PERFORMANCE EVALUATION OF A VISUAL CRYPTOGRAPHY USING HALFTONE IMAGES

[1]Ms. Simpy Gurditta, [2]Mrs.Silvi Thakral

[1] Student, [2]Faculty, Department of Computer Science and Engineering,

MITM, Jevra, Hisar (India)

ABSTRACT

Visual Cryptography is a secret sharing scheme which uses images distributed as shares such that, when the shares are superimposed, a hidden secret image is revealed. In extended visual cryptography, the shares images are constructed to contain meaningful cover images, thereby providing opportunities for integrating visual cryptography and biometric security techniques. In this paper, we propose a method for processing halftone images that improves the quality of the shares images and the recovered secret image in an extended visual cryptography scheme for which size of the shares images and the recovered image is the same as for the original halftone secret image. The resulting scheme maintains the perfect security of the original extended visual crypto grapy approach.

Keywords: Cryptography, Image Processing, Visual Cryptography, Secret Sharing.

I. INTRODUCTION

Visual Crypto grapy (VC), first proposed in 1994 by Nair and Shamir [1],is a secret sharing scheme, based on black-and-white or binary image. Secret image are divided into sharing images which on their own, reveal no information of the original secret. Shares may be distributed to various parties so that only by collaborating with an appropriate number of other parties, can the resulting combined shares reveal the secret image. Recovery of the secret can be done by superimposing the share images and hence, the decoding process requires no special hardware or software and can be simply done by the human eye. Visual cryptography is of particular interest for security applications based on biometrics [2]. For example, biometric information in the form of facial, fingerprint and signature images can be kept secret by portioning into shares, which can be distributed for safety to a number of parties. The secret image can then recovered when all parties release their share images which are then recombined. A basic 2-out-of-2 or (2, 2) visual cryptography scheme produces 2 share images from an original image and must Stack both shares to reproduce the original image. More, generally a (k,n) scheme produces n shares, but only requires combine k shares to recover the secret image. To preserve the aspect ratio for the recovered secret image for a (2, 2) scheme each pixel in the original image can be replace din the shareimagesbya2×2blockofsub pixels.

Table 1. Illustration of A (2, 2) VC Scheme with 4 Sub Pixels

As shown inTable1, if the original pixel is white, one of six combinations of share pixels is randomly created. Similarly, the possible share combination for black pixels is also shown .After stacking the shares with white transparent and black opaque, the original secret image will be revealed. Stacking can be viewed as mathematically O-ring, where white is equivalent to"0"and black is equivalent to "1".The process is illustrated in Figure 1 for a simple binary image. Note that the resulting share images and the recovered secret image contain 4 times more pixels than the original image (since each pixel of the original image was mapped to four sub pixels) [3].It may also be noted that the recovered image has a degradation in visual quality (specifically, the contrast between white and black is decreased) since are covered white pixel is actually comprised of 2 white and 2 black sub pixels, while a black pixel is represented by 4 black sub pixel sin the recovered image.
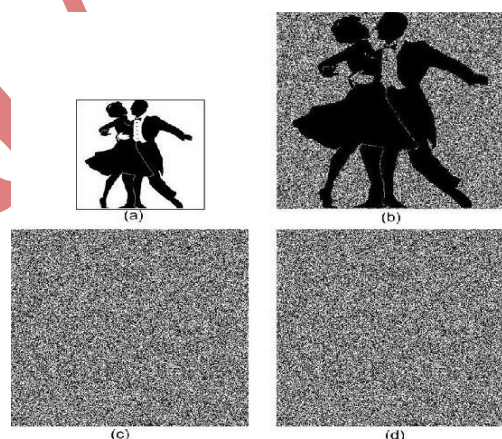

Fig 1 Example Of A (2,2) VC Scheme With 4 Sub Pixels.(A) Secret Dancers Image,(B) Reconstructed Dancers Image,(C)First Share, (D) Second Share

It is also obvious that, while the shares appear to be random (and , in fact, can be shown to contain no informational content that can be used to recover the original secret image on their own), the shares also have no interesting content that could be used to carry other information (such as biometric image) that might be helpful in a security context. For example, if a share image could be selected to be the fingerprint of the share folder, this could be useful in authenticating a user's right to hold that share when the parties meet to combine their share image to reveal the secret. In 1996, Ateniese Blonde and Stinson [4] proposed extended 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 pixels which can then be selected to produce the required images for each share. It can be shown that the resulting scheme is, in fact, also perfectly secure, and in that, no share image leaks any information of the original secret image. Fig 2 illustrates a (2,2) scheme containing the original binary secret image, "Engineering" with two cover image " Memorial" and "University" embedded into the shares.

