Secure Personal Recognition System based on Hashes Keys

Deepak Sharma[1] and Sonakshi Khurana[2]

[1]KITM, Kurukshetra, [2]HCTM, Kaithal
Haryana, India
sharmadeepak2k4@gmail.com, er.sonakshi@gmail.com

Abstract

Human Identification systems provide increased potential for security. In the absence of robust personal recognition schemes, these systems are vulnerable to the deception of an impostor. The proposed work in this paper is used to explore the merits of the Biometric Encryption approach of verifying identity, protecting privacy and ensuring security like secure access to buildings, computer systems, laptops, cellular phones and ATMs. An efficient and secured technique has been proposed by applying the hashed key on biometric template generated from input test image. The cryptographic key is generated independently and can be updated periodically via a re-enrollment procedure. The ease and protection provided by proposed technique will certainly help to promote widespread use of cryptographic systems. This technique not only outputs high entropy keys, but also conceals the original biometric data such that it is impossible to recover the biometric data even when the stored information in the system is open to an attacker.

Keywords: *Biometrics, encryption, Hashed key, identification system*

1. Introduction

Recognizing a person using passwords is not sufficient for reliable identity determination because they can be easily shared, or stolen. A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses [2]. Advantages of using biometrics characteristics are reliability, convenience, universality and so on. History has proven that human beings can remember only short password, most of the users even tend to choose password that can be easily guessed using dictionary or brute force search. This limitation has triggered the utilization of biometric to produce strong cryptographic key.

Biometric encryption is a Class of emerging “untraceable biometric” technologies that seek to irreversibly transform the biometric data provided by the user and it is a process that securely binds a PIN or a cryptographic key to a biometric, so that neither the key nor the biometric can be retrieved from the stored template. The key is re-created only if the correct live biometric sample is presented on verification. There are various applications where personal identification is required such as passport control, computer login control, secure electronic banking, bank ATM, credit cards, premises access control, border crossing, airport , mobile phones, health and social services, etc. Many biometric techniques are available such as facial thermo gram, hand vein, gait, keystroke, odour, ear, hand geometry, fingerprint, face, retina, iris, palm print, voice and signature. Among those iris recognition is one of the most promising approach because of stability, uniqueness and noninvasiveness [3].

This paper is organized as follows: Related work for security enhancement of biometrics system are discussed in section2, section 3 presents the proposed system, results are shown in section 4, section 5 provides discussion and section 6 concludes the paper.

2. Related Work

There are numerous works that suggest the combination of biometrics and cryptography as [4, 5] are referred to cancellable biometrics, which uses one way transformation to convert the biometric signal into irreversible form. JinyuZuo, Nalini K. Ratha and Jonathan H. Connell has proposed four cancellable iris biometrics methods that work with conventional iris recognition systems either at unwrapped image level or at binary iris code level [6]. Nick Bartlow, Nathan Kalka, BojanCukic, Arun Ross ShenglinYang, Ingrid Verbauwhedeand many others have made researches to protect fingerprint and iris data and template [7-16].

Davida, et. al., [7] made the use of error-correcting codes in designing a secure biometrics system for access control.

ChanderKant, et. al., [9] presented the idea for biometric security using steganography to make system more secure. While encoding, the secret key (which is in the form of pixel intensities) will be merged in the picture and only the authentic user will be allowed to decode.

Khalil Zebbiche, et. al., [10] proposed wavelet-based digital watermarking method to hide biometric data (i.e. fingerprint minutiae data) into fingerprint images. This provides a high security to both hidden data (i.e. fingerprint minutiae) that have to be transmitted and the host image (i.e. fingerprint).

Supporting the work [7], Juelsand Wattenberg [11] broadened the system by establishing a different way of using error-correcting codes and the approach is known as “fuzzy commitment”.

To protect fingerprint images K. Zebbiche, et. al., [14] presented an efficient technique for use in fingerprint images watermarking. The underlying principle of the technique is embedding the watermark into the ridges area of the fingerprint images which represents the region of interest.

The viability of template-protected biometric authentication systems was exhibited with a fingerprint recognition system by Tuyls, et. al., [15]. A.K.Jain and Uludag U [13] introduced an amplitude modulation-based watermarking method in which they hide a user’s biometric data in a variety of images. By combining asymmetric digital watermarking and cryptography as a powerful mechanism was proposed by Nick Bartlow, et. al., [8] to store raw biometric data in centralized databases.

Shenglin Yang, et. al., [12] presented a template-protected secure iris verification system based on the Error Correcting Code (ECC) cryptographic technique with the reliable bits selection to improve the verification accuracy. In the scheme a transformed version of the iris template instead of the plain reference is stored for protecting the sensitive biometric data.

