Secure Authentication in Multimodal Biometric Systems Using Cryptographic Hash Functions

Aravind Ashok, Prabaharan Poornachandran, and Krishnasree Achuthan

Amrita Center for Cyber Security, Amrita University, Amritapuri Campus, Kollam, India
aravindashok@am.amrita.edu,
{praba,krishnashree}@amrita.edu

Abstract. In this Information Age, security of personal data is one of the biggest issues faced by most of the nations. Biometrics provides substantial help in guarding against attempts to establish fraudulent multiple identities or prevent identity fraud. The greatest advantage that the biometric data of an individual remains constant acts as its biggest liability. Once the attacker gets biometric password of an individual then security of his data becomes a big problem. This paper comes with a unique solution which will allow people to change their biometric password and helps to overcome some of the present issues in biometric systems. The biometric password is created by hashing the biometric data of the user. Merging of biometrics and cryptography proves to be more secure and helps to provide a better authentication system for the society.

Keywords: Biometrics, Multimodal Biometrics, Authentication, Biometric Set, Hashing, SHA-1 Algorithm, Database.

1 Introduction

Due to rapid increase in cyber-crimes it has become extremely important for all nations to safeguard their confidential data. A biometric system is essentially a pattern- recognition system that recognizes person based on a feature vector derived from a specific physiological or behavioral characteristic that a person possesses [1]. Automated biometric systems have only been available over the last few decades due to significant advancement in the field of computing. Many of these techniques are however based on the ideas that were originally conceived centuries ago. Some of the various biometric recognition methods are face, iris, voice, fingerprint, palm geometry etc. Biometric data cannot be borrowed or forgotten but at the same time it cannot be changed as well. Though it provides better security than the traditional passwords, it has a lot of vulnerabilities which are being exploited by various attackers.

A simple biometric system consists of five basic components or modules [2]:

1. **Sensor**: Module which takes the biometric data as an input.
2. **Feature Extractor**: Module where the data taken from the sensor is converted into vector form.
3. **Template Database**: Module where the vectors regarding biometric data were already stored during enrollment.
4. **Matching Module**: Here the vectors obtained from feature extraction module are compared with the vectors present in the database.

S.M. Thampi et al. (Eds.): SNDS 2012, CCIS 335, pp. 168–177, 2012.

5. **Decision Making Module**: Based on the result of the matching module the claimer's identity is accepted or rejected.

An attack can be done in any of these five modules. There are eight main areas where attacks may occur in a biometric system:

As we can see not only the modules but also the channels connecting the modules are being attacked. In order to make the attacking procedure complex and ensure better security measures multimodal biometric systems were introduced.

In certain situations, the user might find one form of biometric identification is not exact enough for identification. According to a report [3] by the National Institute of Standards and Technology (NIST) to the United States Congress concluded that approximately two percent of the population does not have a legible fingerprint and therefore cannot be enrolled into a fingerprint biometrics system.

Experimental result shows that multimodal biometric systems for small-scale populations perform better than single- mode biometric systems [4]. Multimodal biometric technology uses more than one biometric identifier fused together to compare the identity of the person.

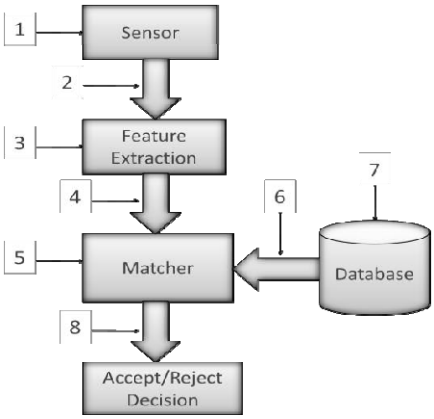

Fig. 1. Places where attack can occur in a biometric system

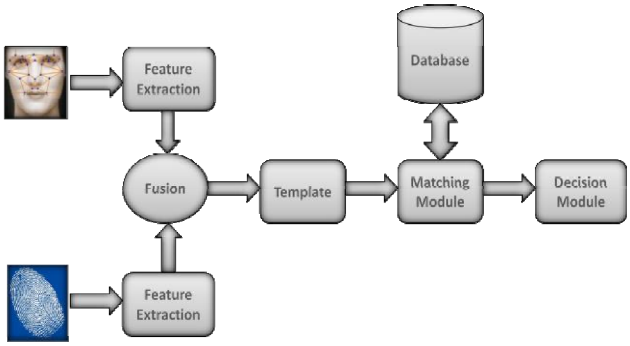

Fig. 2. Working of a basic multimodal biometric system

Though the limitations of uni-modal biometric systems can be overcome by multimodal systems, the later fails to provide solution to the following issues:

