ISSN: 2321-7782 (Online)
Volume 3, Issue 9, September 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Hybrid Approach for Securing Biometric Templates Using Visual Cryptography

K. Sankareswari[1]
Assistant Professor Department of Computer Applications
Fatima College
Madurai, Tamilnadu, India

Dr. S. Arul Jothi[2]
Assistant Professor Department of Computer Science
Fatima College
Madurai, Tamilnadu, India

Abstract: Security of information is one of the most important factors of information technology and communication. Also an accurate automatic personal identification is essential in a wide range of application domains such as national ID card (Aadhar Card), electronic commerce, and automated banking. So systems need strong security to protect data and resources access from unauthorized users. A Biometric-based authentication system provides more security than other conventional approaches. Single biometric systems have a variety of problems such as noisy data, non-universality, spoof attacks and unacceptable error rate. These limitations can be solved by deploying hybrid biometric systems. Hybrid biometric systems utilize two or more individual modalities, like face, iris, retina, signature, voice and fingerprint. Hybrid biometric systems improve the recognition accuracy more than single system. As biometric template are stored in the centralized database, due to security threats biometric template may be modified by attacker. Preserving the privacy of digital biometric data (e.g., face images, iris and fingerprint) stored in a central database has become of paramount importance. Visual cryptography is the technique used to encrypt the data which is in the form of visual information such as images. Since the biometric templates stored in the database is usually in the form of images, the visual cryptography can be efficiently employed to encrypt the templates from attacks. This paper explores the possibility of using visual cryptography for imparting privacy to hybrid biometric data such as fingerprint images and iris codes.

Keywords: Biometrics, Visual cryptography, Fingerprint authentication, Iris authentication.

I. Introduction

A. Biometric System

Biometrics is the science and technology of measuring and analyzing biological data. In computer security, biometrics refers to authentication technique; Biometric authentication is an automated method whereby an individual's identity is confirmed by examining a unique physiological trait or behavioral characteristic, such as a fingerprint, iris, face, voice, retina, or signature [1].

B. Types of Biometric System

The Biometric system is basically divided into two modules

1) Single biometric system and 2) Hybrid (multi) biometric system.

1) Single Biometric System

Biometric systems based on single source of information to identify the user are called single biometric systems. It is also called as unimodal biometric systems [2]. Example: Biometric system based on Face or Palm print or Voice or Gait etc. Each biometric trait should pose attributes like Uniqueness, and hard to circumvent. Sadly, recent researches have shown that an attacker can lift and replicate the biometric traits, which later can be used to attack on biometric systems. As a result, hybrid biometric systems have been proposed to increase the recognition accuracy as well as security against attacks as compared to the single biometric systems that make them up.

2) Hybrid Biometric System

The term "Hybrid" is used to combine two or more different biometric sources of a person (like face and fingerprint) sensed by different sensors. Two different properties (like infrared and reflected light of the same biometric source, 3D shape and reflected light of the same source sensed by the same sensor) of the same biometric can also be combined. In orthogonal multi biometrics, different biometrics (like face and fingerprint) are involved with little or no interaction between the individual biometric whereas independent multimodal biometrics processes individual biometric independently. Orthogonal biometrics are processed independently by necessity but when the biometric source is the same and different properties are sensed, then the processing may be independent, but there is at least the potential for gains in performance through collaborative processing. In collaborative hybrid biometrics the processing of one biometric is influenced by the result of another biometric. The most compelling reason to combine different modalities is to improve the recognition rate. This can be done when biometric features of different biometrics are statistically independent. There are other reasons to combine two or more biometrics. One is that different biometric modalities might be more appropriate for the different applications. Another reason is simply customer preference. Multi-modal biometrics usage is being actively considered in applications involving Border Control, Physical Access Control, and PC/Network security.