Jing Dong, et. al., [16] proposed biometric watermarking for protecting biometric data and templates in biometric systems. The scheme suggests protection of iris templates by hiding them in cover images as watermarks (iris watermarks).

3. Proposed Biometric Encryption Work

With the purview of information exchange across the Internet, and the storage of sensitive data on open networks, cryptography is becoming an increasingly important feature of computer security. Many cryptographic algorithms are available for securing information but in general, data will be secured using a symmetric cipher system, while public-key systems will be used for digital signatures and for secure key exchange between users. However, regardless of whether a user deploys a symmetric or a public-key system, the security is dependent on the secrecy of the secret or private key respectively. Because of the large size of a cryptographically-strong key, it would clearly not be feasible to require the user to remember and enter the key each time it is required. Instead, as and when the user presents his biometric code to the system a secret key is generated every time at the server end. The goal of a biometric encryption system is to embed a secret into a biometric template in a way that can only be decrypted with a biometric image from the enrolled person. In the proposed technique we protect the iris code with a hashed key and compare it with input iris code which is used to verify that the user is an authorized one or not. Somehow it is a complicated task but still it will result in a more accurate and efficient verification of the user and thus increase the security level.

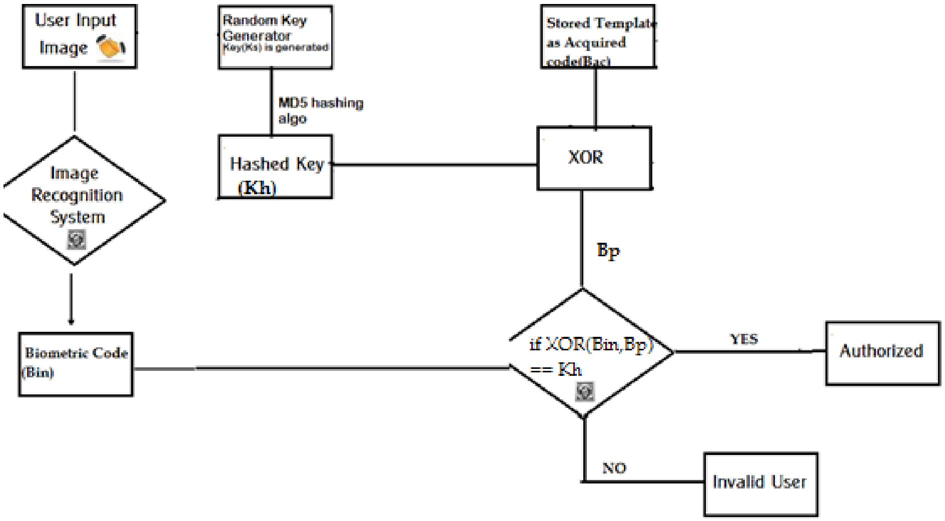

Figure1. Block Diagram of Proposed System

A. Enrollment

The input image is first converted into an Acquired Biometrics code (Bac) with the help of Image recognition system which is a portable transaction terminal comprising a processor; an image configured to produce digital image data using a source of continuous light during production of the digital image data , an image recognition module configured to produce or extract data for a transaction from the digital image data using the processor; and a display linked to the processor being configured to display data or an image corresponding to the digital image data [17]. The image for any person can be utilized to generate unique code. The image passes through a sequence of operations that includes lightening, smoothing, edge detection and binarization proceeds to thinning process and then an initial code is generated.

Secret Key Generation

One of the most critical parts in a security solution is the integrity and confidentiality of the keys used. The production and storage of these keys play a vital role in the security of any key generation system.

Protocol

Let there be a random key generation system, a user and a deterministic algorithm that takes input as seed and output a corresponding secret/public key. The protocol is described as follows

• Enrollment: The user presents biometric data to the system and a template (Bac) is produced corresponding to it.

• Authentication: A user pretending to be original one presents his biometric trait (Bin). As and when the input image is presented random key Ks is computed at the server end. The generated key is then hashed with MD5 hashing algorithm.

Compute XOR (Bac, Kh) = Bp

If XOR (Bp, Bin) = Kh (Hashed Key) then the person is authorized else denied.

The protocol describes steps involved in the key generation and illustrates a special case where only one training sample of the biometric data is presented at enrollment. Moreover user can input their biometric data a few times in order to explore the possible variations of key generated [21].

