ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3,Special Issue 1,April 2015

An Extended Visual Cryptography Scheme Using Balanced Block Replacement Method

Mr. Shivaraj H.G.

VI Sem Part-time M.Tech, ECE Dept., NMAMIT, Nitte

Abstract: In this paper Visual cryptography scheme is a cryptographic technique which allows the information which is visual such as printed text, handwritten notes and images to be encrypted in such a way that its decryption does not require a computer, it can be done by the human visual system. In extended visual cryptography, the meaningful cover images are added to the share images, which provides an opportunity to integrate visual cryptography and biometric security techniques. In this paper, a method has been proposed by using the extended visual cryptography scheme for processing halftone images that improves the quality of the share images and the recovered secret image for which the size of the share images and the recovered image can be preserved as same as that of the original halftone secret image.

I. INTRODUCTION

Visual cryptography is introduced by first in 1994 Naor and Shamir . Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently.

Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images, 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 of particular interest for security applications based on biometrics [2]. The basic idea of visual cryptography can be illustrated with the traditional 2-out-of-2 scheme. In the (2, 2) scheme, every secret pixel of the image is converted into two share images and recovered by simply stacking two shares together.

This is equivalent to using the OR operation between the shares. In this scheme, 4 subpixels are generated from each pixel of the secret image in a way that 2 subpixels are white and 2 are black.

The subpixels for each share are selected randomly. When a pixel from the original image is white, one of the six possible combination of patterns are randomly selected to encode the pixel into 2 shares. Table 1 demonstrates an example showing a part of Naor and Shamir's encoding process. It is easy to see knowing only one share value does not reveal the other visual cryptography (EVC) schemes that can construct meaningful share images.

The (2,2) EVC scheme proposed in [4] required expansion of one pixel in the original image to 4 subpixels which can then be selected to produce the required images for each

share. It can be shown that the resulting scheme is, in share nor any information of the secret image pixel. However superimposing both shares reveals the corresponding binary secret image.

For example, if a share image could be selected to be the fingerprint of the share holder, this could be useful in authenticating a user's right to hold that share when the parties meet to combine their share images to reveal the secret.

In 1996, Ateniese, Blundo, and Stinson [4] proposed extended fact, also perfectly secure, in that, no share image leaks any information of the original secret image. Figure 2 illustrates a (2,2) scheme containing the original binary secret image, "Engineering", with two cover images, "Memorial" and "University", embedded into the shares.

By using the halftoning algorithm[3] we can convert the grayscale images to binary images ,as the visual cryptography works on binary images. Therefore biometric images can be easily used for visual cryptography scheme as they are grayscale images.

Using halftoning techniques is a useful pre-processing step for visual cryptography. By applying halftoning technique for grayscale images there is a degradation in the quality of the image and hence there is a reduction in the visual cryptography scheme.

The objective of the research outlined in this paper is to derive a secure (2; 2) extended visual cryptography preserves a good quality image for both the shares and the recovered image. Our proposed scheme maintains the perfect security of the basic EVC scheme [4].

DOI 10.17148/IJIREEICE

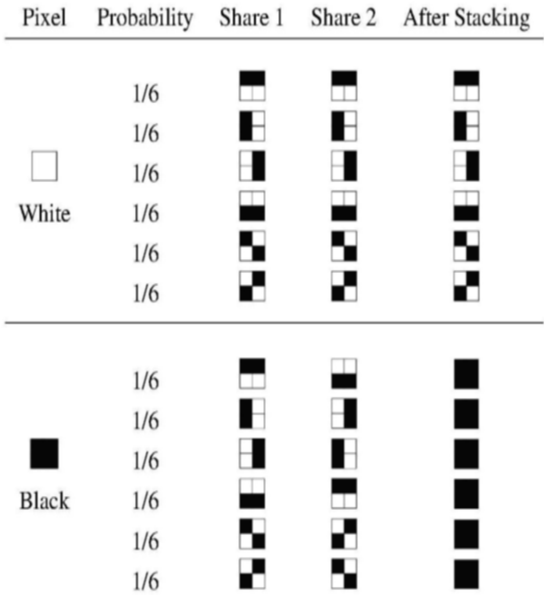
Pixel
Probability
Share 1
Share 2
After Stacking
White
1/6
1/6
1/6
1/6
1/6
1/6
Black
1/6
1/6
1/6
1/6
1/6
1/6

Table 1. Illustration of a (2; 2) VC Scheme with 4 subpixels

II. PRE-PROCESSING OF HALFTONE IMAGES

Grayscale images are converted into binary images by using the halftoning algorithm. After the creation of halftone image simple method can be used in order to preserve the image size when applying visual cryptography and extended visual cryptography. For example, a basic, secure method that is easy to implement is based on a block-wise approach to pre-processing the binary halftone image prior to applying visual cryptography . In this paper, we refer to this basic approach as simple block replacement (SBR)[1].The group of four pixels is taken in the SBR scheme from the halftone secret image in one 2*2 block, referred as a secret block. In this shares are generated block by block instead of pixel by pixel.

