INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at: www.ijariit.com

Bio-metric authentication using non-expanded inverted share image visual cryptography

Ashwini N. Ingle
ingleashwini20@gmail.com
Prof. Ram Meghe Institute of Technology and Research, Amravati, Maharashtra

Dr. G. R. Bamnote
grbamnote@rediffmail.com
Prof. Ram Meghe Institute of Technology and Research, Amravati, Maharashtra

ABSTRACT

A biometric authentication system operates by acquiring raw biometric data from a subject e.g., fingerprint and iris images. This original raw data is stored in the central database. Preserving the privacy of this digital biometric data has become very important. Visual cryptography can be applied to securing this information. The proposed work preserves the privacy fingerprint and iris-based authentication using Inverted Share image Visual Cryptography (ISVC). In ISVC, we invert one share image and stack it with another shared image to obtain the extra confidential data that can be used for authentication. In traditional visual cryptography, the size of the recovered image is expanded because of pixel expansion during encryption. This also leads to recovered image distortion. Therefore, the proposed scheme combines a non-expanded scheme with the extra ability to hide biometric data, such as fingerprint and iris image, in some cover image to maintain privacy. This will also solve the pixel expansion as seen in traditional visual cryptography.

Keywords— *Visual cryptography, Biometric data, Non-Expanded scheme of VC, Extended VC Scheme*

1. INTRODUCTION

Establishing the identity of an individual is very importance in several civilian and government applications such as ATMs, access to nuclear facilities, airport security, issuance of passports or driver licenses, etc. BIOMETRICS-BASED identification technique is a reliable and convenient way for person authentication. It uses physiological or behavioral characteristics of individuals and is becoming increasingly popular compared to traditional token-based or knowledge-based techniques such as Identification Cards (ID), passwords. etc.

For protecting the privacy of an individual enrolled in a biometric database, Davida *et al.* [5] and Ratha *et al.* [6] proposed storing a transformed biometric template instead of the original biometric template in the database. This was referred to as a private template [5] or a cancelable biometric [6]. Feng *et al.* [7] proposed a three-step hybrid approach that combined the advantages of cryptosystems and cancelable biometrics. Apart from these methods, various image hiding approaches [8]–[10] 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.

Visual cryptography (VC), proposed by Naor and Shamir [4], is a method for protecting image-based secrets that has a computation-free decryption process. The basic model of visual cryptography accepts binary image „I‟ as secret image, which is divided into „n‟ number of shares. Each pixel of image „I‟ is represented by „m‟ sub pixels in each of the „n‟ shared images. The resulting structure of each shared image is described by Boolean matrix „S‟
Where S= [Sij] an [n x m] matrix
Sij=1 if the jth sub pixel in the ith share is blackTechnology Research, badnera, India

Sij=0 if the jth sub pixel in the ith share is white

When shares are stacked together secret image can seen but the size is increased by ‘m’ times. Ross and Othmen [1] used (2, 2) visual cryptographic scheme (figure1.) for securing fingerprint and iris images. The biometric image is decomposed into two noise like images called share images. These share images are stored in different databases. During reconstruction phase, these images are fetched and stacked together to get original biometric image process is diagrammatically shown in figure 2.

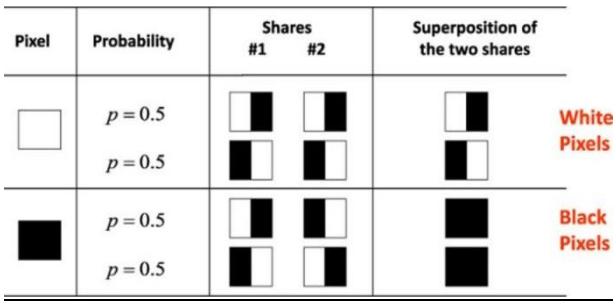


Fig. 1: Illustration of 2- out –of- 2 VCS scheme with 2 sub pixel construction.

