from databases or servers, can reconstruct the raw images once they are able to compromise the existing templates [5].

The security concern of biometrics is that once biometric data are compromised, the effect will be forever. Biometric images are easily susceptible to reconstruction which can be done with the help of few leaked biometric features and full size template can be reconstructed. For example, Ross et al. [5] has shown how minutiae template can give way to the access of three levels of fingerprint information: Namely, orientation field, class or type and friction ridge structure.

Another major and very significant ,difficult to ignore and inherent drawback of the biometric system which put it at disadvantage compared to traditional password or E card systems is uniqueness of the biometric signature and traits of individual person. While we can easily reset and reissue password after they are compromised, the same can"t be done with the biometric input. For Example If thumb impression of certain person are compromised then we can neither reset them nor take new sample of thumbprint because the said samples being unique can"t be entered into system again, which brings permanent loss of the chosen biometric features for authentication purposes[1].

Considering a threat to biometric security systems in the world of connectivity and rising cybercrimes, lot of R & D work has been done in the past few years to secure the biometric template from being compromised. For the authentication purpose biometric protection techniques use transformed data which is sourced and created out of original biometric data. There is different type attacks in biometric system. Most of the attack work on the biometric template. For protecting the biometric template proposed various methods and technique and present a way to the template protection scheme in multimodal biometric system [12].

In the biometric system above mention problems are more discus with understanding the different types of multimodal biometric system and different classes of attacks.

3. Types of Multimodal Systems

Multimodal biometric system has few subtypes based on their feature sets, sensor and other parameters.

Single biometric trait, multiple sensors: In this category multiple sensors record the same biometric characteristic to ensure the advanced level of template security. The raw data collected from different sensors is combined at the feature level or matcher score level thus leading to overall improvement the system performance.

Multiple biometrics: In this type multiple biometric traits such as fingerprints and retina are combined and Different sensors are used to map and collect each biometric characteristic. The system uses interdependency of the traits leading to significant improvement in the performance of the system. For example, a commercial product Bio ID [7] uses Multiple Biometric Traits such as voice, lip motion and face of a user to verify his identity.

Multiple units, single biometric traits: When Two or more fingers of a single user are used as a biometric trait to establish his identity it becomes one of the example of multiple unit‟s single biometric trait. This system doesn‟t require multiple sensors on order to extract feature or match modules. Iris can also be included in this category. Due to the same reason is less costly compared to multiple traits biometric even with improved security.

Multiple snapshots of single biometric: In this category more than one sample of the same biometric trait is used for the recognition. For example multiple impressions of the same finger or multiple samples of the voice of the same user are taken to create templates.

Multiple matching algorithms for the same biometric: this type of system apply different methods to extract feature and to match the biometric characteristic.

4. Attacks on Biometric Systems

Biometric systems has provided a strong and universally accepted alternatives traditional token based or password based identification and access systems along with many advantage over such systems [8]. But the system like its alternative is also not immune to attack and can be compromised

There are eight types of attacks that these systems are vulnerable .These are as follows.

Class I: Spoof attack: this attack is made with the help of and creation fake biometric input given for authentication which is created by copying the original template and (finger made from silicon, face mask, lens including iris texture) can be presented to a sensor [8].

Class II: this attack is known by the name of replay attack. It is possible for an opponent to clarify or acquire a digital copy of the biometric sample which is stored in local database and reply this signal bypassing the biometric sensor.

Class III: Substitution attack: In this type the designer of attack gets access to feature exactor module and replaces it Trojan horse program that functions according to the compromised parameters given by the attacker. Once attacker is successful with the insertion of Trojan horse then he easily gets access to storage either locally or globally. He thus is able overwrite the legitimate user‟s template (i.e. Replace someone‟s thumb impression with other person) with his /her own –leading to the stealth of their identity.

Class IV: there are instances when attacker replaces a genuine feature values with other fake values (synthetic or real)

Class V: In this type of attack the matcher is replaced with a Trojan horse program. This class of attack is called Trojan horse Attack.

Class VI: this type of attack target the template database, leading to the template addition, modification or removal in part or complete from the database.

Class VII: Transmission attack: A man in the middle attack; they target while the data is transmitted from one component to another. The attacker herein compromises the input data stream, create a fake template to represent as an authentic enrolled user, can inject an artificial matching score or even may be able to generate a forged response.