1. **Security of personal identity**: Though comparatively complex, the attacker can perform same type of attacks on the multimodal biometric system as well and once the biometric data is stolen the whole effort to construct the multimodal technology seems useless.
2. **Security of Database**: Cases has been found out where reconstruction of biometric data has been done even from the fused templates stored in the database.
3. **Providing identity to the disabled:** Some systems fail to retrieve biometric data from handicapped or disabled people [3]. Even though the percentage of such users is very less, when this technology comes out for mass identification projects like UIDAI [14] in India, this shortcomings really matter.
4. **Balance between FAR and FRR error:** False Acceptance Rate[FAR] is the probability that a random impostor is accepted as one of randomly selected user by the system [5] whereas False Rejection Rate[FRR] is the probability of a user being rejected by the system. The two error rates FAR and FRR are complementary to each other. Hence a proper balance has to be made between these errors. Generally a threshold value is calculated which decides whether the user's claim should accepted or not.

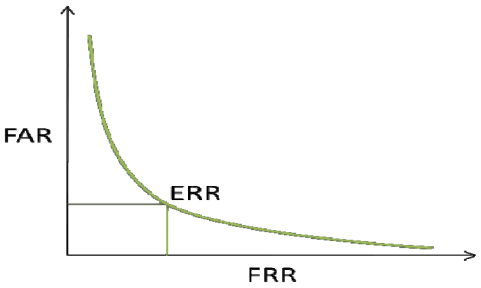

Fig. 3. Estimation of threshold value from error rates

2 Proposed System

In this paper we propose a solution to overcome some of the limitations of present biometric systems. We have merged biometrics with cryptography using Hash functions to produce a changeable biometric password for a user. A strong combination of biometrics and cryptography has the potential to link a user with a digital signature she created with a high level of assurance [6]. Though there are many biometric cryptosystems in existence, the idea of changeable biometric password is unique and more secure.

2.1 System Features

This system has inbuilt five different biometric algorithms:

1. **Face**: One of the oldest and most basic examples of a characteristic that is used for recognition by humans is the face. Face recognition is non-intrusive and cheap as well [7]. This technique uses 3D sensors to capture information about the face. 3D sensors vastly improve the precision of facial recognition and can also identify a face from various angles.
2. **Iris**: Iris recognition is known for its accuracy and use in high level security systems. Compared to other biometric features (such as DNA, face, Voice etc.), iris is more stable and reliable feature [8]. Statistical analysis reveals that irises have an exceptionally high degree-of-freedom up to 266 (fingerprints show about78) [9], and thus are the most mathematically unique feature of the human body; more unique than fingerprints. Hence, the human iris promises to deliver a high level of uniqueness to authentication applications that other biometrics cannot match.
3. **Fingerprint**: Fingerprint recognition is the most developed and economical biometric feature. Also very small storage space is required to store fingerprint templates, thus reducing the size of the database.
4. **Palmprint**: A palm print refers to an image acquired of the palm region of the hand. Like fingerprint, palms of human hands contain unique pattern of ridges and valleys. Since palm is larger than the finger it is expected to be more reliable than fingerprint [2].
5. **Tongue**: Like fingerprint and palm print even human tongue print is unique. The tongue is a unique organ in that it can be stuck out of mouth for inspection, in this act offering a proof of life, and yet it is otherwise well protected in the mouth and is difficult to forge [10].

For biometric identification, it is comparatively difficult as it is a smooth member with different shapes. But the research is interesting since it is very difficult to forge and because of its uniqueness.