Although visual crypto grapy operates on binary images. It can be applied to grayscale images by using a half toning algorithm to first convert the grayscale image to a binary image [5]. This allows for use of visual cryptography scheme to biometric images which are naturally and meaningfully grayscale such as facial images. Hence, using half toning techniques to convert grayscale images to binary images is a useful preprocessing step for visual cryptography .However the half toning process applied to a grayscale image results in a reduction of the image quality and since visual cryptography scheme also results in a reduction in image quality mitigating image degradation becomes an important objective in a visual cryptography. Previous schemes in targeting half tuning and visual crypto grapy have suffered from issues such as image expansion (that is, requiring significantly more pixels for the shares and/or recovered secret image) [6]and compromise of the security of the scheme [7].
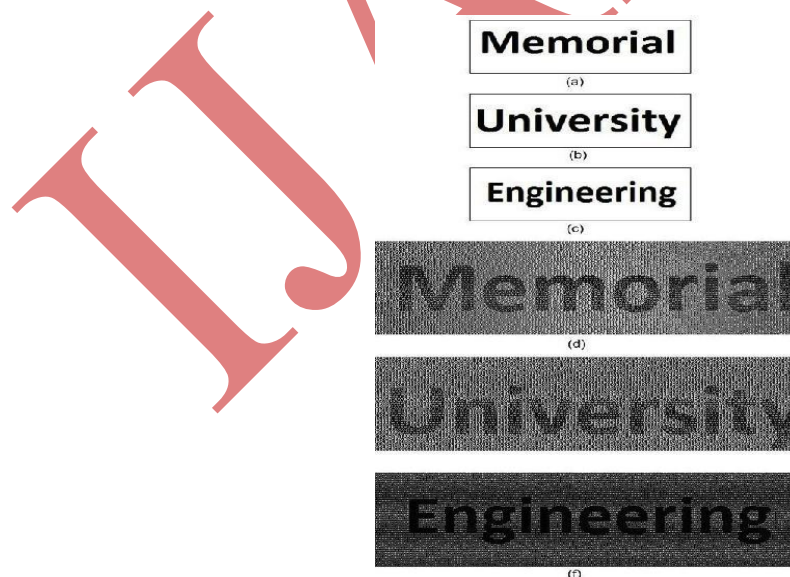

Fig 2. Example Of (2,2) EVC Scheme (A) First Cover Image,(B) Second Cover Image,(C) Secret Image,(D) Share 1,(E)Share2,(F) Recovered Secret Image

The objective of their search out lined in this paper is to derive a secure (2,2)extended visual crypto grapy scheme, which does not require more pixels in the shares and recovered image than the original secret image and yet preserves good quality image for both the shares and the recovered image. Our proposed scheme maintains the perfect security of the basic EVC scheme [4].

II. PREPOSING HALFTONE IMAGES

In this section, we consider the application of visual crypto grapy to gray scale images by first converting the images to a binary image using a half toning algorithm. After creating a half tone image, in order to preserve the image size when applying visual crypto grapy and extended visual cryptography, simple method scan be applied. For example, a basic, secure method that is easy to implement is based on a block-wise approach to pre-processing the binary half tone image prior to applying visual crypto grapy [8]. In this paper, were far to this basic approach as simple block replacement (SBR).The SBR scheme considers groups of four pixels from the half tone secret image in one2×2 block, referred and block and generates the shares block by block (rather than pixel by pixel).As each secret block with four pixels encodes in to two secret shares each containing four pixels, the size of there - constructed image is the same as the original secret image after stacking the two shares together. In this technique, all the secret blocks in an image need to be processed before visual cryptography encoding and 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).

