MULTIMODAL BIOMETRIC AUTHENTICATION: SECURED ENCRYPTION OF IRIS USING FINGERPRINT ID

Sheena S¹ and Sheena Mathew²

^{1,2}Department of Computer Science & Engineering, School of Engineering, Cochin
University of Science & Technology, Kochi, India

ABSTRACT

Securing data storage using biometrics is the current trend. Different physiological as well as behavioral biometrics like face, fingerprint, iris, Gait, voice etc.. is used in providing security to the data. The proposed work explains about the biometric encryption technology which will securely generate a digital key using two biometric modalities. Iris is encrypted using Fingerprint ID of 32-bit as the key in this work. For encryption Blowfish algorithm is used and the encrypted template is stored in the database and one is given to the user. During the authentication time user input the template and the fingerprint. This template is then decrypted and verified with the original template taken from the database to check whether the user is genuine or an imposter. Hamming distance is used to measure the matching of the templates. CASIA Iris database is used for experimentation and fingerprint images read through the R303 - fingerprint reader.

KEYWORDS

Multi-modal Biometrics, Minutiae, Fingerprint, Iris, Feature Extraction, Encryption, Blowfish, Hamming Distance, FAR, FRR, EER

1. INTRODUCTION

In modern era protecting our data in a unique manner is an inevitable requirement. Biometric Technology has proven that it has an important role in the field of Security, access control and monitoring the various applications because of its non-reputable authentication method. Reliable user authentication technique has highly demanded due to the progress in networking and communication. Biometric authentication based on physiological modalities like the fingerprint, iris etc. is found to be more secure and reliable than the traditional way of authentication by means of password [1]. The biometric authentication process is done by validating the unique feature of an individual by using any of the physiological or behavioral features. During this process, user's identity is compared with the template already stored, and the permission is granted only to a genuine user that has an adequate match. Basically, biometric-based authentication system operates in two modes viz. Enrollment and Authentication. The user's biometric data is acquired using a biometric reader and then it is stored in the database with a user identity for further verification. The user's biometric data is acquired once again to verify the claimed identity of the user. Biometric authentication system which uses physical characteristics to verify the identity of a person, which ensures much higher security compared to password or PIN number, because Biometric feature cannot be forgotten and also difficult to forge easily.

However each biometric technology has its own strength and limitations and no single biometric is expected to effectively satisfy the requirements of all verification or authentication applications [2].

A single biometric sometimes fails to be accurate enough for the identification of a large user population. Another disadvantage of using only one biometric is that the physical characteristics of a person for the selected biometric might not be always available or readable. Biometrics systems based on one biometric (uni-modal) are often not able to meet the desired performance requirements and have to contend with a variety of problems such as noisy data, intra-class variations, a restricted degree of freedom, non-universality, spoof attacks and unacceptable error rates. These practical problems can be overcome by the use of multimodal biometrics system in which two or more biometric features like finger, face, iris, or Gait can be used to improve the recognition accuracy. One of the specific reasons for using multi-modal biometrics is the security requirements of some specific applications [3].

Biometric encryption is one of the emerging research areas, which is a method of combining biometric features with cryptographic keys. Consecutively will provide the advantage of both fields and is named as biometric encryption. Such systems map biometric data into a unique stream of a binary string, which in turn can be mapped to an encryption key or direct hashing [4]. This approach eliminates the need of storing the biometric template. The cryptographic key generated from biometrics will enhance the security; hence it can be relinquished with the key storage using passwords or PIN numbers.

There is a relatively high chance of intrusion at any step so that one must provide an additional security management [5]. Encrypting one biometric modality (Iris in the proposed work) with another biometric modality (fingerprint is the second biometric modality) is found to be the most effective methods to enhance the security of the system. The security of the system is based on the associated secret key [6].

2. RELATED WORKS

From the literature extensive researches have been reported for generating cryptographic keys from biometric modalities and multimodal biometrics based user authentication. Brief reviews of such recent research work are conferred here.

