Improving Image Quality In Extended Visual Cryptography For Halftone Images With No Pixel Expansion

J. Tamilarasi, V. Vanitha, T. Renuka

Abstract: Visual cryptography is a secret sharing scheme that divides secret images into shares such that, when the shares are superimposed, a hidden secret image is revealed. In extended visual cryptography, an extra security is provided by giving cover images to the shares. However, in either case, loss of resolution, contrast, and image size expansion are challenging problems that the researchers are facing. In this paper, we propose a method for processing halftone images that improves the quality of the recovered images and also avoids pixel expansion. The resulting scheme maintains the perfect security of the original extended visual cryptography approach and also provides a better result.

Index Terms: extended visual cryptography, image processing, improving image quality, secret sharing, visual cryptography

1 Introduction

With the increasing usage of networks, providing security to the confidential information is a challenging job as the hackers are increasing in numbers nowadays. To deal with the security problems, various secret sharing schemes have been developed. One such secret scheme is extended visual cryptography. It is the way for combining visual cryptography and stenography. This extended visual cryptography (EVC) can be applied for the images as well as the text in the image format. The main application of this scheme is to keep the biometric images safe and secret.

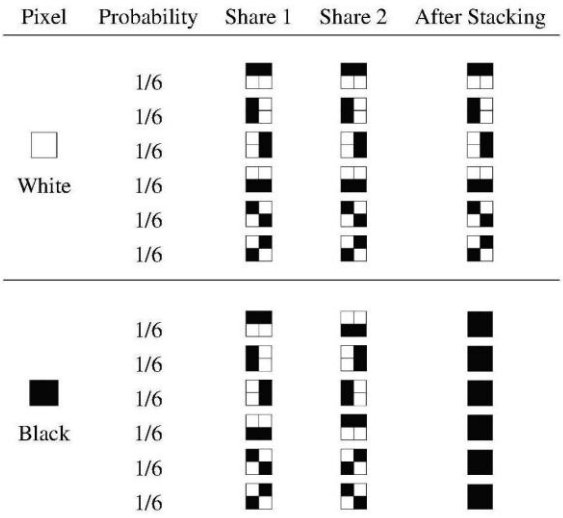
1.1 Visual Cryptography

Visual cryptography (VC), first proposed in 1994 by Naor and Shamir [1], is a secret sharing scheme, based on black-and-white or binary images. Secret images are divided into share 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 super-imposing 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 (VC) is of particular interest for security applications based on biometrics [2].

- *J. Tamilarasi is currently pursuing Bachelor degree program in Information Technology in V.S.B. Engineering college, Karur, India, PH-+91-7373412716.: tamilajayaraj@gmail.com*
- *V. Vanitha is currently pursuing Bachelor degree program in Information Technology in V.S.B. Engineering college, Karur, India, PH-+91-9698645220.: vanithavsbit@gmail.com*
- *T. Renuka is currently pursuing Bachelor degree program in Information Technology in V.S.B. Engineering college, Karur, India, PH-+91-9894041613.: renukathiyakarajan@gmail.com*

For example, biometric information in the form of facial, finger-print and signature images can be kept secret by partitioning 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.

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



A basic 2-out-of-2 or (2; 2) visual cryptography scheme produces 2 share images from an original image and shares must be stacked to reproduce the original image. More generally, a (k; n) scheme produces n shares, but only requires combining 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 replaced in the share images by a 2 2 block of sub pixels. As shown in Table 1, 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 ORing, 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 degradation in visual quality (the contrast between white and black image is decreased) since a recovered pixel is a combination of 2 white sub pixels and 2 black sub pixels.

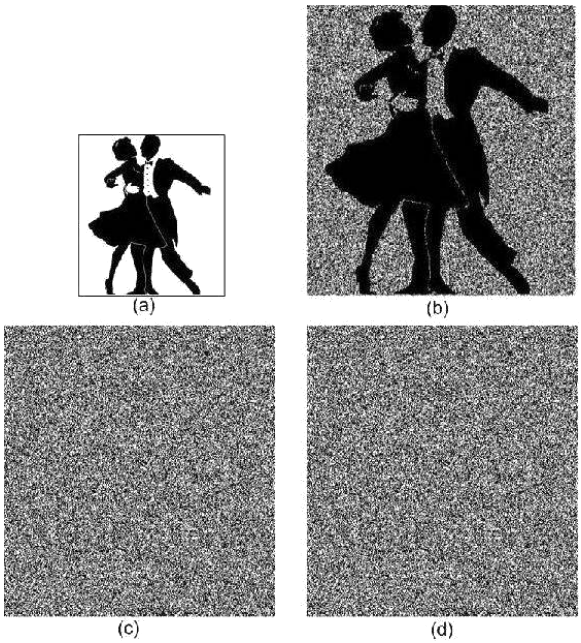


Fig. 1. Example of a (2; 2) VC Scheme with 4 Subpixels: (a) secret Dancers image; (b) reconstructed Dancers image; (c) first share; (d) second share