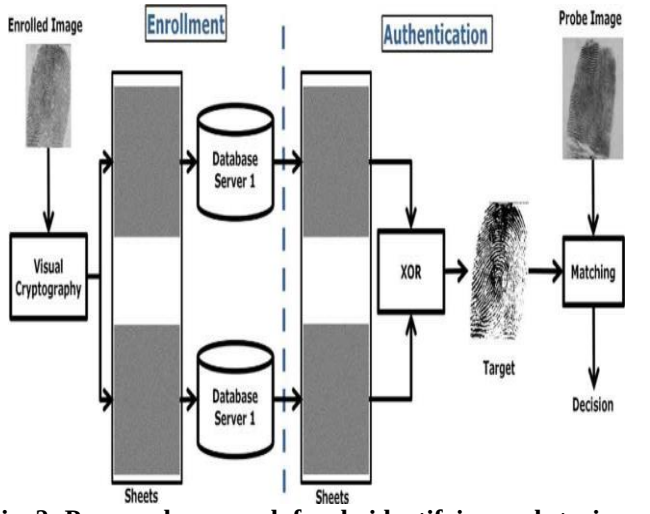


Fig. 2: Proposed approach for de-identifying and storing a fingerprint image

A similar technique is used for iris codes. The characteristic of expansion leads to recovered image distortion. To solve this problem, a novel method of non-expanded scheme with block encoding [3], which encodes a black-and-white image into the same size of share images as the original secret image is proposed. Fang and Lin‟s scheme [11] combine the principle of traditional visual cryptography with authentication characteristic, when we fix the first share image and shift the other share image for certain unit, we can obtain the extra confidential data. But in traditional visual cryptography, secret pixels are expanded to cause the size of the recovered image is larger than the original one. So Haung and Chang [2] combined the non-expanded scheme with the extra ability of hiding confidential data to prevent the detection of information. They divided the secret image into four regions according to sequence to generate region shares. In the generation of region shares phase, they use the block encoding method to generate share blocks in every region. This method include extra log book to generate share image.

There is another visual cryptographic scheme without expansion known as random grid method [12-14]. This paper propose the use of random grid method with ability of hiding the biometric image using Inverted Share Image Scheme. The major properties of the proposed method are security, fast decoding and share image size equal to that of original image. Moreover, this method also does not need extra code book in generating shares.

2. RANDOM GRID ALGORITHM

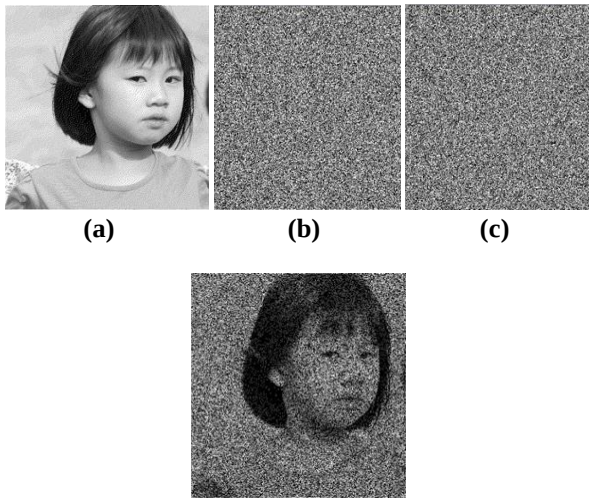
Random Grid Method for visual secret sharing was introduce by Kafri and Keren [12]. They presented three similar algorithms for image encryption by random grids. Precisely, the binary secret image I with the size of h×w will be encrypted into two cipher-grids S1 and S2 with the same size as that of I. Firstly, the cipher-grid S1 is created by randomly assigning each pixel the color 0 or 1, i.e., white and black. Secondly, the other cipher- grid S2 will be created by referring both the secret image I and the cipher grid S1 according to one of Kafri and Kerens three algorithms. Chen and Tsao[14] proposed an extension method that the algorithms mainly consist of three operations: (1) randomization, (2) complement, and (3) equivalence for general operation. This Algorithm is stated below:

2.1 Random Grid Algorithm

Input: Original image I, where I is a halftone image
for(i=0;i<512;i++)
for(j=0;j<512;j++)
Random assign S1[i][j] as white or black
If I[i][j] is white then S2[i][j]=S1[i][j];

Else S2[i][j]=complement of S1[i][j];
End;

The example of random grid method is illustrated in figure 3. Figure 3(a) is the original image. Figure 3(b) & (c) are the share images. Figure 3(d) is the recovered image formed by stacking share images together



(a) (b) (c)

(d)

Fig. 3: An example of Random grid visual cryptography method (a) is original image, (b) and (c) are shares, (d) is the stack result.