C. Need of Hybrid Biometric System

Biometric systems based on one (one-modal) biometric 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, restricted degree of freedom, non-university, spoof attacks and unacceptable error rates. It leads to considerably high false acceptance rate (FAR) and false rejection rate (FRR), limited discrimination capability, upper bound in performance and lack of permanence. Some of these limitations can be addressed by deploying hybrid biometric systems that integrate the evidence presented by multiple sources of information.

II. Visual Cryptography

For protecting the privacy of an individual enrolled in a biometric database, Davida et al. [3] and Ratha et al. [4] proposed storing a transformed biometric template instead of the original biometric template in the database. This was referred to as a private template [3] or a cancelable biometric [4]. Feng et al. [5] proposed a three-step hybrid approach that combined the advantages of cryptosystems and cancelable biometrics. Apart from these methods, various image hiding approaches [6]–[8] have been suggested by researchers to provide anonymity to the stored biometric data. Arun Ross and Asem Othmen suggested the use of Visual Cryptography for protection of biometric template. Cryptography introduced by Naor and Shamir [9] is a method used for encrypting a secret image into shares, such that stacking the shares reveals the secret image. The main advantage of Visual Cryptography is the decryption of the message which does not involve more process. The decryption time is very less when Visual Cryptography provides a very powerful technique by which one secret can be distributed in two or more shares. When the shares on transparencies are superimposed exactly together the original secret can be discovered without computer participation.

This scheme is referred to as the *k*-out-of-*n* VCS [2][3] which is denoted as (*k*,*n*)VCS. Given an original binary image, it is encrypted in *n* images, such that

$$T\oplus = S_{h1} \oplus S_{h2} \oplus \quad S_{h3} \qquad \ldots\ldots\ldots\ldots\ldots \; S_{hn} \, (1)$$

where ⊕ is a Boolean operation, k≤n, n is the number of noisy images, *Shi; hi €* 1,2,….*k* is an image which appears as white noise, *k* d" *n*, and *n* is the number of noisy images. It is difficult to decipher the secret image *T* using individuals *Shi*'s [6]. The encryption is undertaken in such a way that *k* or more out of the *n* generated images are necessary for reconstructing the original image *T* . In the case of (2, 2) VCS, each pixel *P* in the original image is encrypted into two sub pixels called shares.

For biometric privacy, here 2-out-of-2 scheme is using. In this scheme for sharing a single pixel p, in a binary image Z into two shares scheme 1 and scheme 2 is illustrated in figure 1. If p is white, one of the two schemes in the first row of figure 1 is chosen randomly to encode A and B. If p is black, one of the two schemes in the last row in figure 1 is chosen randomly to encode A and B.

	Scheme 1			**Scheme2**			**Output of**	
Pixel in original image	**Share 1**		**Share2**	**Share 1**		**Share 2**	**Scheme 1**	**Scheme 2**
For White pixel □	■□	+	■□	□■	+	□■	■□	□■
For black pixel ■	■□	+	□■	□■	+	■□	■■	■■

$$C_0 = \left\{ \begin{bmatrix} 01 \\ 01 \end{bmatrix} \begin{bmatrix} 10 \\ 10 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \begin{bmatrix} 01 \\ 10 \end{bmatrix} \begin{bmatrix} 10 \\ 01 \end{bmatrix} \right\}$$

Fig. 1 Partition for black and white pixels in 2 by 2 scheme

Thus, neither A nor B exposes any clue about the binary color of p. When these two shares are superimposed together, two black sub-pixels appear if p is black, while one black sub-pixel and one white sub-pixel appear if p is white as indicated in the figure 2. Based upon the contrast between two kinds of reconstructed pixels can tell whether p is black or white.

III. SECURE FINGERPRINT TEMPLATES

As Nalini K. Ratha et al[10] pointed out that the stored template in the database attacker may try to alter result in authorization for a unauthorized users, or denial of service for the authenticated user related with the corrupted template. Here iris and fingerprint template is protected by applying visual cryptography. Visual cryptography is used for securing fingerprint templates. In this system there are two modules: Enrollment module and Authentication module. First is enrollment, in which admin creates shares by enrolling employees fingerprints. And the second part is related to the authentication which is required to be done by employee. These two parts are explained below.