Class VIII: Here in the attacker manipulates the result directly instead of template or matcher and be able to manipulate the end results that is match or mismatch.

5. Biometric Protection & Security

The Methods for protection & Security are categorized into following types:

(1) Feature transformations (or cancellable biometrics) [3], [6] and [7].

(2) Biometric cryptosystems [1] [2].

1) Feature Transformations. This Technique uses non-invertible transformations to modify original biometric data. The Modified template is stored in the database for authentication. In the case of transformed template being compromised, the system simply reissue a new transformed template using different transformation parameters.

2) Biometric cryptosystems: Use of digital cryptography for the enhancement of the security of biometric system is recent invention and is still in early stage though applied worldwide now. With the help of biometric cryptosystems we get an innovative solution for cryptographic key generation, encryption as well as biometric template protection. Biometric cryptosystems replace original templates with biometric-dependent information (referred to as helper data),

with the help of which the cryptographic keys are recovered. In this type Matching of the template is performed indirectly by verifying the validity of recovered keys.

Multimodal Biometric system uses multiple interdependent or weakly correlated biometric template from an individual (e.g., Fingerprint and retina of the same person, or fingerprints from two different fingers of a person) [8]. The major problem in using a single biometric is its insufficient security as well as difficulty in providing sufficient coverage of the user population. Biometric cryptosystems initially applied single biometric (such as face, fingerprints etc.) Their accuracy and security is limited, which has lead to the first theoretical work and then practical applications of multibiometric cryptosystems (MBC). With higher authentication accuracy and flexibility in usage, wider coverage and multiple and stronger security layers, multibiometric cryptosystems are rapidly replacing the Single biometric Cryptosystems.

Multibiometric cryptosystems are categorized into two Based on fusion modes: (1) in the first category the fusion is applied at the feature level (also known as biometric level), and (2) in the second category the fusion is applied at the decision level (also known as cryptographic level) [13].

Cryptography is the technique of conversion of data into a secure and encrypted code that is sent across a private or public network and then decrypted at the end [10]. Biometric Encryption is a process that securely link up a digital key to a biometric as an additional level of security or in some cases generates a key from the biometric. The key which is „„encrypted"‟ with the biometric, leads to creation of biometrically encrypted key, also called biometric encryption template or helper data, and is stored in the data. The same digital key is „„decrypted"‟ when it verifies that the presented biometric sample is correct. This „„encryption/decryption"‟ process is fuzzy by nature, because the biometric sample is different each time, in contrast to encryption key in conventional cryptography. A major technological challenge we face while using this system is that there are many natural variations in the input biometrics t based on which the creation of digital key becomes difficult.

Based on the retrieval data, of biometric cryptosystems, they can be classified into two categories: key-binding systems and key generating systems [4].

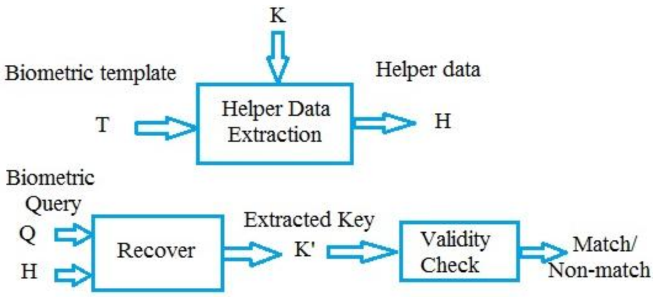

Figure 2: The framework of key-binding systems

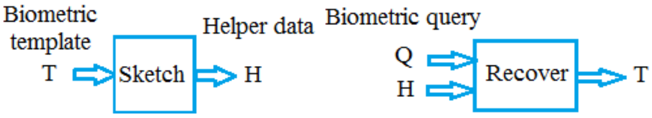

Figure 3: The frameworks of a secure sketch (Key Generating Systems)

1) Key-Binding Systems: Helper data is Retrieved by linking a special cryptographic key which is attached with biometric template., this system recovers the cryptographic key from the helper data with the help of biometric query During the matching process (see Figure 2)[1]. These keys are always designed to ensure that they can be successfully recovered with higher probability as and when required based on the query run from legitimate user.