B. Verification

The foremost step in any biometric technique is to authorize the user who is accessing the system. The authorization is done in the following steps:-

1. **Enrollment:** The input image is presented to the user and biometric code (Bin) is generated from it.
2. **Key Linking**: At the same time a random key is generated by random key generator at the back end. The produced random key (Ks) is then hashed using any hashing algorithm to produce the hashed key (Kh).This hashed key is XORed with the acquired biometrics code (Bac) to form protected biometrics code (Bp)
3. **Key Validation**: Now if XOR (Bp, Bin) = Kh then the user is authorized else the user is not an authorized person.

The choice of hash function is independent of the Biometric Encryption process.MD5 Message-Digest Algorithm is a cryptographic hash function that produces a 128-bit (16-byte) hash value.MD5 algorithm can be used as a digital signature mechanism. Takes as input a message of arbitrary length and produces as output a 128 bit “fingerprint” or “message digest” of the input. Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message [20].

MD5 (Message Digest algorithm) is defined as follows:-

a) Append padded bits: The message is padded so that its length is congruent to 448, modulo 512.

b) Append length: A 64 bit representation of b is appended to the result of the previous step and the resulting message has a length that is an exact multiple of 512 bits.

c) Initialize message digest Buffer which is four-word buffer (A, B, C, D) used to compute the message digest and each of A, B, C, D is a 32 bit register. The registers are initialized to the following values in hexadecimal:

   Word A: 01 23 45 67

   Word B: 89 ab cd ef

Word C: fe dc ba 98

Word D: 76 54 32 10

d) Message is processed in 16-word blocks and four auxiliary functions that take as input three 32-bitwords and produce as output one 32-bit word are defined.

F(X, Y, Z) = XY v not(X) Z

G(X, Y, Z) = XZ v Y not (Z)

H(X, Y, Z) = X xor Y xor Z

I(X, Y, Z) = Y xor (X v not (Z))

e) If the bits of X, Y, and Z are independent and balanced, the each bit of F(X,Y,Z), G(X,Y,Z), H(X,Y,Z), and I(X,Y,Z) will be independent and balanced.

f) The message digest generated as output is A, B, C, D

Mathematical Formulation:-

Here Ks=generated key, Bp=Protected code, Kh = Hashed key, Bac = Acquired biometric code from the image at time of enrollment, Bin= Biometric code from the input image,
Bp = Protected biometric code

Enrollment

1. → *Ue* (Enrolled image).
2. Code_gen(*Ui*) → *Bac.*
3. *Bac is stored.*

Verification

1. →Ui(Input Image)
2. RAND *()*→Ks
3. *Ks*is produced.
4. HashAlgorithm(*Ks*) → *Kh*
5. XOR (Kh, *Bac)* →Protected Code *(Bp).*
6. XOR (*Bp*, *Bin*) == *Ks*
7. If Produced *Kh* = Original Kh then
8. Authentication Achieved
9. Else
10. Access Denied.

4. Results and Discussions

The proposed technique maybe used for implementation and produced unique identifier works more efficiently and uniquely in determining whether the person is authorized or not. The performance of the technique is evaluated in terms of FAR, FRR, EER.

4.2 Performance Evaluation

The performance of system is described by its false acceptance rate (FAR) and false rejection rate (FRR). Another index of performance is equal error rate (EER) defined as the point where FAR and FRR are equal. A perfect system would have zero EER.

Proposed approach may be concluded that the claim of having achieved a zero EER is based upon the impractical hidden assumption of no stealing of the Hash key. The results are worse than when using the biometric alone.

Table 1. Summary of Implementations

Biometric modality	Proposed technique EER	Baseline system EER	Reference
Fingerprint	0%	5,66%	[23]
Iris	0%	3,20%	[25]

5. Conclusion

Both cryptographic method and biometrics based identification have their shortcomings, yet biometric encryption system which combines biometrics and cryptography may provide another effective method to protect peoples' sensitive information. This system has been found to surpass traditional cryptographic systems, because, it is impractical for a person to lose his/ her biometrics, and also the biometrics are difficult to falsify or steal thus providing an efficient approach for concealing biometric templates.

The tentative results have portrayed the efficacy of the proposed approach in protecting the template by immutable cryptographic key. The concluding remarks about proposed technique are:

- performance does not rely on specific biometrics;
- Zero equal error rates can be achieved;
- Clean separation between impostor and genuine distribution;
- Even if the feature extractor is low, performance is accurate;
- Privacy is granted.

References

[1] F. Abdullayeva, Y. Imamverdiyev, V. Musayev and J. Wayman, "Analysis of Security Vulnerabilities in Biometric Systems", Institute of Information Technology of ANAS, Baku.

[2] R. Belguechi and C. Rosenberger, "A Study on the Convergence of Finger Hashing and a Secured Biometric System", LCSI Laboratory, National School of Computer Science, ESI, Algeriar_belguechi@esi.dz, GREYC Laboratory, ENSICAEN - University of Caen - CNRS, France.