This system can be best explained by dividing it into three main parts:

1. **Enrollment**: First the user has to enroll by providing his biometric data and creating a biometric password in the system.
2. **Database**: Both the biometric data and password are stored in the database which can be used for matching during authentication.
3. **Authentication**: The user has to enter his biometric set by which a biometric password will be created. This password is then matched with the one in the database to accept/reject the user's claim.

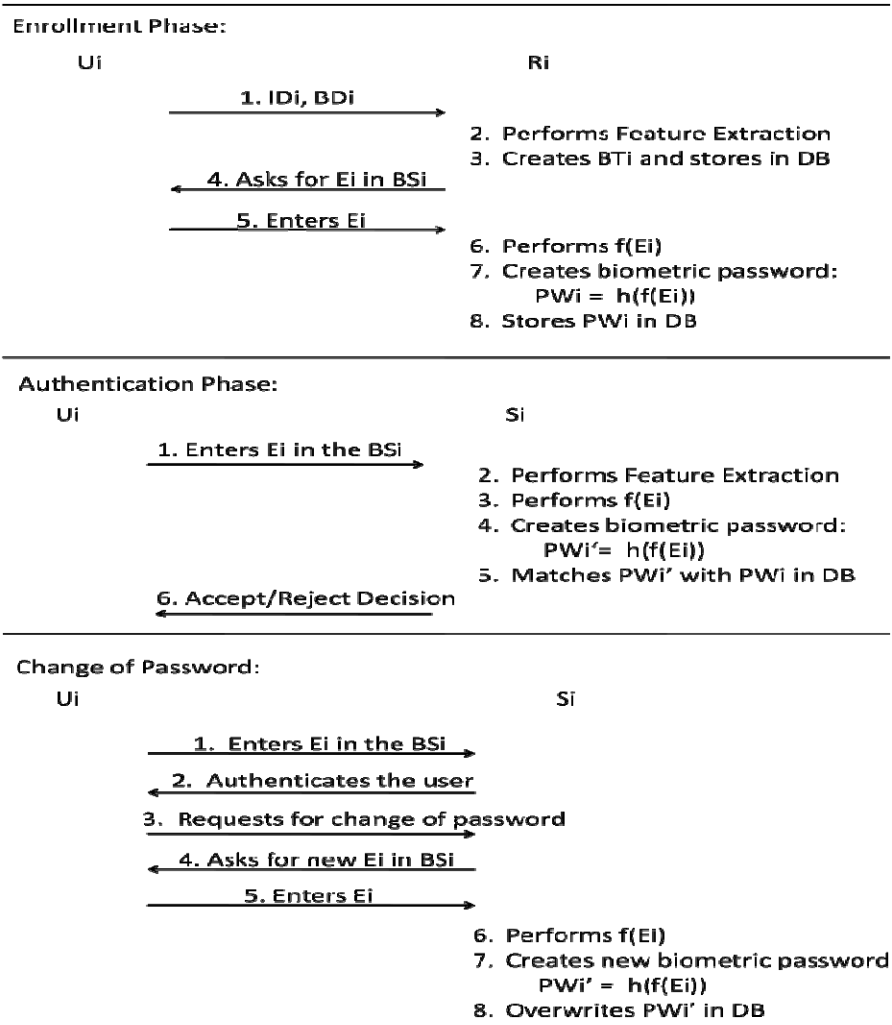

Fig. 4.1. Our proposed scheme

Ui - User	**IDi - Identity of user**
BDi - Biometric data	**BTi - Biometric template**
BSi - Biometric set	**Si - System**
Ei - Elements in BSi	**DB - Database**
h(.) - Hash function	**f(.) - Fusion function**
Ri- Registration center	**PWi - Biometric Password**

Fig. 4.2. Notations used in the proposed scheme

2.2 Enrollment

As mentioned earlier this system has inbuilt five different biometric algorithms and hence the user will have to provide the biometric data of each biometric part during enrollment.