A. Enrollment

In the enrollment part, the administrator will collect the fingerprint and eye image of the eligible users those are having access to secure resource. The enrolled biometric image is required to be processed so characteristic fingerprint and iris features can be extracted and are divided in to two shares. Among these shares first share is stored on the user's identity card and other is saved in the database. So next time when user comes for authentication he need to provide his ID card, finger print and iris as he is already enrolled in the system.

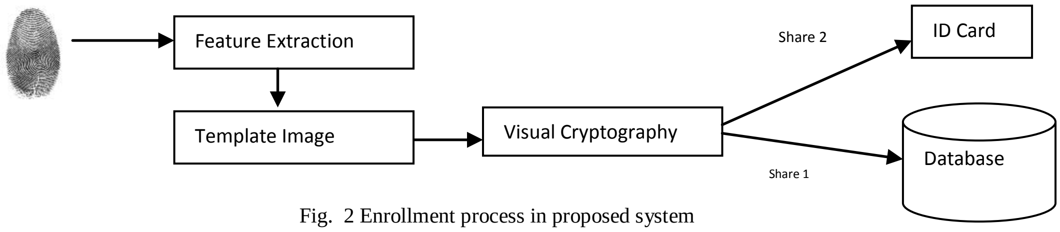

Fig. 2 Enrollment process in proposed system

B. *Authentication*

Authentication part of the proposed system is related to the each time authentication done by the enrolled user of system or employee. In this he has to provide ID card allocated to him and his fingerprint and iris image in order to complete authentication. As there is one share saved on ID card and other is in the database when user provides ID card, by using the share on the ID card and other share in the database we create the temporary image which have the features from the original image which was provided during the enrollment of user. This temporary image is then matched with the fingerprint which is provided in the authentication. Which then provides result as either authenticated or not.

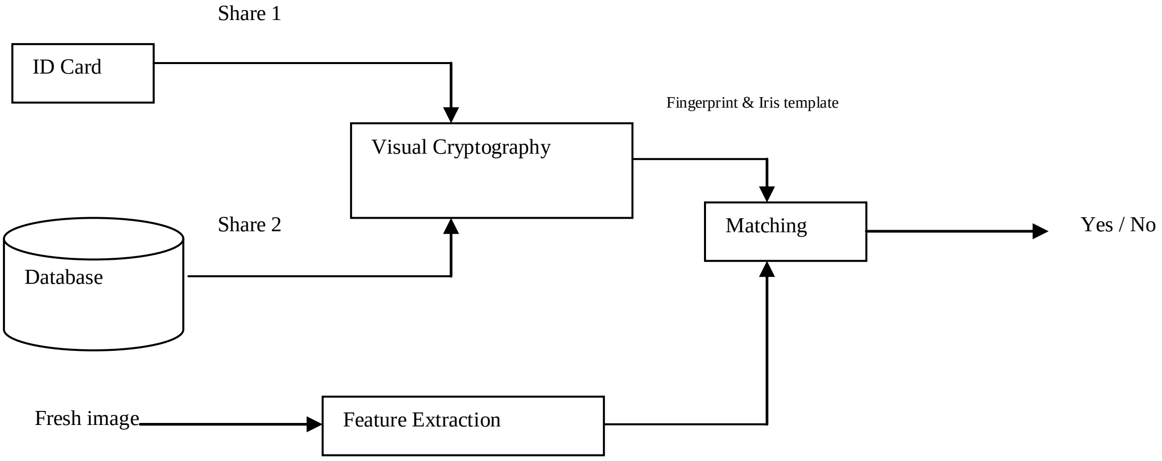

Fig. 3 Authentication process in proposed system

IV. Conclusion

Various approaches were adopted by researchers to secure the raw biometric data and template in database. In this paper a method is proposed to store hybrid biometric templates securely in the database. To secure finger print and iris image in the database, the input fingerprint and iris image is decomposed and encrypted in two independent shares. The fingerprint and iris image can be reconstructed only when both sheets are simultaneously available. It is able to obtain the reconstructed images from sheet images similar to original image. Applying visual cryptography techniques on hybrid biometric template provides more security. Also it is computationally hard to obtain the biometric image from the individual stored sheets due to visual cryptography, which enhance the system security.

