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 S. Varpe†* and Prabhudev Irabashetti†

†Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar, India

Accepted 10 Aug 2015, Available online 15 Aug 2015, **Vol.5, No.4 (Aug 2015)**

Abstract

Biometric authentication is consider as best authentication than the other, because it uses unique physiological characteristics such as face images , palm images ,iris code. It is important to keep biometric data that generated at the time of enrollment .Using visual cryptography it is easy to enhance the privacy of biometric data. A private face image is to hide into two host images and convert them into gray scale image and encrypt it and generate sheets that stored on database server. In GEVCS Authentication only done when original image and gray scale sheet and other sheets are available. So visual cryptography provides better privacy to biometric data. This system is used for any images.

Keywords: *Visual cryptography, Image processing, Authentication, Biometric data, Privacy.*

1. Introduction

Biometrics means use of unique physiological characteristics such as face, fingerprints, retina, vein to identify an individual. Biometric is used for identification as well as verification of person. A biometric authentication system operates by using raw biometric data from a subject (e.g., face image), extracting a feature set from the data and comparing the feature set with the templates stored in a database to identify the particular person. At the time of enrollment the template of a person is generated and that template is stored along with original raw data. This has increase the need to preserved privacy to the person image by protecting the contents of the database. A grayscale image is an image in which the value of each single pixel is a sample, that is, it carries only intensity information. The darkest possible shade is black, which is the total absence of transmitted or reflected light and the lightest possible shade is white. According to their physical characteristics, different media use different ways to represent the color level of images. The computer screen uses the electric current to control lightness of the pixels. The diversity of the lightness generates different color levels. The use of face images as hosts for a private face image has many advantages in the area of biometric applications.

A private image is converted into gray scale image for this multiplying red ,green, blue by random numeric values, after that giving name to that gray scale image, then choosing two host image and splitting original image into two host image and encrypting that grayscale image and generating sheets. Encrypting image using key and that key is generated by using math.random() function, storing sheets on database server.

Few basic definitions

Plaintext is the original message.
Encryption means transforming plaintext message into ciphertext.
Secrete key use for encryption and decryption of message.
Ciphertext is the scrambled message produced as output.
Decryption means obtain original message from cipher text.
The science and art of manipulating messages to make them secure is called **Cryptography.**
Cryptanalysis the process of trying to break cipher text message to obtain the original plain text message itself is called cryptanalysis.
Secrete image- original image of user.
Host- face images use for encryption of secrete image. We have database from which choosing host images.
Sheets- The secret image is encrypted into sheets .
Target- secrete user image is reconstructed.

2. Motivation

- Preserving the privacy of digital biometric data (e.g. face images) stored in a central database has become of paramount importance. This work explores the possibility of using visual cryptography for providing privacy to biometric

*Corresponding author: **Santosh S. Varpe**

data such as fingerprint images, iris codes, and face images.

- The template of a person in the database is generated during enrollment and is often stored along with the original raw data. This has increases need of privacy to protecting the contents of the database.
- In the existing biometric authentication system the image template of a person is stored as such in the authentication server and is prone to security attacks at the server side.

3. Proposed System

In the proposed scheme, a private image is converted into gray scale image for this multiplying red ,green, blue by random numeric values. after that giving name to that gray scale image, then choosing two host image and splitting original image into two host image and encrypting that grayscale image and generating sheets. Encrypting image using key and that key is generated by using math.random() function. Downloading two sheets on user computer and storing other sheets in database. At the time of authentication selecting original secrete image after that selecting downloaded sheets and pressing match button, it will show the other encrypted sheets only if the selected secrete image is right. After that combining all the sheets and match with original secrete image if match then authentication successful.

Algorithm

1. Calculating size of secrete image
2. Split into two host images
3. Convert to grayscale image and encrypt using key.
4. for(int i=0; i<width; i++){
5.
6. for(int j=0; j<height; j++){
7.
8. Color c = new Color(image.getRGB(i, j));
9. int red = (int)(c.getRed() * 0.299);
10. int green = (int)(c.getGreen() * 0.587);
11. int blue = (int)(c.getBlue() *0.114);
12. Color newColor = new Color(red+green+blue,
13.
14. red+green+blue,red+green+blue);
15.
16. image.setRGB(i,j,newColor.getRGB());
17. }
18. }
19. Generating sheets
20. ArrayList sheets=new ArrayList();
21. int targetSum=Math.abs(pixels[k][j]);
22. // System.out.println("\t"+pixels[k][j]);
23.
24. sheets=gs.n_random(targetSum,3);
25.
sheet1[k][j]=Integer.parseInt(sheets.get(0).toString());
26.
sheet2[k][j]=Integer.parseInt(sheets.get(1).toString());
27.
sheet3[k][j]=Integer.parseInt(sheets.get(2).toString());
28. Downloading sheets.
29. Matching original image with reconstructed sheets at time of authentication.

I have convert each grayscale block into a binary block. First of all each pixel value in a grayscale block is transformed into binary representation. For example take a grayscale block and transform into binary blocks.