1.2 Extended Visual Cryptography

In visual cryptography, 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 a biometric image) that might be helpful in a security context. For example, if a share image could be selected to be the finger-print 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 visual cryptography (EVC) schemes that can construct meaningful share images. More security is provided for the shares as a cover image is provided for it. For example, if one of the shares of a finger print is covered by another person's finger print then the outsiders may think that the covered share is the original secret image of the finger print.

2 Previous Work

The associated secret sharing problem and its physical properties such as pixel expansion, image quality, and contrast were studied by various research scholars and many solutions and schemes had been proposed. The (2; 2) EVC scheme is proposed in [4] and it required expansion of one pixel in the original image to 4 sub-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. Although visual cryptography operates on binary images, it can be applied to grayscale images by using a halftoning algorithm to first convert the grayscale image to a binary image. The halftoning algorithm is proposed in [5]. This allows use of visual cryptography schemes to biometric images which are naturally and meaningfully grayscale, such as facial images. Hence, using halftoning techniques to convert grayscale images to binary images is a useful pre-processing step for visual cryptography. The security of the basic EVC scheme is proposed in [4] and in [7]. The halftoning process applied to a grayscale image results in a reduction of the image quality and since visual cryptography schemes also result in a reduction in image quality, mitigating image degradation becomes an important objective in a visual cryptography scheme. Scheme used in [6] integrating halftoning and visual cryptography have suffered from issues such as image expansion (that is, requiring significantly more pixels for the shares and/or recovered secret image) and compromise of the security of the scheme [7]. A secure (2; 2) extended visual cryptography scheme, which does not require more pixels in the shares and recovered image than the original secret image and yet preserves a good quality image for both the shares and the recovered image is proposed in [10].

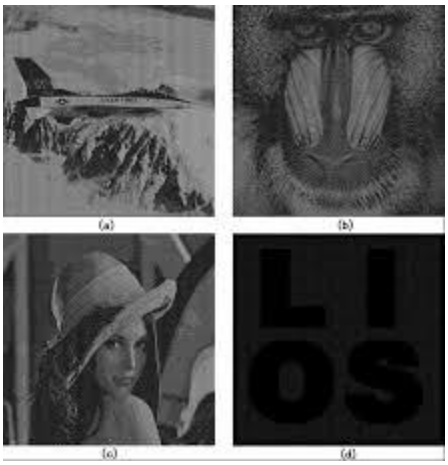


Fig 2. Example for Extended Visual Cryptography (a)First cover image; (b)Second cover image; (c)Third cover image; (d)Original image after all the shares are stacked together.

3 Proposed Scheme

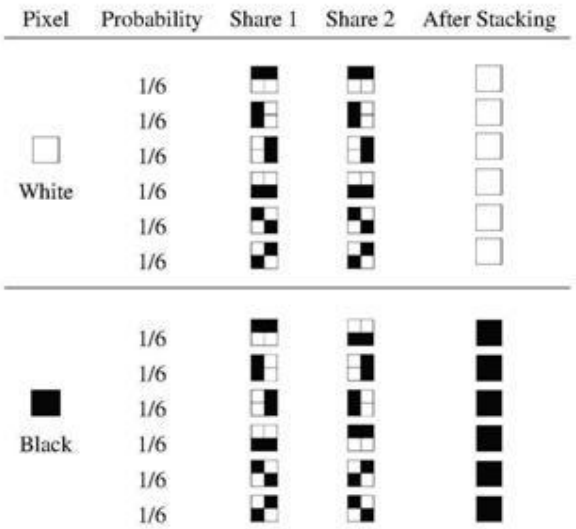
In this paper, we propose a novel extended visual secret sharing scheme without image expansion. Compared to traditional method, the advantage of our method is that secret and share images have same size. Compared to the scheme that does not have expansion, our scheme produces less noisy recovered image. Our scheme recovers the image by stacking the shares by performing logical XOR operation. In the proposed scheme, the grayscale image is converted into binary image by halftoning algorithm. In order to avoid image expansion, preprocessing is done for the image after it is halftoned. Once the preprocessing of the halftone image is done, the shares are created. The shares are XORed (the same color

pixel from both the shares are converted into white and different color pixel are converted into black) to get the processed image back. Better result can be obtained by using the proposed scheme. The scheme proposed is compared with the scheme proposed in [10].