3. PROPOSED WORK

In this project the biometric template is protected by hiding it in a cover image using inverted share image visual cryptography. The Random Grid Method is used for avoiding pixel expansion problem. Random grid Method is enhanced for hiding secret image by adding inversion scheme. This method is described below-

Random Grid Method with Inversion*:*
Input: cover image I1 and secret image I2, both are halftone images
Output: sharesS1andS2

Step 1: Assign the pixel values of S1U randoml y.
Step 2: Assign the pixel value of S2U
ifI1[x][y]=whitethen
S2U[x][y]=S1U[x][y].
Else
S2U[x][y]=complement of S1U[x][y].

Step 3: Reverse S2U, that is Temp[x][y]= S2U [image size-x][y].

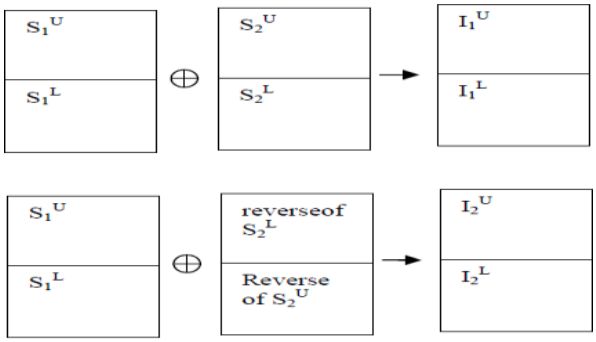
Step 4: Assign the pixel value of S1L.

If I2[x][y]=white, then

S1L[x][y]=temp[x][y].
else
S1L[x][y]=complement of temp[x][y].

Step 5: Assign the pixel value of S2L
if I1[x][y]=white then
S2L[x][y]= S1L[x][y].Else
S2L[x][y]=complement of S1L[x][y].

End;



The cover image, I1, and the secret image (biometric template), I2, are taken as input and the share images S1 and S2 are generated as outputs. The input images are first halftone and divided into two parts as pre-processing step. The share images are also divided into two parts. According to Random Grid Method, the upper part of S1

S1U is taken randomly by assigning the pixel values 0 or 1. The upper part S2U, the lower part S1L, and the lower part S2L are generated by using above algorithm. When S1 and S2 are stacked together, the cover image is obtained. When inverted S2 is stacked together with S1 then secret image (here, the biometric image) is obtained.

4. EXPERIMENTAL RESULTS

In this project, biometric images (fingerprint and iris templates) are secured by hiding them in some cover images using visual cryptographic scheme that is free from pixel expansion problem. This project used UPEK fingerprint database [15] and Michal Dabes and Libar Machala iris database [16].

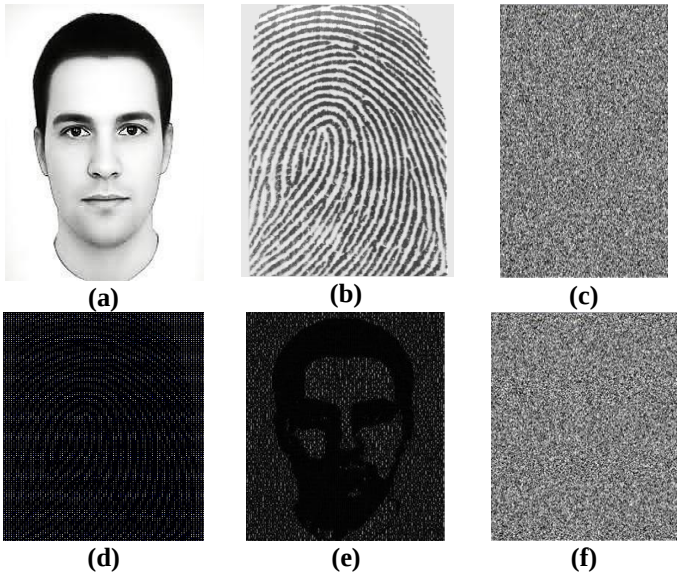


Fig. 4: The experimental results (a) and (b) are original image, (c) and (d) are share image, (e) is the result of stacking (c) and (d), (f) is the result of stacking (c) and inverse of (d).