111 159 20
254 10 198
40 215 100
Its corresponding binary blocks are as follows:

[0 1 1 0 1 1 1 1] [1 0 0 1 1 1 1 1] [0 0 0 1 0 1 0 0];
[1 1 1 1 1 1 1 0] [0 0 0 0 1 0 1 0] [1 1 0 0 0 1 1 0];
[0 0 1 0 1 0 0 0] [1 1 0 1 0 1 1 1] [0 1 1 0 0 1 0 0].

Take each binary block and perform different possible combinations of that number, and trying to design the block into different shares. For example take a grayscale block and divide the block into shares and apply the above scheme.

Four-of-Four Scheme using Grayscale Images

Here I design the shares such a way that when combining any two shares will reveal the original bit information, but not the whole share just half of each single share will give me high quality image when reconstructed. I will explain this scheme by taking a value from the grayscale block and divide that value into shares.

254: [1 1 1 1 1 1 1 0]

Table-1: Grayscale bits are transformed into Binary bits

	1st half	2nd half
Share1:	1 1 1 0 0 1 1 0	1 1 0 1 1 0 1 0
Share2:	0 0 0 1 1 0 0 0	0 1 0 0 0 1 0 0
Share3:	0 0 1 0 1 0 0 0	1 0 1 0 0 1 0 0

Share1 (1st half): 1 1 1 0 0 1 1 0
Share2 (1st half): 0 0 0 1 1 0 0 0

1 1 1 1 1 1 1 0 = 254

Share3 (1st half) : 0 0 1 0 1 0 0 0
Share1 (2nd half): 1 1 0 1 1 0 1 0

1 1 1 1 1 1 1 0 = 254

Combining any two half shares will give me exact bit and doing same procedure for the whole grayscale block gives perfect high quality image when reconstructed without any loss of contrast.

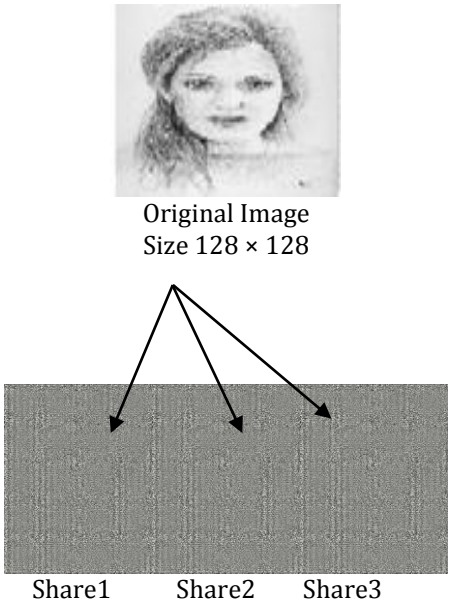

Fig.1: Generating three separate shared transparencies for gray-level visual cryptography.

The beauty of this scheme is, when you combine the direct shares you can't see a perfect gray-scale image only when you combine the all shares, the original quality of the image will be revealed without any loss of quality.

.

4. Activity Diagram

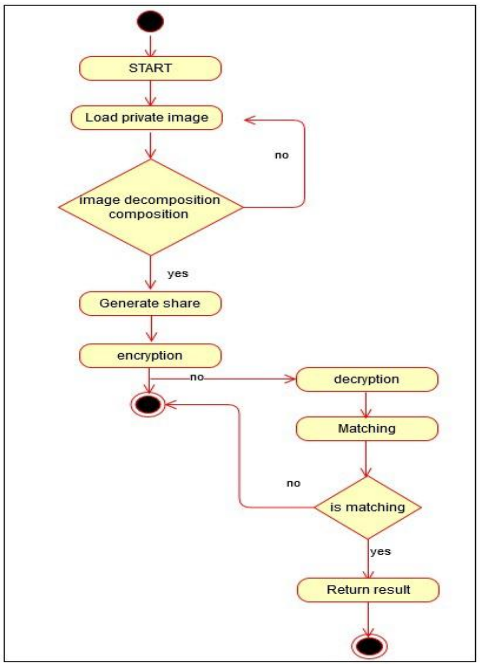

Fig.2: Activity diagram

In this diagram user load the private host image and also load two public image. System convert image into grayscale image and encrypt that image then generate share. At time of authentication user load there private image and two downloaded sheet, the database server automatically load other two sheet. after pressing submit button it match image and sheet using and, return result.