2) Key Generating Systems: Helper data is retrieved from the biometric template and the cryptographic key is generated with the helper data combining it with the biometric query. When the template stored and query raised are from the same user, then the generated keys will be the same with overwhelming probability. These Key generating systems are also known by the names such as "fuzzy extractor" or "secure sketch" (see Figure 3), both of which are formally defined in [2]. In general, a fuzzy extractor composes secure sketch and use a strong extractor. The secure sketch uses helper data to recover original biometric templates while the strong extractor generates nearly uniform random keys from biometric data.

With the Growing flow of all types information across internet, which has led to access of secured and sensitive data being linked to open networks, computer systems throughout the world has started using cryptography as an indispensable security enhancement tool. And there many open source as well as licensed cryptographic algorithms are available for securing information even commercially now a days.

6. Conclusion

This paper presents a brief light on multibiometric cryptographic security systems. At first due consideration is given problems related to the biometrics that is to protect the uniqueness of biometric from permanent loss of biometrics (fingerprints, eye irises and retinas). And second is to create more secure process or system by using multibiometric cryptosystem which protect the biometric template. Hereby we have also discussed the role and necessity of encryption to enhance the security of biometric systems. We have discussed the two type‟s techniques that is Cryptographic techniques and cancellable biometrics which are used for encryption

Biometric technology secure with identification and authentication. But biometric authentication systems also infected by several attacks such as transmission, replay and spoofing. Biometric feature transformation and cryptographic techniques are two different way to providing a security, integrating the both techniques and goes to work for more secure techniques is a need for feature, for the systems are proved highly confidential computer based security systems.

References

[1] Cai Li, Jiankun Hu, Josef Pieprzyk, And Willy Susilo ,"A New Biocryptosystem-Oriented Security Analysis Framework And Implementation Of Multibiometric Cryptosystems Based On Decision Level Fusion" IEEE Trans. Information Forensics And Security, Vol. 10, No. 6 Pp. 1193–1206, June 2015

[2] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in Proc. Eurocrypt, 2004, pp. 523–540.

[3] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate-based cancelable fingerprint templates," Pattern Recognit., vol. 44, nos. 10–11, pp. 2555–2564, Oct./Nov. 2011.

[4] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," IEEE Trans. Inf. Forensics Security, vol. 2, no. 4, pp. 744–757, Dec. 2007.

[5] A. Ross, J. Shah, and A. K. Jain, "From template to image: Reconstructing fingerprints from minutiae points," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 544–560, Apr. 2007

[6] S. Wang and J. Hu, "Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach," Pattern Recognit., vol. 45, no. 12, pp. 4129–4137, Dec. 2012

[7] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–572, Apr. 2007.

[8] Bo Fu, Simon X. Yang, Jianping Li, and Dekun Hu. "Multibiometric Cryptosystem: Model Structure and Performance Analysis," IEEE Transactions on Information Forensics and Security, vol. 4, NO. 4, pp. 867–882, December 2009.

[9] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," Proc. IEEE, vol. 92, no. 6, pp. 948–960, Jun. 2004.

[10] Forozan an Mukhopadhay, "Cryptography and Network Security," Mc Graw Hill, 2007, (book style)

[11] Abhishek Nagar, Karthik Nandakumar, and Anil K. Jain, "Multibiometric Cryptosystems Based on Feature - Level Fusion," IEEE Transactions ON Information Forensics And Security, vol. 7, NO. 1, pp. 225–268, February 2012.

[12] Chulhan Lee a, , Jaihie Kim, "Cancelable fingerprint templates using minutia e-based bit-strings," Journal of Network and Computer Applications vol. 33, pp. 236–246, (2010)

Author Profile

Mr. Vaibhavkumar S. Gaikawad, is pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. He received his B.E (Computer) Degree from SESCOE Navalnagar, Dhule, India. North Maharashtra University, Jalgaon, Maharashtra, India -425001. His area of interest is network Security, Distributed Computing.

Prof. S. N. Kini, received his M.E. (Computer) Degree from B.M.S. College of Engineering, Basavanagudi, Bangalore, India. He received his B.E (Computer) Degree from K L E Society's College of Engineering Udyambaug Belgaum, India. He is currently working as Prof (Computer) at Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. His area of interest is network security and mobile computing.