According to Selvarani *et. al.*[5] the data from the cloud is accessed by the secret key which is wrapped by the two different biometric modalities viz. Fingerprint and the Iris for decryption. Only after decryption the user gets the original message. Thus the user secures their data from unauthorized access. Jagdeesan *et.al.*[1] proposed a method to generate a 256-bit secure cryptographic key from the multi-biometrics template. For that the two biometric modalities like fingerprint and the Iris is used. Vincenzo Conti *et al.*[17] put forward a feature level fusion of Iris and fingerprint and resulted with a homogeneous biometric vector. In his work matching is done using Hamming Distance matching algorithm. The template level fusion algorithm working on a unified biometric descriptor was suggested in his work. Feng Hao *et. al.* [4] developed a recurring binary string, called as biometric key, generated from an Iris image by using auxiliary error correction data. This will help to conceal the biometric key and can be stored as a token like a smart card. The Iris biometric and the token are required to reproduce the key. Sanaul Hoque *et al.*[18] proposed an approach which generates the biometric key from the live

biometrics. In order to generate the key, they divided feature space into subspaces and then to cells and these cell subspaces contribute to the generation of the key. Muhammad Khuram Khana *et. al.*[19] suggested a novel multi-modal biometrics authentication system on space-limited tokens using face and fingerprint modalities. Combining biometrics and cryptography is found to be a promising solution, at the same time biometric encryption system must be acceptable only when it can consider a minute change in the selection of similar biometric modalities during the time of generating decisive keys.

3. SECURED MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEM

A secure authentication system using multimodal biometric system is an emerging research area. Studies reveal that this system is highly efficient and consistent than knowledge-based (e.g. Password) and token-based (e.g. Key) techniques. The proposed work focussed on describing the security-enhancement methodology by using both biometrics and encryption technology to secure data access. In this work multi-biometric encryption, a methodology is proposed with the help of two biometric modalities like Fingerprint and Iris. The figure1 shows the enrollment phase of the proposed system. Here the Iris is encrypted using Fingerprint ID as a key. The sensor will accept the two inputs: Fingerprint and the Iris for each user. At first stage enrollment of a user is being done. This process will be completed by extracting the fingerprint features through the fingerprint reader R303. Correspondingly the Iris texture features are also extracted through different steps viz. segmentation, Iris Edge detection, Iris localization. After the feature extraction the encryption is carried out by using Blowfish algorithm. Blowfish is an encryption algorithm that can be used as a replacement for the DES or IDEA algorithms. It is a symmetric block cipher that uses a variable-length key, from 32 bits to 448 bits of binary strings. In the second stage authentication of a user is performed. In this stage decrypting the biometric template and matching is done using the Hamming distance.

- A. Enrollment: Fingerprint Feature Extraction, Iris Feature Extraction, Encryption
- B. Authentication: Decryption, Matching

Figure 1: Enrollment

Figure 2: Authentication

2.1. FINGERPRINT FEATURE EXTRACTION

Feature extraction of the Fingerprint is being done using the minutiae point extraction methods. This method will identify the local ridge discontinuities, which are of two types: ridge endings and bifurcations. A good quality image has around 40 to 100 minutiae [7]. It is these minutiae points which are used for determining the uniqueness of a Fingerprint. Fingerprint consist of ridges in a different orientation, in this method ridges orientation at each pixel location in the image is identified in x and y directions. By using fingerprint reader R303 the minutiae points are extracted and obtain a fingerprint ID from the fingerprint reader and this is converted into a hash using MD5 algorithm and 32 bit hash is treated as the key for encrypting the Iris. Blowfish symmetric block cipher algorithm encrypts block data of 32-bits at a time.

2.2. IRIS FEATURE EXTRACTION

Iris biometric features are one of the most secure because the iris texture is formed in the fetal development and it is highly stable with age and health condition [8,9]. The uniqueness of iris texture is highly promising and hence it is chosen as one of the biometric modality for the user authentication. In this work CASIA, Iris v3 database is used. Iris feature extractions done through the steps like Edge-detection using Sobel filters, Contrasting, Iris localization using Hough Transform as shown in figure 3a, Normalization by the concept of Daugman's Rubber Sheet model [10] as shown in figure 3b, and then extracting the Iris feature using Gabor filter, which is the linear filter that gives the normalized image, from this normalized image each row of pixel is taken as the input signal. Thus gets the iris code.

