International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Visual Cryptography for Providing Privacy to Biometric Data

Santosh Varpe[Á*]

[Á]Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar, India

Accepted 30 Nov 2014, Available online 01 Dec 2014, **Vol.4, No.6 (Dec 2014)**

Abstract

It is important to keep privacy of biometric data that stored in a central database. using visual cryptography it is easy to enhance the privacy of biometric data such as face images, palm images, iris code. A private face image is dithered into two images and stored them on two different database server. When the both images combine together after that we find the private image. Visual Cryptography is a process of creating shares from an Image so that it would become unreadable for unauthenticated person. This paper implements visual cryptography for color images

Keywords: *Face Detection, Visual Cryptography, Image Authentication, Privacy.*

1. Introduction

In general, **biometrics** is a collection of measures of human physiology and behavior. A biometric system could scan a person's fingerprint or analyze the way he types on a keyboard. The purpose of most biometric systems is to authenticate a person's claimed identity. There are various application where authentication is required (such as online banking, mobile phones, computer data) for this biometric is best way for providing robust or high authentication. Many biometric techniques are available such as fingerprint, face, iris, retina, palm print, ear, gait, keystroke, odor, voice, hand geometry and signature. Among all of this face recognition is best option for authentication.

For example three persons have deposited their money in a bank account. These persons do not trust each other and they do not want a single member of themselves to withdraw the money. However, they assume that withdrawing money by two members of the group is not considered a conspiracy; rather it is considered to have received "authorizations". Therefore, they decided to encode the bank code into three partitions so that any two or more partitions can be used to reconstruct the code. Since the person representatives will not have a computer with them to decode the bank code when they come to withdraw the money, they want to be able to decode visually: each person gets a transparency. The transparency should yield no information about the bank code. However, by taking any two transparencies, combining them together and aligning them, they will get a secret number". How can this be done? The solution is proposed in 1994 by Naor and Shamir who introduced a simple and secure way that allows secret sharing without any cryptographic computation, which they called as Visual Cryptography Scheme (VCS).

*Corresponding author: **Santosh Varpe**

With the rapid changes of network technology, it is easy to transmit multimedia information on the Internet. Many times confidential information such as company project work, military information are transmitted over the Internet. Before using secret images, firstly security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want .To deal with the security problems of secret images, various image secret sharing schemes have been developed. Visual cryptography is introduced by first in 1994 Noar and Shamir. The following fig 1.shows the encryption and decryption of image using cryptography.

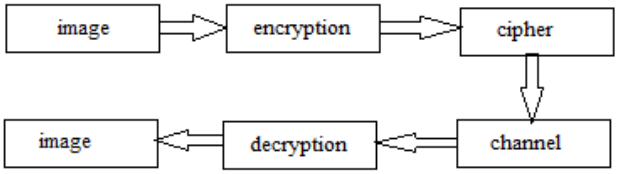

Fig.1 cryptography

Cryptography is a method of storing and transmitting data in a particular form. The term is most often associated with scrambling plaintext or clear text into cipher text called encryption then back again called decryption.

Now, Advantages and disadvantages and Applications of visual cryptography

Advantages

1) Simple to implement.
2) Lower computation cost since secret message is recognized only by human eyes.

Disadvantages

1) The contrast of the reconstructed image is not maintained.

2) Perfect alignment of the transparencies is troublesome.

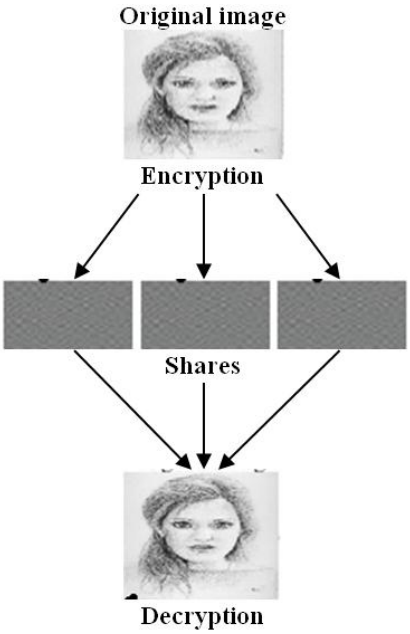

Fig.2 Example of Visual Cryptography

Problem Identification

Applications

1) For providing the high level of security to Biometric.
2) For the watermarking.

Possibility of biometric data stored on the database server may be altered by attacker. Due to this authorize user will not access the system. For this visual cryptography technique can be applied on biometric template. It provides the high security to user. There is many attacks that attack on biometric data.