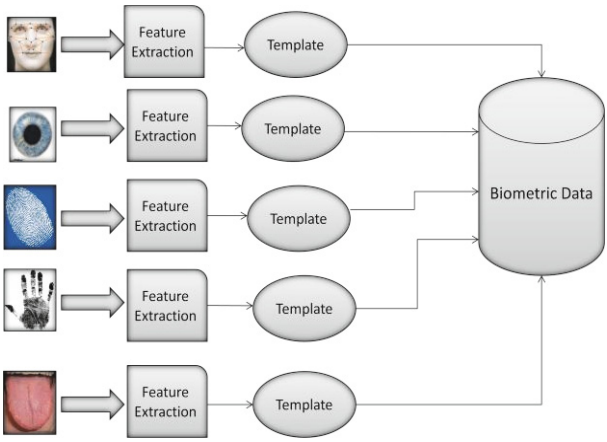

Fig. 5. Enrollment process by providing biometric data

The data enters the feature extraction module where it is converted into vector forms. These vector forms are then stored in templates which finally goes to the database.

2.2.1 Secure Hash Algorithm (SHA-1)

A Hash function is a one-way encryption algorithm which creates a unique fixed length output for a variable length unique input. A hash function is more complex and irreversible in nature when compared with encryption algorithms. Even if 1 bit is flipped in the input string, at least half of the bits in the hash value will flip as a result. SHA and MD-5 are some of the most secure hashing algorithms. For any given message **m** its hash value **h** remains unique. It is difficult for two different messages **m** and **m'** to have the same hash value. Also it is very difficult to get the original message from its hash value [15].

$$\text{hash (m)} = \text{hash (m')} \text{ only if } m = m'$$

The elements inside the biometric set are hashed to produce a biometric password. The elements are none other than the biometric data of the user. For our proposal we have used SHA-1 hash algorithm. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used security applications and protocols. SHA-1 produces a 160-bit message digest based on principles similar to MD4 and MD5 message digest algorithms, but has a more conservative design [11]. SHA-1 requires the operation of 80 rounds which can be grouped into 4 groups, 20 rounds each [12]. The four different functions are as follows:

$$f(B,C,D) = \begin{cases} Ch(B,C,D) = (B \bullet C) \wedge (\neg B \bullet D) & , 0 \le t \le 19 \\ Parity(B,C,D) = B \oplus C \oplus D & , 20 \le t \le 39 \\ M(B,C,D) = (B \bullet C) \wedge (B \bullet D) \wedge (C \bullet D) & , 40 \le t \le 59 \\ Parity(B,C,D) = B \oplus C \oplus D & , 20 \le t \le 39 \end{cases}$$

$\oplus$, $\bullet$, $\wedge$, $\neg$ denote the XOR, AND, OR and NOT operations respectively.

The working of SHA-1 algorithm can be understood by the link in [16]. However, weak and normal hash passwords can be cracked [17] i.e. the plain text can be obtained from its hash output using brute force attacks [18], rainbow tables and lookup tables [19]. Since the biometric characteristic is extremely large and complex, it is nearly impossible to reverse it [17] and we will need to utilize multiple rounds of a hash algorithm, and that adds to the complexity of the cryptanalysis [20].

2.2.2 Password Creation Module

Biometric password is made from the biometric data stored in the database. The system asks the user to select at least two out of the five biometric parts in any sequence to create the password. For e.g. {Face, Iris, Finger} can be a biometric set. Even repetition of biometric parts is allowed. Hence even sets like {Face, Iris, Face} or {Iris, Iris, Tongue} can be used to make the password. The minimum number of elements required inside the set is 2, whereas there are no restrictions to the maximum number of elements to be included in the biometric set.

The biometric password thus formed will be stored in the database. As there will be minimum of two elements in a biometric set, doing all permutations and combinations a user can have a total of:

$$\sum_{i=2}^{n} 5^i = 5^2 + 5^3 + 5^4 + \cdots + 5^n = \infty$$

Thus a user can have **infinite** number of different biometric sets and thus **infinite different biometric passwords**. Whenever the user wants to change his password he will just have to login into the system and select a new biometric set. The new password automatically gets updated to the system database.