The block replacement process in the SBR pre-processing scheme is based on a number of black and white pixels in each secret block. 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 equalto1, it is converted to a white block. This step produces a new secret image which contains only white and black blocks. The image obtained from this step is referred to as a *processed* secret image. The processed image is now ready to be used as a secret image in visual crypto grapy scheme and secret additional VC or EVC.

The SBR approach is straight forward and is very effective for unprocessed binary secret images which have large numbers of all white and all black blocks. However, for halftone images, with high variability in the distribution of black and white pixels within each secret block, the resulting processed secret image is generally poor, being darker than the original image, with poor contrast, causing the loss of many fine detail sin the images. In our experiments applied to EVC, we shall see these effects in Figure5.

III. AN IMPROVED PRE-PROCESSING SCHEME

We now present a novel and effective method for replacing the candidate blocks of a half tone secret image, which we refer to as the balanced block replacement (BBR) method. The novel as pectin is approach is to perform the block replacement such that there is a better balance of white and black in the processed secret image. The previously described SBR scheme results in darker images, since blocks which contain two white and two black pixels are converted to a black block. We shall refer to blocks of two white and two black pixels

as candidate blocks. In the BBR approach, we balance white and black in the processed image by assigning some candidate blocks to black and others to white. Although we have discovered that doing the candidate block assignment randomly to black or white improves the visual quality of the processed secret image, even better visual results can be achieve during an intelligent block replacement approach that considers the characteristic so the original image in determining whether a candidate block should be assigned to black or white. The block replacement approach proposed here 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 half tone secret image. Therefore, the resulting recovered image is closer in quality to the original gray scale image.

3.1   General Description of Scheme

The preparation of a gray scale image for use in visual crypto grapy in voles 3 steps. The first step is the transformation of a gray scale image into a half tone image and portioning the half tone image in to non-over lapping blocks of 2×2pixels. Then, the half tone image is divided into a number of over lapping squares of four 2×2 blocks. Each grouping of 4 blocks is referred to as a cluster. In the second step, the number of black pixels in each cluster from the half tone image are counted and saved in a template. This number is the threes hold value for that cluster. The step then classifies all the secret blocks containing 1 black (resp. white) pixel. If the secret block contains1black (resp. white) pixel, it is converted to a white (resp. black) block. The image obtained from this step is 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. The processing of the blocks in each cluster starts from the top left block, and then moves from left to right and top to bottom in raster for- mat. When the first candidate block in a cluster is identified, the numbers of black pixels in the cluster are counted. The idea is to keep the number of black and white pixels in each cluster of the initial processed image as close as possible to the corresponding threshold value from the cluster of the original half tone image. Therefore the number of black pixels in the case of changing the candidate block to a black or white block is computed and is compared to the threshold value that was derived for the same cluster in the original half tone image. 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 a cluster. The conversion is based on the smallest difference between the thres hold and the number of black pixels in the image being processed. If changing the candidate blocks to black makes this difference smaller, the candidate block is converted to a black block. Similarly, if turning 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.
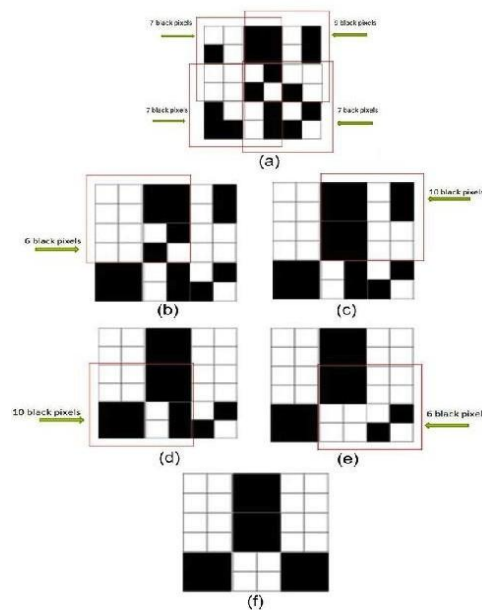
Fig 3.Example of the BBR Method

