International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Visual Cryptography for Biometric Privacy

Shubhangi Rajanwar[1], Shirish Kumbar[2], Akshay Jadhav[3]

Abstract: ***"Biometric", is used for authentication. The "Biometric" word is come from the two separate words 'bios and metricos' i.e. Greek words. That means for "life measure". The Biometrics are user friendly. To work with the biometrics authentication that is used to collect some raw biometric data (e.g. image) and then that data compares with the data (e.g. image) stored in the database for providing access. So at the same time there may be possibilities of the attackers to attack on the data stored in database. Therefore the security of the biometrics is very important thing. Biometrics Systems consists of the physical and behavioural features for e.g. face, fingerprints etc. So the purpose of this paper is to protect biometrics data from the various attacks. We are using the concept of visual cryptography, where cryptography is the concept of sending and receiving encrypted messages and that can be decrypted by the authorised persons with the required keys only. In another way cryptography is the secret communication of the images with authorised persons.***

Keywords: Balanced Block Replacement(BBR), Cover Images, Extended Visual Cryptography (EVC), Floyd Steinberg Error Diffusion, Gray scaling, Rescaling, Transparencies Secret Image

1. Introduction

1.1 About the Project

In current times identity of a person is what matters the most so in accordance with that we are proposing a concept "Visual Cryptography for Biometric Analysis' under which we are providing security to the images. We are implementing this project to provide secure way to send and receive the images which are of critical importance to us.

1.2 Purpose

When we transmit data(image) over the network, then any unauthenticated person can read our data (image). So in order to provide the security to data (image) generally the sender will encrypt the data(image) and then send it to the intended person and the receiver will decrypt that encrypted data(image) and uses it. Visual cryptography comes with the guarantee of the security by means of defining perfect secrecy. Usually, a set of players(attackers) are not allowed to learn any information about the (one)secret image even under the possibility of collusion.

2. Proposed

In the Visual Cryptography, There are some algorithms for encrypting and decrypting the images. In this project we are using one secret image and two cover images, Then the secret image and cover images are overlapped with each other. And if both the cover images are simultaneously available then only we can access the secret image. The single share cannot give any data(information) about the secret image. We are using "Floyd Steinberg Error Diffusion" Algorithm for Half toning an input image and Converts into Gray scale image of the range 0-255 scale into the much smaller scale like all of the pixels in an image will be either 0, 80,120,150,170,225,255 only. We are using BBR Algorithm for process of Encryption and the process of decryption is an OR operation of the project. So when pixel values are at defined positions that are read from the two shares and the minimum of the two is selected as pixel value of secret image.

3. Existing System

Cryptography is one of the most important technique for protecting the data such as biometric templates. It is the concept of sending and receiving encrypted messages that is the communication of the messages that can be decrypted only by the authorized sender or the receiver. The Encryption Process and decryption Process are accomplished by using the mathematical algorithms in such a way that only intended receiver(authorized receiver) can decrypt that encrypted message and read it. Naor and Shamir are the most popular authors for introducing the Visual Cryptography Scheme(VCS), as a simple and secure way to provide the secret communication of images without any cryptographic computations. VCS(Visual Cryptographic Scheme) is a cryptographic technique for the encryption of visual information such that the decryption process can be done by the human visual systems. Using this technique the biometric data(e.g. image) is captured from the authorized user. This original image is divided into the two cover images and, then each cover image is stored in two different databases geographically apart. When both the cover images are simultaneously available then only we can access that original image. But it requires more space for storing sheets due because of the pixel expansion. So the size of the original image becomes larger instead of original size this is the disadvantage of the existing system and we are providing a solution for this.

3.1 Drawback of Existing System

When we apply visual cryptography in the existing system, the pixel expansion occurs resulting in the increased size of original image.

4. Proposed System

4.1 Extensive Technical Research

4.1.1 Visual Cryptography Scheme (VCS)
In the Existing System of visual cryptography, the secret image and cover images should be of the similar size. But in the proposed system if size of all three images is different from each other, still we are able to use visual cryptography

on those images by using the rescaling module. So in our proposed system this bug is countered. VCS allows one to encode a secret image into different sheet images, each having no information about the original image(secrete image). Since these sheets are having a random set of pixels, they may get the curiosity of an interceptor by giving the existence of a secret image. To mitigate this Ateniese has introduced new framework technique known as the extended VCS.

4.2 Pre-processing Halftone Images

We consider the application of visual cryptography to grayscale images by first converting the images to a binary image using a halftoning algorithm. After creating a halftone image, in order to preserve the image size when applying visual cryptography and extended visual cryptography, simple methods can be applied.

4.3 Rescaling Images

In earlier times it used to happen that whenever we upload images the secret image turns out to be of larger size in terms of pixel resolution. To counter this problem we are using rescaling method. Rescaling algorithm was introduced which functions in a way such that when we upload irrespective of their pixel size variances, the algorithm adjusts the sizes of the images to a fixed size and reveals the output image of the same size. As the Visual Cryptography works only on the black and white images and images of the fix size. If the Uploaded images are of the different size then visual cryptography not work, So we are converting those images into fix size by using rescaling method.