Algorithm:

1. Read the entered Biometric Set.
2. Fetch the feature extracted template of the first element in the biometric set stored in database.
3. Search whether another element is present in the entered set.
   3.1. If yes, fetch the biometric template of that element. The templates are fused and the contents are then hashed to form a 160bit key. This 160 bit key cipher text is then stored inside a sample template. Goto step 3.
   3.2. If no, the data stored in the previous template acts as the biometric password.
4. Save the biometric password into the database.

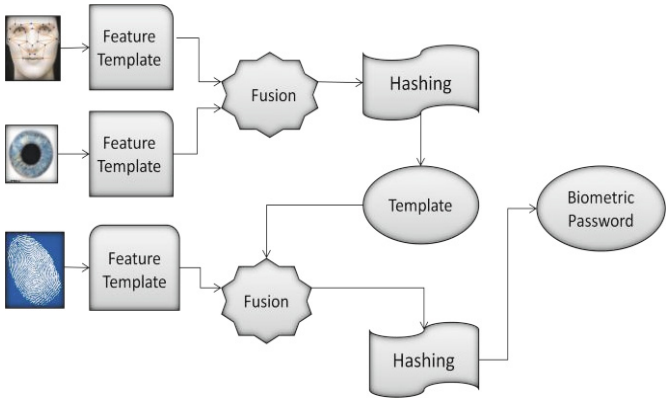

Fig. 6. Biometric password creation process

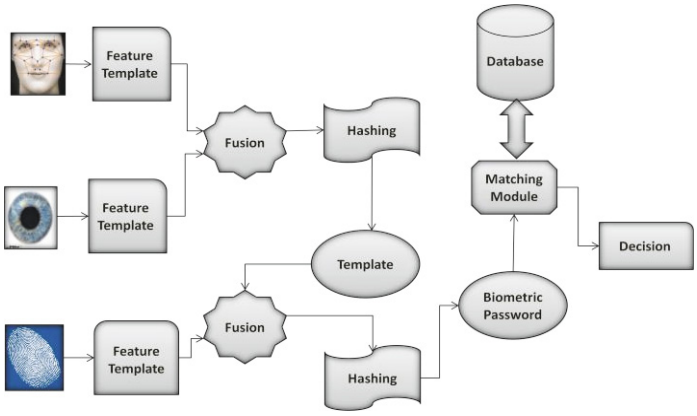

Fig. 7. Detailed view of Authentication of the User

2.3 Database

For the proper functioning and performance evaluation of biometric recognition systems large multimodal databases are required under real working conditions [21]. In this section we describe the characteristics and uses of the database system. Database of this system consists of two parts:

1. **Biometric data**: It consists of templates which has the vector form of five biometric parts of the user.
2. **Biometric Password**: Some of the biometric data templates are chosen by the user in a sequence and encrypted to create the biometric password.

Even if the attacker gets the biometric data of an individual, authentication will not be verified until the proper biometric set is entered. Moreover, finding out biometric set from the biometric password is tough.

2.4 Authentication

During authentication the user has to enter the elements present in his biometric set in the exact sequence as he had chosen during enrollment.

The biometric password thus formed during authentication is matched with the one in the database. According to the result obtained from the matching module a decision is made whether to accept or reject user's claim. The only constraint is that the user should remember the exact biometric set by which he had enrolled into the system. Any change in the sequence of elements in the biometric set will reject the authentication of the user.

3 Strengths and Advantages

- People can change their biometric password according to their wish.
- Even if attacker gets the biometric data he won't be able to login unless he knows the sequence in which it has to be used.
- Extremely tough to reconstruct biometric set from the biometric password.
- Provides alternative measures of identification for physically challenged or handicapped persons.

4 Conclusion

Biometrics refers to an automatic recognition of a person based on his physiological or behavioral characteristics. Many applications will in future rely on biometrics as it is the only way to guarantee the presence of the owner when a transaction is made [2]. The common drawback of all biometric systems is that they fail to provide an alternative even if an individual's account has been hacked by an attacker. In this paper we have put forward an idea which will actually allow an individual to change his biometric password and solve some of the problems present in the modern biometric systems.