Each secret block with four pixels encodes into two secret shares each containing four pixels. So that after stacking the two shares together the size of the reconstructed image is same as the original secret image. Before applying visual cryptography encoding all the secret blocks in an image need to be processed. Each secret block is replaced by the corresponding predetermined candidate, which is a block with 4 white pixels (a white block) or a block with 4 black pixels (a black block).

Based on a number of black and white pixels in each secret block, the block replacement process in the SBR pre-processing scheme is used. If the number of black pixels in a secret block is larger than or equal to 2, the secret block converts to a black block. If the number of black pixels in a secret block is less than or equal to 1, it is converted to a white block. The processed secret image can be obtained from this step. This processed image can be used as a secret image in visual cryptography schemes such as traditional VC or EVC. High variability in the distribution of black and white pixels for halftone images within each secret block, the resulting processed secret image is generally poor being darker than the original image, causing the loss of many fine details in the image.

III. AN IMPROVED PRE-PROCESSING SCHEME

An improved Balanced Block Replacement(BBR) method is used in order to replace the candidate blocks of the halftone-secret image. This approach is used to obtain the better balance in the black and white pixels in the processed secret image by performing the block replacement. The SBR scheme since blocks which contain two black and two white pixels are converted to a black block, the scheme results in darker images.

A block with two white and two black pixels are referred to as candidate blocks. In the BBR approach, some candidate blocks are assigned to black and others to white in order to balance white and black in the processed image. Assigning the candidate block randomly to black and white improves the visual quality of the processed secret image, even better visual results can be achieved using an intelligent block replacement approach that considers the characteristics of the original image in determining whether a candidate block should be assigned to black or white.

This method tries to keep the local ratio of black to white pixels in the processed image close to the local ratio of black to white pixels in the original halftone secret image. Therefore, the resulting recovered image is closer in quality to the original grayscale image.

IV. GENERAL DESCRIPTION OF THE SCHEME

There are three main steps involved in the preparation of the grayscale images for use in the visual cryptography. The first step is the conversion of grayscale images to a halftone images. The halftone image is partitioned into non-overlapping blocks of 2*2 pixels. Each grouping of 4 blocks is referred to as a cluster. In the second step threshold value of the cluster is calculated by counting the number of black pixels in the each cluster. This value is stored in the template.

The secret block containing 1 black pixel is classified in this step. The secret block containing 1 black pixel is converted into white block. The image obtained from this step referred to as the initial processed image. The third step starts from the first block in the top left of the first cluster of the initial processed image.

In each block processing of the cluster is done from left to right and then from top to bottom in raster format. The number of black pixels in the cluster is counted when the first candidate.

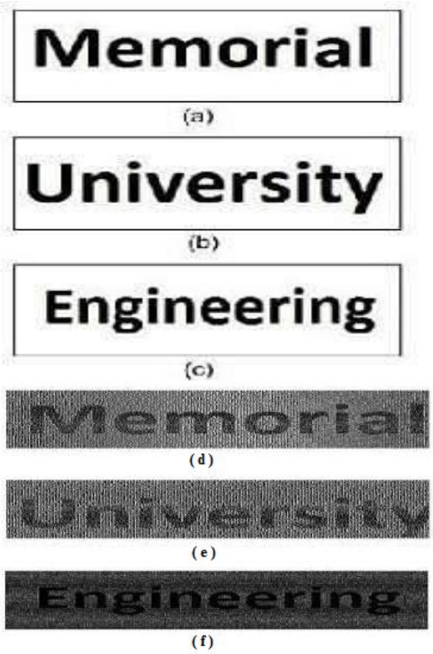

Fig. 1. Example of (2; 2) EVC Scheme: (a) first cover image;(b) second cover image; (c) secret image; (d) share 1; (e) share 2; (f) recovered secret image

block is identified. In this we are trying to keep the number of black and white pixels of the initial processed image as close as to the threshold value of the original halftone image. Therefore while changing the candidate block to white or black pixels, the number of black pixels are computed and it is compared with the threshold value of the original halftone images. If the corresponding candidate block converts to a black block, 2 pixels will be added to the number of black pixels in a cluster and if the candidate block turns to white block, 2 black pixels will be deducted from the cluster. The conversion is based on the smallest difference between the threshold and the number of black pixels in the image being processed. If changing the candidate block to black makes this difference smaller, the candidate block is converted to a black block. Similarly, if turning the candidate block to white makes this difference smaller, the block converts to a white block. In the case that turning the candidate to black or white produces the same difference, the block randomly converts to either a black or white block.