Acknowledgement

We thank God the Almighty of showering his grace and without which we would not have finished the work. Our heart felt thanks to our beloved Secretary Sr. S. Francis Pauline and beloved Principal Dr. Sr. K. Fatima Mary, Fatima College for their constant support and encouragement. We thank our colleagues from Fatima College, Madurai who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper. Finally, we sincerely thank to our parents, family, and friends, who provide the advice and financial support. The product of this research paper would not be possible without all of them.

References

1. K. Jain, A. Ross, and S. Prabhakar. An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, 14(1): 4–20, January 2004.
2. A. Ross, K. Nandakumar, and A. K. Jain. Hand book of Multi biometrics. Springer, New York, USA, 1st edition, 2006.
3. G. I. Davida, Y. Frankel, and B. J. Matt, On enabling secure applications through off-line biometric identification, in Proc. IEEE Symp. Security and Privacy, 1998, pp. 148–157.
4. N. Ratha, J. Connell, and R. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Syst. J., vol. 40, no. 3, pp. 614–634, 2001.
5. Y. Feng, P. Yuen, and A. Jain, A hybrid approach for face template protection, in Proc. SPIE Conf. Biometric Technology for Human Identification, Orlando, FL, 2008, vol. 6944.
6. A. Jain and U. Uludag, Hiding biometric data, IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 11, pp. 1494–1498, Nov. 2003.
7. J. Dong and T. Tan, Effects of watermarking on iris recognition performance, in Proc. 10th Int. Conf. Control, Automation, Robotics and Vision, 2008 (ICARCV 2008), 2008, pp. 1156–1161.
8. N. Agrawal and M. Savvides, Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching, in Proc. Computer Vision and Pattern Recognition Workshop, 2009, vol. 0, pp. 85–92.
9. M.Naor and A. Shamir, Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.
10. Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle, An Analysis of Minutiae Matching Strength, In Proceedings of the 3rd AVBPA, Halmstad, Sweden,223-228 ,June 2001.
11. Y. Rao, Y. Sukonkina, C. Bhagwati, and U. Singh, Fingerprint based authentication application using visual cryptography methods (improved id card), in Proc. IEEE Region 10 Conf., Nov. 2008, pp.1–5.
12. P. Revenkar, A. Anjum, and W. Gandhare, Secure iris authentication using visual cryptography, Int. J. Comput. Sci. (IJCSIS), vol. 7, no. 3, pp. 217–221, Mar. 2010.

AUTHOR(S) PROFILE

K.Sankareswari, received the M.Phil degree in Computer Science from Madurai Kamaraj University in 2007, MCA degree and B.Sc Computer Science from Sri Meenakshi Govt. College for Women, Madurai, Tamilnadu, India in 2005 and 2001. From 2006 worked as a Web Developer in DHAN Foundation till 2014, Madurai. After that she is working as an Assistant Professor in Fatima College, Madurai. She has published various papers on journals, seminars and conferences. Her area of interest is information security and biometric systems.

Dr. S. Arul Jothi, received the PhD degree in the area of Cryptography from Kalasalingam University in 2015, M.Phil, M.Sc, and B.Sc, degree from Madurai Kamaraj University. From 2000 she worked as an Assistant Professor in N.M.S. Sermathai Vasan College till Nov 2014. After that and till now she is working as Assistant professor in Fatima College. She has 6 publications in various international journals and 2 international conferences. Her current research interests are Information security and Image Processing.