TABLE 2.XOR OPERATION ON PIXELS

Pixel in Share 1	Pixel in Share 2	Pixel after XORed
Black	Black	White
Black	White	Black
White	Black	Black
White	White	White

TABLE 3.ILLUSTRATION OF THE PROPOSED (2; 2) SCHEME



4 PREPROCESSING SCHEME

In this section, 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. In this technique, all the 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 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 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 novel aspect in this approach is to perform the block replacement such that there is a better balance of white and black in the processed secret image. 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 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. 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 halftone secret image. Therefore, the resulting recovered image is closer in quality to the original grayscale image. This step produces a new secret image which contains either white block or black block. The processed image is now ready to be used as a secret image in visual cryptography schemes such as traditional VC or EVC.

4.1 General Description of the Scheme

The preparation of a grayscale image for use in visual cryptography involves 3 steps. The first step is the transformation of a grayscale image into a halftone image and partitioning the halftone image into non-overlapping blocks of 2 2 pixels. Then, the halftone image is divided into a number of overlap-ping 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 halftone image are counted and saved in a template. This number is the threshold value for that cluster. The step then classifies all the secret blocks containing 1 black (resp. white) pixel. If the secret block contains 1 black (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 format. When the first candidate block in a cluster is identified, the numbers of black pixels in the clusters 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 halftone 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 halftone 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 threshold 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 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.

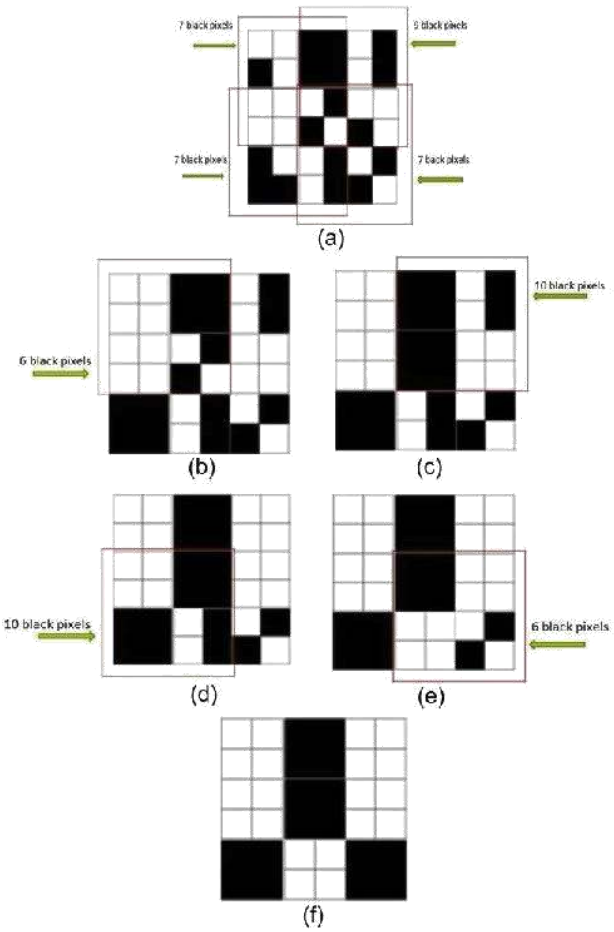


Fig. 3. Example of the Proposed Scheme

4.2 An Example of the Scheme

Figure 3 is an example of how the proposed algorithm works. A halftone 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 overlapping clusters each 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, blocks with 0, 1, 3, or 4 black pixels are converted, leaving only black, white, and candidate blocks to be processed. Figure 3(b) is the resulting initial processed image. Next, the algorithm starts with partitioning the initial processed image into overlapping clusters. Figure 3(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 3(f).