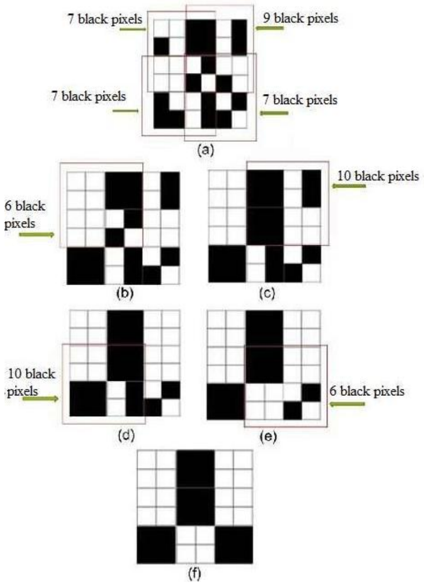

Fig. 2. Example of the BBR Method

In BBR algorithm, the halftone image is divided into 4 overlapping clusters each containing 4 secret blocks. the number of black pixels for each cluster is computed and saved in a template. The block with 0,1,3 black or white pixels are converted, leaving behind only the candidate blocks and the blocks with 4 black pixels or 4 white pixels to be processed. Figure 2(b) illustrates the first cluster in an initial image; this cluster contains 1 candidate block and 6 black pixels. According to the algorithm, the threshold value is 7 for this cluster and we want to replace the candidate block in a way that the number of black pixels in the cluster will be very close to 7. It is obvious that if we change the block to a black block, the number of black pixels will be 8 and if we turn it to a white block, the number of black pixels in this cluster will reduce to 4. Therefore, the block will be replaced with a black block. This procedure is repeated for the next 3 clusters and the final processed image is shown in Figure 2(f).

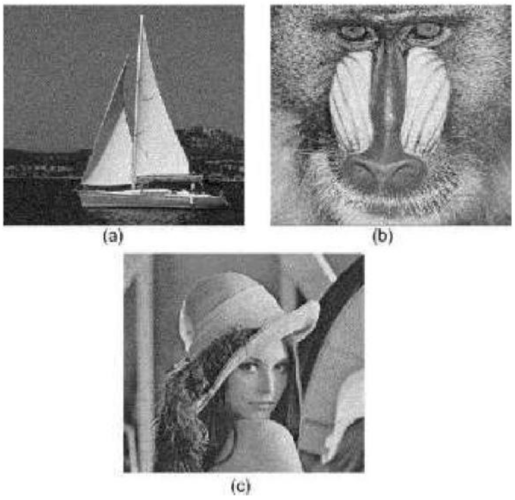

Fig. 3. Images Used for EVC Scheme: (a) halftone boat; (b) halftone baboon; (c) halftone Lena

V. APPLICATION TO EXTENDED VC

A meaningful cover images are added in each share in the extended VC scheme. The image expansion becomes necessary in order to preserve the secret information present in the original halftone image into the reconstructed image. By using the basic pre-processing scheme SBR and advanced BBR method, the share and the recovered image will have the three halftone images as inputs. In this first two images are considered as meaningful cover images and the third image is the secret image. The processed images are generated for all the three images by using one of the block replacement method which contains only black and white pixels. After the creation of processed image, the two share images are created by using EVC encoding scheme[4]. The secret image is recovered by stacking the two shares together by using non-expansion EVC[4]. Figure 4 shows the results of using the SBR pre-processing method in an EVC scheme. As expected, the shares and the recovered secret image have the same size as the original halftoned images; however, compared with the original halftone images, the shares and the recovered image have a visual quality that is very poor with a severe darkening effect.