3.2 An Example of the Scheme

Figure3 is an example of how the proposed algorithm works. A half tone image of size 6×6 is assumed to be an original halftone image in this example. According to the BBR algorithm, the halftone image is divided into 4 over lapping cluster search containing 4 secret blocks.As shown in Figure 3(a), the number of black pixels for each cluster is computed and saved in a template. Subsequently, blockswith0, 1,3, or 4 black pixels are converted, leaving only black, white, or candidate blocks to be processed. Figure3 (b) is the resulting initial processed image. Next, the algorithm starts with partition in the initial processed image in to over lapping clusters.
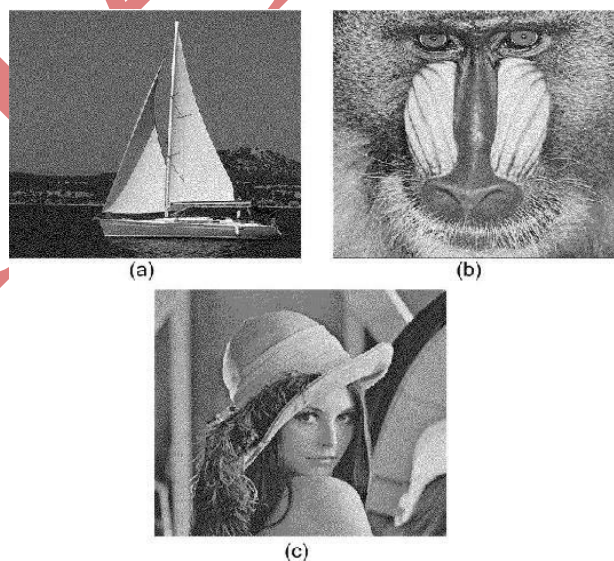

Fig 4, Images Used For EVC Scheme (A) Halftone Boat,(B) Halftone Baboon,(C) Halftone Leena

Figure3 (b) illustrates the first cluster in an initial image; this clustercontains1candidate block and 6 black pixels. According to the algorithm, the thres hold value is 7 forth is 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 3clustersandthefinal processed image is shown in Figure 4

IV. APPLICATION TO EXTENDED VC

As previously noted, an extended VC scheme adds a meaningful cover image in each share. Although image expansion is necessary to exactly preserve the information from the pixels of the original secret image in the recovered secret image, we can use either the basic preprocessing scheme, SBR of section 2 or the more advanced BBR method of section3 to ensure that the share and recovered image use the same number of pixels as the original halftone secret image. Of course, the trade off in such an approach is a decline in image quality. In this section, we examine the application of the preprocessing schemes to construct a (2, 2) EVC scheme without image size expansion. In doing so, we take three halftone images as inputs. The first two image are considered to be meaningful cover images and third image is the secret image. One of the block replacement algorithms converts the three input images into the processed images. A processed image contains white and black block sand can be used as an input secret image in any visual cryptography encoding process. After producing the three processed images by appropriate method. The two shares are generated according to the EVC encoding process specified in [4]. The secret image is recovered by stacking the two shares together. It should be noted that our non-expansion EVC scheme is as secure as the scheme introduced in [4]. As the new scheme does not change the share generation approach.

In order to check the validity of the proposed scheme and also evaluate the effects of the block replacement algorithms on the visual quality of the cover images and the recovered image, we have conducted a visual experiment. As depicted in Figure4,the half tone boat and the half tone baboon, both of size 512×512, are consider red to be two cover images and halftone Lena with the same size as the cover images is assumed to be a secret image. These halftone images are created from the original gray scale images using the Floyd-Steinberg half toning technique [5].

Figure5 shows the results of using the SBR pre-processing method in an EVC scheme. As expected, the and there covered secret image have the same size as the original halftone 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 6 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 Figure6 (d) versus Figure5 (d). As well, distinguishing between background detail is clearly visible in the BBR result of