Figure3: a, b: Iris Localisation, Iris Normalisation

2.3. ENCRYPTION

Here the biometric sources are fingerprint and iris image. The extracted biometric feature of the fingerprint is used as the fingerprint ID which is used to encrypt the extracted Iris biometric feature [11, 12]. The encrypted multimodal template is generated using the encryption of Iris image and Fingerprint ID using Blowfish algorithm and this template is given to the user for further authentication. Blowfish is an encryption algorithm that can be used as a replacement for the DES or IDEA algorithms. It is a symmetric (that is, a secret or private key) block cipher that uses a variable-length key, from 32 bits to 448 bits, making it useful for both domestic and exportable use. The Encryption key generated using the Blowfish algorithm that provides fast and secure communication. A hash function with MD5 algorithm and the 32 bit hash is taken randomly. And the iris stored in the database is retrieved and is encrypted using this 32-bit Fingerprint ID [13]. The encryption is done using Blowfish algorithm as mentioned earlier..

2.4. DECRYPTION

The decryption is the reverse process of encryption as represented in figure 4. The decryption can be performed with the appropriate digital key only if the same biometric sample is presented during authentication time [14]. In the proposed work the blowfish algorithm is used for decryption. This is done by inputting the template generated during the encryption and the fingerprint. During the decryption process an iris image is taken from the database. Similarly the template corresponding to the given fingerprint is taken from the database and it is also decrypted. For decryption again the same Blowfish algorithm is applied by supplying the Pi sub-keys in reverse order [15]

Figure 4: Image Decryption

2.5. MATCHING

The iris decrypted from the template inputted by the user and the one which is decrypted from the database using fingerprint ID as the key will be compared. The Hamming distance method is used in matching. The Hamming distance gives a measure of how many bits are the same between two bit patterns. Using the Hamming distance of two bit patterns, a decision can be made as to whether the two patterns were generated from different irises or from the same one. If the compared irises are same, then the user is granted access else it is denied. The table1 shows the evaluation based on different observations on various inputs. Based on this observation FRR (False Rejection Rate) and FAR (False Acceptance Rate) on different values of Hamming distance was plotted as shown in the figure 5a. From this figure EER(Equal Error Rate) is found as 6. Figure 5b is plotted based on the Hamming distance 6.

Table 1. Evaluation based on various inputs observations

Sl. No.	Input Image	Detected Image	Hamming Distance
1	a20	a20a	3.46
2	a1b	a1a	0.797
3	a1c	a1c	1.917
4	a1	a1c	1.917
5	a1b	a2	8.651
6	a2crop	a1b	1.04
7	a7	a7a	2.16
8	a7a	a7c	0.136
9	a13	a7a	7.4
10	a13	a13a	4.9
11	a3	a3crop	2.3
12	a49	a49crop	6.02
13	a49a	a7a	4.9
14	a13a	a13d	3.2
15	a3crop	a3b	3.4
16	a2c	a2c	0.03
17	a2d	a2	5.034
18	a7d	a7	4.02
19	a20c	a20	2.9
20	a13c	a7d	5.02

Figure 5a. FAR & FRR on different values of hamming distances

Figure 5b. FAR & FRR at Hamming Distance of 6

3. CONCLUSION

In this paper Security of data storage using multimodal biometrics is proposed with the help of biometric encryption. Multimodal Biometric authentication is done using Iris and Fingerprint aims to achieve data storage security. For that biometric features like Fingerprint and Iris of the user is collected and extracted. A template is created using this features by encrypting the iris using a blowfish algorithm. Then the template is stored in the database. When the user logs in

order to use the cloud storage system, the system authenticates the user by using the template provided and the fingerprint, which is used here as the key for decryption. Without the use of fusion the proposed work reduces the complexity of the algorithm and this method increases the overall security of the system with less computational time.