[3] A. Juels and M. Wattenberg, "A fuzzy commitment scheme", In Proceedings of the 6th ACM conference on Computer and communications security, New York, NY, USA: ACM Press, **(1999)**, pp. 28–36.

[4] A. K. Jain and U. Uludag, "Hiding biometric data", Proceedings of the IEEE, vol. 25, no. 11, (2004) November.

[5] A. Cavoukian, and A. Stoianov, "Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication", Security AND Privacy, **(2007)** March.

[6] T. Connie, A. Teoh, M. Goh and D. Ngo, "PalmHashing: a novel approach for dual-factor authentication", Pattern Anal. Appl., **(2004)**, pp. 255–268.

[7] C. Kant, R. Nath and S. Chaudhary, "Biometrics security using steganography", International Journal of Security, vol. 2, no. 1, pp. 1-5.

[8] G. Zheng, W. Li and C. Zhan, "Cryptographic Key Generation from Biometric Data Using Lattice Mapping".

[9] Federal Information Processing Standards Publication 180-11995 announcing the standard for secure hash algorithm, **(1995)** April 17.

[10] G. I. Davida, Y. Frankel and B. J. Matt, "On enabling secure applications through off-line biometric identification" , In Proceedings of the IEEE Symposium on Security and Privacy, **(1998)** May, pp. 148–157.

[11] A. Goh and D. C. L. Ngo, "Computation of cryptographic keys from face biometrics", Information Processing, **(2003)**.

[12] J. Dong and T. Tan, "Effects of watermarking on iris recognition performance", 978–1–4244–2287–6, IEEE, **(2008)**.

[13] J. Daugman, "High confidence recognition of persons by test of statistical independence", IEEE Trans. on PAMI, vol. 15, **(1993)**, pp. 1148-1160.

[14] Z. Jinyu, K. R. Nalini and H. C. Jonathan, "Cancelable Iris Biometric", 19th International Conference on Pattern Recognition, **(2008)** December, Tampa, FL, USA.

[15] K. Zebbiche, L. Ghouti, F. Khelifi and A. Bouridane, "Protecting fingerprint data using watermarking", In Proceedings of the first NASA/ESA conference on Adaptive Hardware and Systems (AHS'06), **(2006)**.

[16] B. Kong, K. Cheung, D. Zhang, M. Kamel and J. You, "An analysis of BioHashing and its variants", Pattern Recognition, **(2006)**, pp. 1359–1368.

[17] Key Production System Production of encryption keys in the SecuriVPN system by business security at reqinfo@businessecurity.com.

[18] K. Zebbiche, F. Khelifi and A. Bouridane, "An efficient watermarking technique for the protection of fingerprint images", EURASIP Journal on Information Security, vol. 2008, Article ID 918601, 20 pages doi:10.1155/2008/ 918601, **(2008)**.

[19] B. Ne'ma and H. Ali, "Multi Purpose Code Generation Using Fingerprint Images", The International Arab Journal of Information Technology, vol. 6, no. 4, **(2009)** October.

[20] N. Bartlow, N. Kalka, B. Cukic and A. Ross, "Protecting iris images through asymmetric digital watermarking", 1-4244-1300-1, IEEE, **(2007)**.

[21] L. Nanni and A. Lumini, "Empirical tests on BioHashing", Neuro computing, **(2006)**.

[22] Portable transaction terminal having an image recognition system, Lockheed Martin Corporation, **(2008)** April 8.

[23] N. K. Ratha, S. Chikkerur, J. H. Conne and R. M. Bolle, "Generating cancelable fingerprint templates", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, **(2007)** April, pp. 561-572.

[24] S. Prabhakar, S. Pankanti and A. K. Jain, "Biometric recognition: security and privacy concerns", In Proceedings of the IEEE Security & Privacy, **(2003)** March-April, pp. 33-42.

[25] M. Savvides, B. V. Kumar and P. Khola, "Cancelable biometric filters for face recognition", in Proceedings of the 17th International Conference on Pattern Recognition (I ICPR04), vol. 3, **(2004)** August, pp. 922–925

[26] S. Yang and I. Verbauwhede, "Secure iris verification", In Proceedings of the ICASSP, **(2007)**, pp. 133-136.

[27] A. Teoh, D. Ngo and A. Goh, "BioHashing: two factor authentication featuring fingerprint data and tokenised random number", Pattern Recognition, **(2004)**.

[28] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G. -J. Schrijen, A. M. Bazen and R. N. J. Veldhuis, "Practical biometric authentication with template protection", In Proceedings of the 5th International Confernce on Audioand Video-Based Personal Authentication, **(2005)**, pp. 436-41.