The Fig.4.shows the experimental results. Figure 4(a) is the cover image in which the fingerprint image (figure 4(b)) is hided. After applying the Random Grid Method with Inversion, the share images (figure 4(c) and (d)) are formed. When share image (c) and (d) are stacked together then the image figure 4 (e) is obtained and when (c) and inverse of (d) are stacked together then the fingerprint is retrived. The same process is applied for iris templates.

The Equal Error Rate (EER) was used to observe the matching performance of the original as well as the reconstructed image. The EER for iris images was ~6.3% and that for fingerprint images was ~8%.Next, the possibility of exposing the identity by using the share images and the original images was investigated. However, this resulted in an EER of 50% suggesting the difficulty in using individual sheets to reveal the original images

5. CONCLUSION

This paper explored the use of Random Grid Method of visual cryptography with inversion for preserving the privacy of biometric image. In this the share images are generated by hiding the biometric image in some cover image and applying visual cryptography. Here, the pixel expansion problem in traditional VC scheme is avoided by generating share image equal to the size of original image.

Thus the distortion resulted by pixel expansion of share image is also avoided. Moreover, there is need of code book in some VC scheme with block encoding .In the proposed scheme this code book is not needed. The difference between traditional visual cryptography and non-expanded Inverted Share Image Visual Cyptography (ISVC) is given in table 1. For future studies, hiding more than one biometric image in single cover image can be explored for enhancing the security factor and also reducing the storage space of share image

Table1.Comparision

Properties	Traditional VC scheme	ISVC scheme (proposed)
Pixel expansion	YES	NO
Secret data hiding	NO	YES
Code book Needed	YES	NO

6. ACKNOWLEDGMENT

The authors are grateful to UPEK and Michal Dabes and Libar Machala for fingerprint and iris databases.

7. REFERENCES

[1] Arun Ross and Asem Othman, "Visual Cryptography for Biometric Privacy", IEEE Transaction on Information Forensic and Security, vol. 6, no. 1, March 2011.

[2] Yi-Jing Huang and Jun-Dong Chang, "Non-expanded Visual Cryptography Scheme with Authentication", IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25-26, 2013.

[3] Y. J. Huang, C.C. Lee, H.C. Wu, J. D. Chang, C.S. Tsai, and Y.T.Tsao, "Novel Non-expanded Visual Cryptography Scheme with Block Encoding" Journal of computers, Vol. 22, No.2, pp. 61-71, 2011

[4] M. Naor and A. Shamir, "Visual cryptography," Advance in Cryptology: Eurpocrypt"94, Lecture Notes In Computer Science, Springer Verlag, Germany, Vol. 950, pp. 1–12, 1995.

[5] 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.

[6] 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.

[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] A. Jain and U. Uludag, "Hiding biometric data," IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 11, pp.

1494–1498, Nov. 2003.

[9] 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.

[10] 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.

[11] W.P. Fang and J.C. Lin, "Visual cryptography with extra ability of hiding confidential data," Journal of Electronic Imaging, Vol. 15, No. 2, pp.0230201–023020 7, 2006.

[12] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Optics Letters, Vol. 12, No. 6, pp. 377 - 379, 1987.

[13] S. J. Shyu, "Image encryption by random grids," Pattern Recognition, Vol. 40, Issue 3, pp. 1014 - 1031, 2007

[14] Tzung-Her Chen and Kai-Hsiang Tsao, "Visual secret sharing by random grids revisited", Pattern Recognition, 2008,online(http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6V14-4V1TXMJ11&_cdi=5664&_user=2414342&_orig=mlkt&_coverDate=11%2F30%2F2008&_sk=999999999&view=c&wchp=dGLzVtzzSkzV&md5=0f9b092b81e841ed86e4a8c6eadd4a22&ie=/sdarticle.pdf)

[15] Fingerprint Database, www.advancesourcecode.com/fingerprintdatabase.asp/,

[16] Iris Database, http://www.inf.upol.cz/iris/, "Michal Dabes and Libar Machala iris database.