5. Results

VCS Method

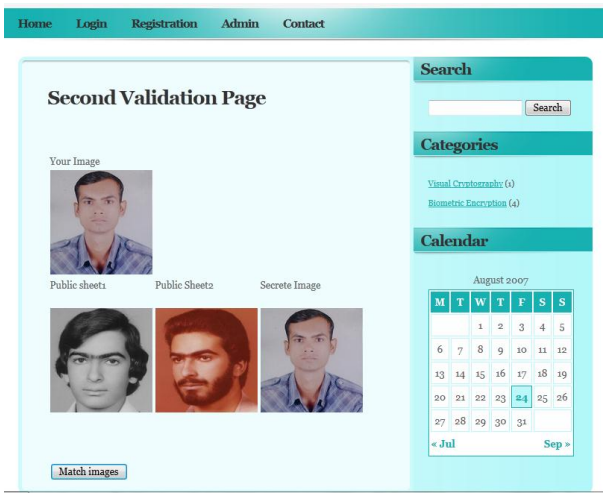

Fig.3: VCS Method

Giving input as user image and using secrete key decrypting the sheet, matching the user image with secrete image if match then authentication successful otherwise authentication fail.

GEVCS Method

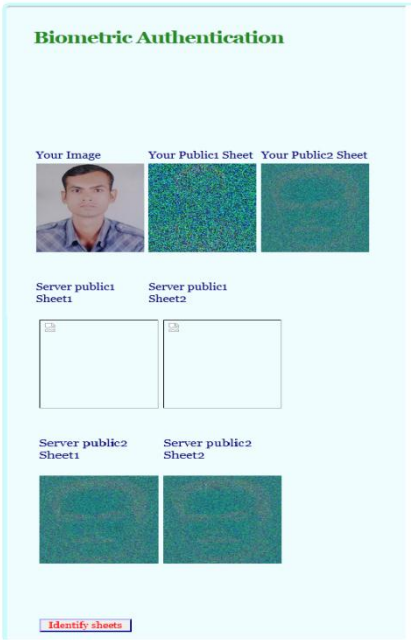

Fig.4: GEVCS Method

Giving user image and two downloaded sheets as input server automatically select other sheets, when all sheets match then authentication successful otherwise authentication fail.

Space Complexity

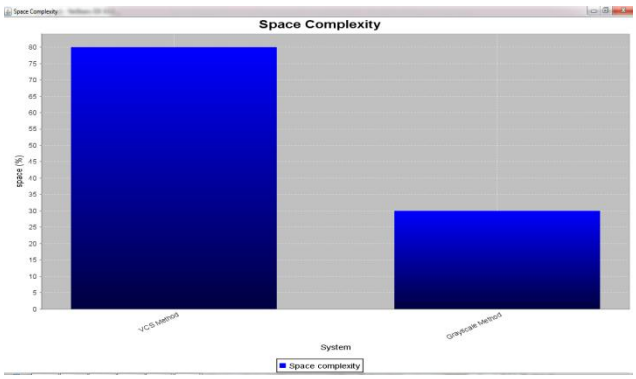

Fig.5: Space Complexity

Our proposed system required less space because we are using code optimization and also scaling the all images at same size.

Time Complexity

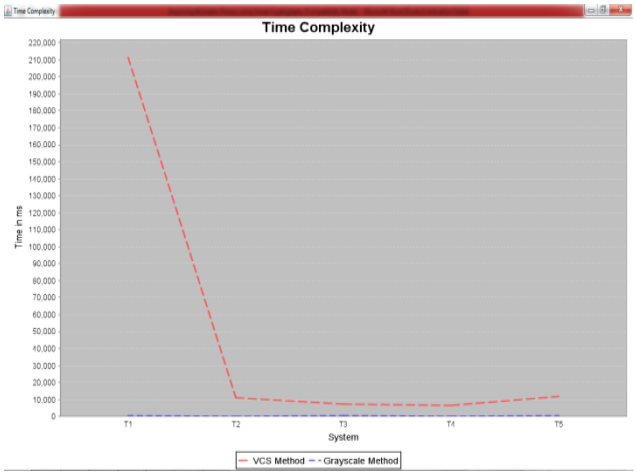

Fig.5: Time Complexity

Our proposed system required the less time than the old system because we are using array for generating sheets. The red dash line shows VCS method and green dash line shows GEVCS method.

Conclusion

This paper proposes a GEVCS scheme to enhance the privacy of biometric data. When all sheets are available then and then the authentication successful otherwise authentication fail.

Acknowledgement

"Feeling gratitude and not expressing it, is like wrapping a present and not giving it". I take this opportunity to express my profound gratitude and deep regards to my guide and truly teacher of teachers **Prof. Prabhudev S. Irabashetti** for her exemplary guidance, monitoring and constant encouragement throughout the course of this project. I also express a deep sense of gratitude **to Prof. Sarika Joshi**, Head of Computer Engineering Department for his valuable guidance and encouragement. I am obliged to our Principal **Dr. A. K. Kureshi** for his inspiration and co-operation.

References

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

Kafri, O and Keren, E.(1987). Encryption of pictures and shapes by random grids. *Optics Letters* 12: 377-379.

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

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.

Author's Profiles

Santosh Varpe received the B.E.(Hons.) degree in Computer Engineering from the S.G. Raisoni COE, Ahmednagar(2012), 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.

Prof. Prabhudev S. Irabashetti working as Asst. Professor in Computer department of Vishwabharati Academy's COE, A.nagar, savitribai phule pune university, Maharashtra, India.