Figure6(e),in comparison to the result for SBR of Figure5(e).Similarly, the share image of the baboon shows improved clarity around the eyes for the BBR result versus the SBR result.
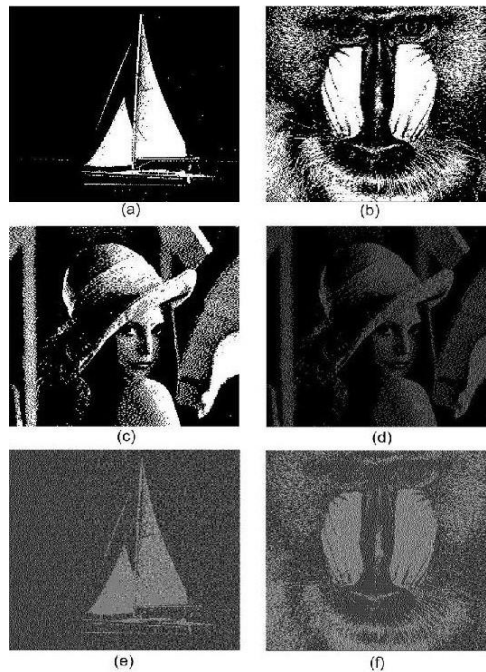

Fig 5 Experimental Results Of SBR Method Applied To EVC: (A) Processed Boat, (B)Processed Baboon,(C) Processed Lena,(D) Reconstructed Lena,(E) First Cover Image,(F) Second Cover Image.
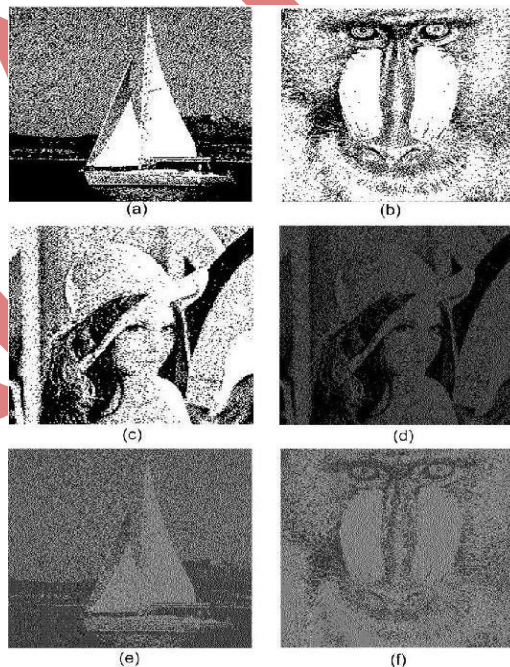

Fig 6: Experimental Results Of EVC With BBR Method Applied To EVC(A) Processed Boat,(B)Processed Baboon,(C) Processed Lena,(D) Reconstructed Lena,(E) First Cover Image,(F) Second Cover Image

V. CONCLUSION

In this paper, we have explored extended visual cryptography without expansion. We have shown that using an intelligent preprocessing of halftone images based on the characteristics of the original secret image, we are unable to produce good quality images in the shares and the recovered image. Note that other applications can also benefit from the preprocessing approach, such as multiple image visual cryptography which hides multiple images in shares [9].

REFERENCES

[1] M. Naor and A. Shamir, "Visual crypto grapy", in EU- ROCRYPT'94Proceedings, Lecture Notesin Computer Science, Springer-Verlag, vol.950, pp. 1-12,1995.

[2] A. Ross and A.A. Othman, "Visual Crypto grapy for Biometric Privacy" IEEE Transactions on Information Forensic sand Security, vol.6, no. 1, pp. 70-81,2011.

[3] N. Askari, C. Moloney and H.M. Heys, "A Novel Visual Secret Sharing Scheme Without Image Size Expansion", IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Montreal, pp.1-4,2012.

[4] G. Ateniese, C. Blundo, A. De Santisand D.R. Stinson, "Extended Capabilities for Visual Crypto grapy", theoretical Computer Science, vol.250, pp.143-161,2001.

[5] R.W. Floyd and L. Steinberg ,"An Adaptive Algorithm for Gray Scale .In proceeding of the society for information Display, vol.17, no.2 pp 75-77, 1976.

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

[7] M. Nakajima and Y. Yamaguchi, Extended Visual Crypto grapy for Natural Images, in Proceedings of WSCG, pp. 303-310, 2002.

[8] C.L. Chou, "A Watermarking Technique Based on Non- expansible Visual Cryptography", Thesis, Department of Information Management, National University, Tai- wan, 2002.

[9] C.C. Wu and L. H. Chen, "A Study on Visual Crypto grapy", Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan,1998