4.4 Gray Scaling

Visual Cryptography is not work for the color images, it only works for the black and white images. So that we are using Gray scaling method for converting the color images into grayscale images

4.5 Floyd–Steinberg

In this technique, The Digital Haftoning Method is used. There are some printer devices that does not contain so many shades of the grayscale. If minimum shades are available then it will print only that no of minimum shades otherwise it will not print. So by using printer palate we can define our own values for the palate.

e.g. if we have define palate values as (0 70 120 180 255) then every pixel is having values nearer to the palate values then that palate value is assign to that pixel that is new value of that pixel. e.g. if the pixel value is 60 then the 70 is nearest value for the pixel then the 70 is assign to that pixel instead of 60 but the initial value of that pixel is 60 and extra is 10 (70-60),this occurring quantization error. So we have to remove this error by using error diffusion method. Error diffusion is a type of halftoning in which the quantization error is distributed to neighboring pixels.

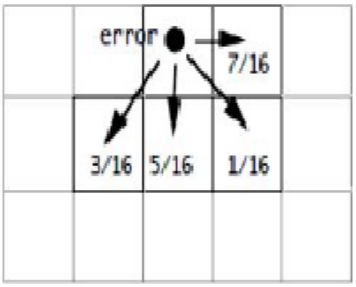

Figure 4.5.1: Error Diffusion

In the above diagram the error is diffuse with nearest four pixels.

4.6 Balanced Block Replacement (BBR)

We are using this technique for avoiding pixel expansion during hiding the original image into cover images. There are certain combinations to place the pixels either in white color or black color. Each pixel is divided into parts and each part is called as cluster. In the table below, Each pixel in share 1 and share 2 is divided into four parts, i.e. combination of black and white pixel's color. if we have black shade for one cluster in the share one and white shade for one cluster in the share two then we have to store it with the black shade in the stack.

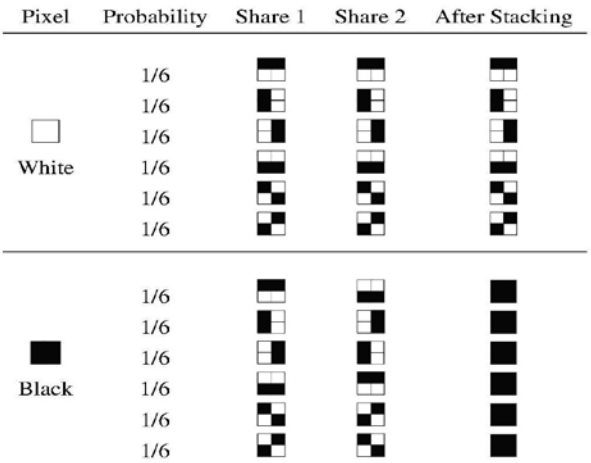

Figure 4.6.1: Diagram for BBR

4.7 Pattern Match

Pattern Matching is the act of checking a given sequence of tokens for the presence of the constituents of some patterns. When we access the secret image then that image is compared with the image stored in the database. If the comparison is nearer to 98% or 99% then we can access secret image. But if the comparison is less than 98% then image cant access by that unauthorized person.

4.8 Advantage

1) No Pixel Expansion The size of original image is as it is.
2) High Level Security for biometric privacy.
3) Prevent Attacks of biometric images.
4) Secure Databases.

5. Software Tools

5.1 Software Requirement-

1) Operating System - Windows 7/8
2) Application Server - Apache Tomcat 7.0.34
3) Front End - HTML, Java, Jsp, Css
4) Scripts - JavaScript
5) Server side Script - Java Server Pages
6) Database - MySQL
7) Database Connectivity - JDBC

5.2 Hardware Requirement-

1) Personal computers with required Configuration.
2) Biometrics kit to fetch human biometric data and transform it into a image.

6. Data Flow Diagram

6.1 DFD Level-0-

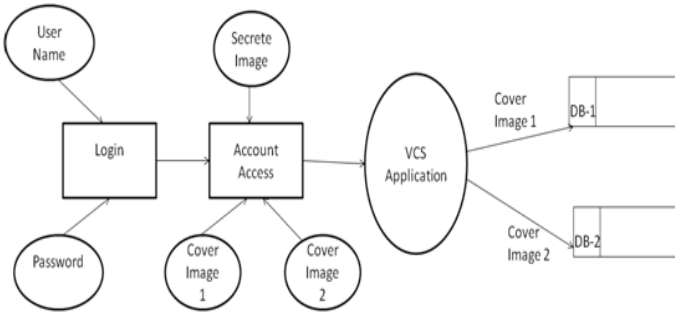

Figure 6.1.1: DFD Level-0 for Proposed System.