REFERENCES

- [1] A. Jagadeesan et.al."Cryptographic Key Generation from Multiple Biometric Modalities: fusing Minutiae with Iris features", International Journal of Computer Applications (0975-8887) volume: 2 No.6, 2010.
- [2] P.Balakumar et. al, "A Survey on Biometrics based Cryptographic Key Generation Schemes", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555, Volume: 2, No. 1, 2012
- [3] Vinayak Ashok Bharadi et.al., "Multimodal Biometric Recognition using Iris & Fingerprint By Texture Feature Extraction using Hybrid Wavelets", Conference Paper, September 2014.
- [4] Feng Hao et.al., "Combining cryptography with biometrics effectively", Technical Report, Computer Laboratory, Cambridge University, UKICAM-CL-TR-640, ISSN 1476-2986.
- [5] Selvarani et.al., "Multi-model Bio-cryptographic Authentication in Cloud Storage Sharing for Higher Security", Research Journal of Applied Sciences, Engineering and Technology 11(1): 95-101, 2015
- [6] Abhishek Nagar, Karthik Nandakumar, Anil K. Jain, and Dekun Hu,"Multibiometric Cryptosystems Based on Feature-Level Fusion, IEEE Transactions on Information forensics and security", volume 7, no. 1, pp. 255268, February 2012
- [7] DrPS SV Ravi Kumar ,"Novel Cryptographic Algorithm based Fusion of Multimodal Biometrics Authentication system",Journal of Research in Science, Technology, Engineering and Management (JoRSTEM) Volume:1 and Issue -1, September 2015
- [8] Sowkarthika.S et.al., " Securing Iris Templates using Double Encryption Method", IJARCSSE. Volume: 2, Issue 11, November 2012, ISSN: 2277 128X
- [9] A. Jagadeesan et.al, "Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris", (IJCSIS) International Journal of Computer Science and Information Security, Volume: 7, NO.2, February 2010.
- [10] M.Natarajan et.al." Multimodal Crypto-Biometric System Based On Session Key Navigation for Secure Transaction, 2014 International Conference on Secure Transaction, 2014 International Conference on Innovations Conference on Innovations in Engineering Technology (ICIET' 14)
- [11] Saad Abuguba, Milan M. Milosavljevi and Nemanja Maek, "An Efficient Approach to Generating Cryptographic Keys from Face and Iris Biometrics Fused at the Feature Level", in IJCSNS International Journal of Computer Science and Network 6 Security, Volume.15 No.6, June 2015
- [12] Muthukumar Arunachalam and Kannan Subramanian," AES Based Multimodal Biometric Authentication using Cryptographic Level Fusion with Fingerprint and Finger Knuckle Print" in The International Arab Journal of Information Technology September 2015
- [13] M. Devi, "Secure Crypto Multimodal Biometric System for the Privacy Protection of User Identification", in International Journal of Innovative Research in Computer and Communication Engineering, March 2014
- [14] Ann Cavoukian et.al., " Biometric Encryption Chapter from the Encyclopedia of Biometrics", Office of the Information and Privacy Commissioner, Toronto, Ontario, Canada
- [15] Algimantas Venckausakas et. al. "Cryptographic Key Generation from Finger Vein", Conference of Informatics and Management Sciences, March 25-29, 2013.

- [16] Bo Fu, Simon X. Yang, Jianping Li, and Dekun Hu, "Multibiometric Cryptosystem: Model Structure and Performance Analysis", IEEE Transactions on information forensics and security, volume: 4, no. 4, pp.867882, December 2009
- [17] Conti, Vincenzo, et al. "A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems." IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS PART C, Applications and reviews" 40.4 (2010)
- [18] Sanaul Hoque , Michael Fairhurst and Gareth Howells, "Evaluating Biometric Encryption Key Generation Using Handwritten Signatures", in Proceedings of the 2008 Bio-inspired, Learning and Intelligent Systems for Security, pp.17-22, 2008.
- [19] Muhammad Khurram Khana and Jiashu Zhanga, "Multimodal face and fingerprint biometrics authentication on space-limited tokens ", Neurocomputing, volume:71, no. 13-15, pp.3026-3031, August 2008.