Figure 5 demonstrates the effect of using the BBR method in the EVC scheme. A significant improvement can be observed in the visual quality of the two shares and reconstructed image in comparison to the SBR method. For example, in the recovered secret image, Lena, improved detail in the hair is clearly visible in Figure 5(d) versus Figure 4(d). As well, in the shares using the boat as a cover image, greater distinguishing between background detail is clearly visible in the BBR result of Figure 5(e), in comparison to the result for SBR of Figure 4(e). Similarly, the share image of the baboon shows improved clarity around the eyes for the BBR result versus the SBR result.

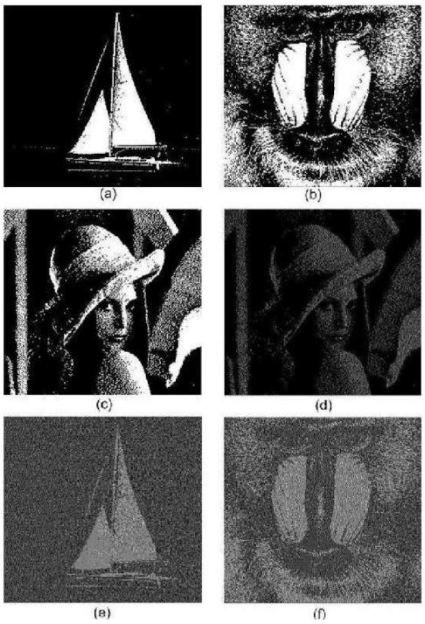

Fig. 4. Experimental Results of SBR Method Applied to EVC: (a) processed boat; (b) processed baboon; (c) processed Lena; (d) reconstructed Lena; (e) first cover image;(f) second cover image

VI. CONCLUSION

In this paper, an extended visual cryptography scheme is used for the non expansion of the images. It can also be used in the application such as multiple image visual cryptography in which multiple images can be hided in the shares. The intelligent pre-processing scheme we can obtain good quality of the image and the shares. It uses all the three input images of same size, the improvement can be done by taking the inputs of different sizes.

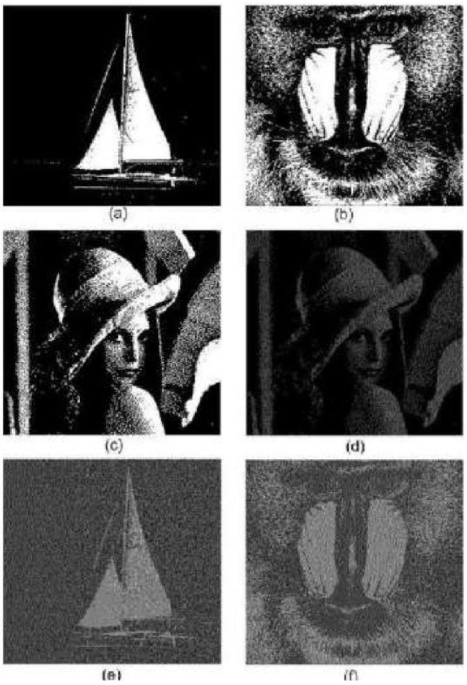

Fig. 5: Experimental Results of EVC with BBR Method Applied to EVC: (a) processed boat; (b) processed baboon; (c) processed Lena; (d) reconstructed Lena; (e) first cover image;(f) second cover image

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography",in EUROCRYPT '94 Proceedings, Lecture Notes in Computer Science, Springer-Verlag, vol. 950, pp. 1-12, 1995.

[2] M. Naor and A. Shamir, "Visual cryptography", in EUROCRYPT'94 Proceedings, Lecture Notes in Computer Science, Springer-Verlag, vol. 950, pp. 1-12, 1995.

[3] R. W. Floyd and L. Steinberg, "An Adaptive Algorithm for Spatial Gray Scale", in Proceedings of the Society for Information Display, vol.17, no. 2, pp.75-77, 1976.

[4] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, "Extended Capabilities for Visual Cryptography", Theoretical Computer Science, vol. 250, pp. 143-161, 2001.

[5] Z. Zhou, G.R. Arce, and G. Di Crescenzo, "Halftone Visual Cryptography", IEEE Transactions on Image Processing,vol. 15, no. 8, pp. 2441-2451, 2006.

[6] M. Nakajima and Y. Yamaguchi, Extended Visual Cryptography for Natural Images, in Proceeedings of WSCG, pp. 303-310, 2002.

[7] C.L. Chou,"A Watermarking Technique Based on Nonexpansible Visual Cryptography", Thesis, Department of Information Management, National University, Taiwan, 2002.
[8] C.C. Wu and L.H. Chen, "A Study on Visual Cryptography", Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, 1998.

DOI 10.17148/IJIREEICE