2. Research Objectives

- One of the main objectives for visual cryptography is to achieve Security. It is hard to obtain the private biometric image from the individual stored sheets because of visual cryptography. The private image is found only when both sheets are available.
- To keep the quality of original image as it is after decryption.
- It is numerous efforts to protect data stored in distributed databases from unauthorized modification and inaccurate updates.

3. Authentication of shares

Firstly share1 and share2 are combine and face image shares of visual cryptography are match together if match then image is display otherwise image does not display.
Suppose the data D is divided into n shares D can be constructed from any k shares out of n complete knowledge of k-1 shares reveals no information about D.
K of n shares is necessary to reveal secret data.

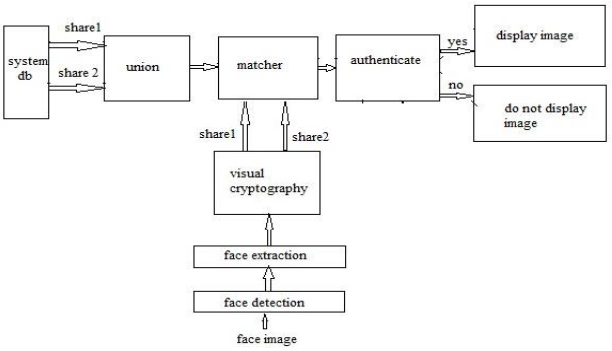

Fig.3 Authentication of user

Conclusion

Using visual cryptography it is easy to increase the privacy of biometric data such as face images, iris code. A private face image is dithered into two images and stored them on two different database server. When the both images combine together after that we find the private image. It is impossible to recover the original image without accessing both the shares. It is hard to attackers to decrypt the data of database. if he try to decrypt the share of one database server, he cannot access the application he need the both the shares of distributed database server.

Performance of visual cryptography depends on security, accuracy, share generated. Visual cryptography provides the best authentication for the biometric authentication system. Increasing the more shares it decreases the decrypted image quality. So use the optimal shares for accuracy.

Acknowledgment

This paper has completed only because support from teachers, colleague. Especially, my acknowledgment of gratitude toward the following important persons: First I would like to thank my teachers Mr. M. Kshirsagar Sir, Mr. Jaypal sir, Mr. Prabhudeo sir to their support and encouragement. Second, I sincerely thank to my parents who provide the advice.

References

Atul Sureshpant Akotkar, Chaitali Choudhary (2014), Secure of Face Authentication using Visual Cryptography, IJISME, ISSN: 2319-6386, Volume-2, Issue-5.

Arun Ross, Asem Othman (2013), Visual Cryptography for Biometric Privacy, IEEE Transaction on information forensics and security , vol.6 no.1.

A. Jain, P. Flynn, and A. Ross (2007), Handbook of Biometrics, New York: Springer.

N. Ratha, J. Connell, and R. Bolle (2001), Enhancing security and privacy in biometrics-based authentication systems, IBM Syst. J., vol. 40,no. 3, pp. 614–634.

A. Jain and U. Uludag (2003), Hiding biometric data, IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 11, pp. 1494–1498.

P. S. Revenkar, W. Z. Gandhare (2007), Secure iris authentication using visual cryptography, IJCSIS,1947-5500.

P. S. Revenkar, Anisa Anjum, W. Z. Gandhare (2010), Survey of Visual Cryptography Schemes, International Journal of Security and its Applictions, Vol.4, No.2.

N. Agrawal and M. Savvides (2009), 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 , vol. 0, pp. 85–92.

B. Moskovich and M. Osadchy (2010), Illumination invariant representation for privacy preserving face identification, in Proc. IEEE Computer Society and IEEE Biometrics Council Workshop on Biometrics, San Francisco, CA, pp. 154–161.

R. Gross, L. Sweeney, F. De la Torre, and S. Baker (2006), Model-based face de-identification, in IEEE Workshop on Privacy Research in Vision, Los Alamitos, CA.

D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. K. Nayar (2008), Face swapping: Automatically replacing faces in photographs, ACM Trans. Graph., vol. 27, no. 3, pp. 1–8.

E. M. Newton, L. Sweeney, and B. Malin (2005), Preserving privacy by de-identifying face images, IEEE Trans. Knowl. Data Eng., vol. 17, no. 2, pp. 232–243.

Santosh Varpe received the B.E.(Hons.) degree in Computer Engineering from the S.G. Raisoni COE, Ahmednagar(2013), Savitribai phule pune university, and Pursuing M.E.(Hons.) degrees in Computer Engineering from Vishwabharati Academy's COE, A.nagar, savitribai phule pune university, Maharashtra, India.