6.2 Activity Diagram

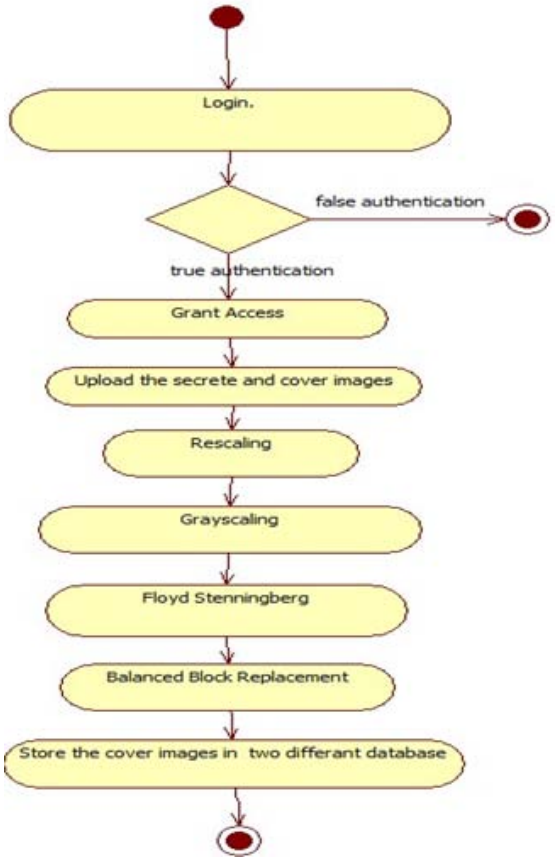

Figure 6.2.1: Activity Diagram For Proposed System.

7. Conclusion

Thus we have studied to protect the privacy of a image database by decomposing an input private image into two independent sheet images such that the private image can be reconstructed only when both sheets are simultaneously available. The proposed algorithm selects the host images that are most likely to be compatible with the secret image based on geometry and appearance. Increasing the pixel expansion factor can lead to an increase in the storage requirements for the sheets. In the recent literature there have been some efforts to develop a VCS without pixel expansion. But no such scheme currently exists for generating sheets that are not random noisy images. Thus, more work is necessary to handle this problem.

8. Future Enhancement

It can be used for all of the security related institutions like military, offices, confidential laboratories. It will work for the multiple systems and multiple cover images. It will work for more databases for more security.

9. Acknowledgement

We thank Dr. R.S. Jahagirdar (Principal IOKCOE Pune) for providing necessary facilities to carry out the work. We are very thankful to Prof. Saba Siraj (Assistant Professor) for her useful guidance.

References

[1] Pardhasaradhi, P.Seetharamaiah, "A Rumination of Error Diffusions in Color Extended Visual Cryptography", *International Journal of Computer Trends and Technology (IJCTT) – volume 15 number 1 – Sep 2014,ISSN: 2231-5381.*

[2] N. Askari, H.M. Heys, and C.R. Moloney, "AN EXTENDED VISUAL CRYPTOGRAPHY SCHEME WITHOUT PIXEL EXPANSION FOR HALFTONE IMAGES", IEEE Canadian Conference Of Electrical And Computer Engineering (CCECE), 2013 26th.

[3] Dr.V.R.Anitha, Dilipkumar Kotthapalli, "Extending the Visual Cryptography Algorithm Without Removing Cover Images", *International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue4- April 2013*, ISSN: 2231-5381.

[4] Arun Ross, Asem Othman, "Visual Cryptography for Biometric Privacy", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, MARCH 2011.

[5] Arun Ross and Asem A. Othman, "Visual Cryptography for Face Privacy", Proc. of SPIE Conference on Biometric Technology for Human Identification VII, (Orlando, USA), April 2010.

[6] 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.

[7] 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.

[8] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. K. Nayar, "Face swapping: Automatically replacing faces in photographs", *ACMTrans.Graph.*, vol. 27, pp. 1–8, 2008.
[9] B. Thuraisingham and W. Ford, "Security constraint processing in a multilevel secure distributed database management system", *IEEETrans. Knowl. Data Eng.*, vol. 7, pp. 274–293, Apr. 1995.
[10] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40,pp. 614–634, 2001.
[11] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Secaucus, NJ: Springer-Verlag New York, Inc.,2003.
[12] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy*, vol. 1, pp. 33–42, Mar./Apr. 2003.
[13] Souvik Roy and P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography", 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science 978-1-4799-2526-1/14/$31.00 ©2014 IEEE.
[14] Prateek Kumar1, Suneeta Agarwal2, and Shivendra Shivani3 *1, 2, 3MNNIT Allahabad, Uttar Pradesh*, "Halftone Visual Cryptography with Pixel Expansion through Error Diffusion", International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 14 (2014), pp. 1419-1427 © International Research Publications House http://www. irphouse.com.
[15] Anandhiand S.Satthiyaraj," Embedded Visual Cryptography Schemes for Secret Images ", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.12, December 2012 153 Manuscript received December 5, 2012 Manuscript revised December 20, 2012.

Author Profile

Miss. Shubhangi S. Rajanwar born on July 8, 1994 is pursuing BE Computer Engineering, from Institute of Knowledge College of Engineering, Pune, Maharashtra, India

Mr. Shirish S. Kumbar born on July 8, 1993 is pursuing BE Computer Engineering, from Institute of Knowledge College of Engineering, Pune, Maharashtra, India

Mr. Akshay A. Jadhav. born on February 5, 1994 is pursuing BE Computer Engineering, from Institute of Knowledge College of Engineering, Pune, Maharashtra, India