References

[1] Prabhakar, S., Pankanti, S., Jain, A.K.: Biometirc Recognition: Security and Privacy Concerns. IEEE Security & Privacy, 33–44 (March/April 2003)

[2] Delac, K., Grgic, M.: A Survey of Biometric Recognition Methods. In: 46th International Symposium Electronics in Marine, Zadar, Croatia (June 2004)

[3] NIST report to United State Congress. Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability (November 13, 2000), http://www.itl.nist.gov/iad/894.03/NISTAPP_Nov02.pdf

[4] Snelick, R., Indovina, M., Yen, J., Mink, A.: Multimodal Biometrics: Issues in Design and Testing. In: International Conference on Multimodal Interfaces (ICMI), Vancouver, British Columbia, Canada. ACM (November 2003) 1-58113-621-8/03/0011

[5] Korte, U., Krawczak, M., Martini, U., Merkle, J., Plaga, R., Niesing, M., Tiemann, C., Vinck, H.: A cryptographic biometric authentication system based on genetic fingerprints. LNI, vol. P-128, pp. 263–276. Springer (2008)

[6] Hao, F., Anderson, R., Daugman, J.: Combining Crypto with Biometrics Effectively. IEEE Trans. on Computers 55(9) (September 2009)
[7] Jain, A.K., Ross, A., Prabhakar, S.: An Introduction to Biometric Recognition. IEEE Trans. on Circuits and Systems for Video Technology 14(1), 4–19 (2004)
[8] Zhang, Z.B., Ma, S.L., Zuo, P., Ma, J.: Fast Iris Detection and Localization Algorithm Based on AdaBoost Algorithm and Neural Networks. In: International Conference on Neural Networks and Brain (ICNN), vol. 2, pp. 1009–1014 (October 2005)
[9] Chen, W.-S., Chih, K.-H., Shih, S.-W., Hsieh, C.-M.: Personal Identification Technique based on Human Iris Recognition with Wavelet Transform. In: International Conference on Acoustics, Speech and Signal Processing (ICASSP), vol. 2, pp. 949–952 (March 2005)
[10] Liu, Z., Yan, J.-Q., Zhang, D., Tang, Q.-L.: A Tongue-Print Image Database for Recognition. In: Procedings of the Sixth International Conference on Cybernetics, Hong Kong (August 2007)
[11] SHA-1 Hash function, http://en.wikipedia.org/wiki/SHA-1
[12] Pongyupinpanich, S., Choomchuay, S.: An Architecture for a SHA-1 Applied for DSA. In: 3rd Asian International Mobile Computing Conference, AMOC 2004, Thailand, May 26-28 (2004)
[13] National Institute of Standards and Technology (NIST), "Secure Hash Standard", Federal Information Processing Standards Publication 180-2 (August 2002)
[14] Unique Identification Authority of India, Planning Commission, Government of India, http://uidai.gov.in/
[15] Cryptographic hash function, http://en.wikipedia.org/wiki/Cryptographic_hash_function
[16] Alderson, N.: Increasing Security Expertise in Aviation- oriented Computing Education: A Modular Approach, part of Cryptography module, Embry-Riddle Aeronautical University in Prescott, Arizona, http://nsfsecurity.pr.erau.edu/crypto/sha1.html
[17] Kisasondi, T., Baca, M., Lovrencic, A.: Biometric Cryptography and Network Authentication. Journal of Information and Organizational Sciences 31(1) (2007)
[18] How hashes are cracked, http://crackstation.net/hashing-security.html
[19] How Crackstation cracks hashes, http://crackstation.net/
[20] Hellman, M.E.: A cryptanalytical time-memory trade off. IEEE Transactions on Information Theory IT-26 (1980)
[21] Ortega-Garcia, J., Fierrez-Aguilar, J., Simon, D., Gonzalez, J., Faundez-Zanuy, M., Espinosa, V., Satue, A., Hernaez, I., Igarza, J.-J., Vivaracho, C., Escudero, D., Moro, Q.-I.: MCYT baseline corpus: a bimodal biometric database. IEE Proc.-Vis. Image Signal Process. 150(6), 391–401 (2003)