5 Application Of Extended Visual Cryptography

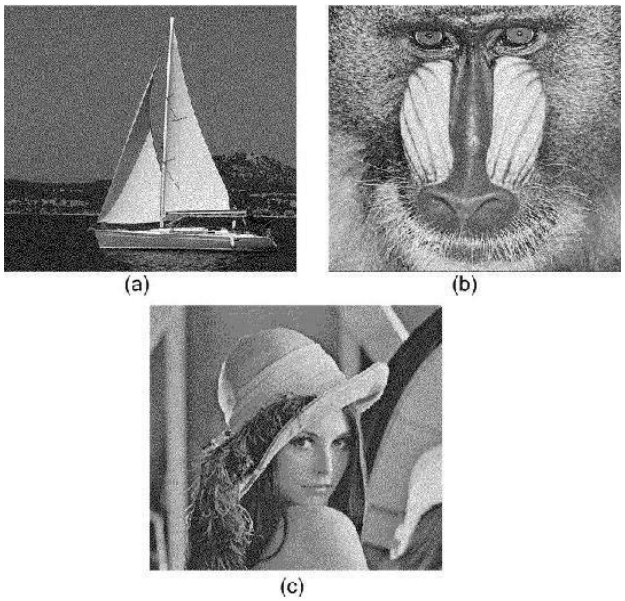


Fig. 4. Images Used for EVC Scheme: (a) halftone boat; (b) halftone baboon; (c) halftone Lena

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 proposed method to ensure that the share and recovered images use the same number of pixels as the original halftone secret image. In this section, we examine the application of the pre-processing schemes to construct a (2; 2) EVC scheme with-out image size expansion. In doing so, we take three halftone images as inputs. The first two images are considered to be meaningful cover images and the 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 blocks and can be used as an input secret image in any visual cryptography encoding process. After producing the three processed images by the appropriate method, the two shares are generated according to the EVC encoding process specified in [4]. The secret image is recovered by XORing 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 proposed scheme on the visual quality of the cover images and the recovered image, we have conducted a visual experiment. As depicted in Figure 4, the halftone boat and the halftone baboon, both of size 512x512, are considered 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 grayscale images using the Floyd-Steinberg halftoning technique [5].

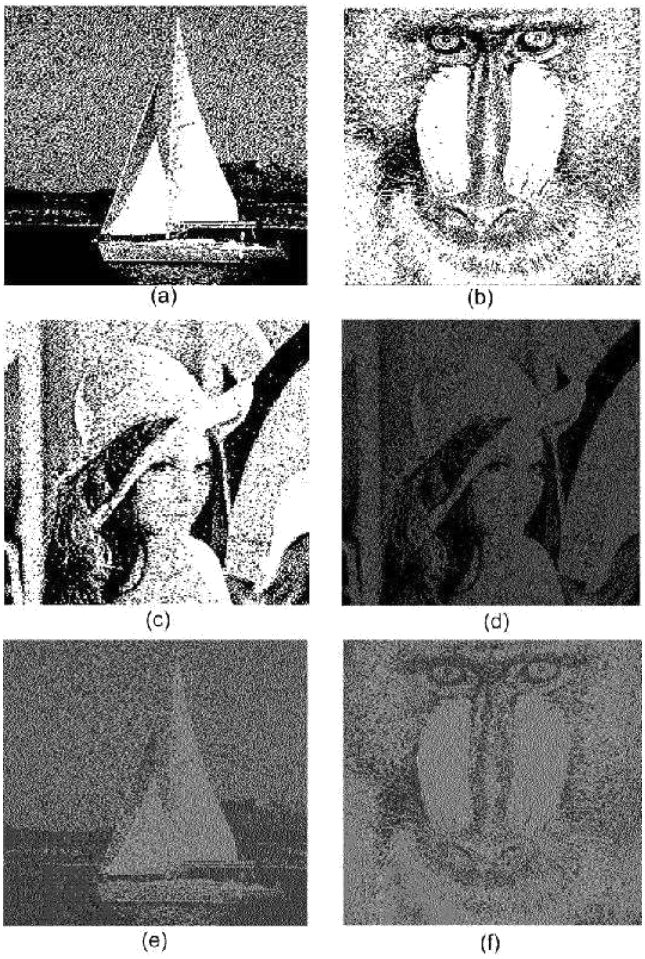


Fig. 5. Experiment Result of BBR method by Askari, Moloney, Heys in [10]; (a) processed boat; (b) processed baboon; (c) processed Lena; (d) Reconstructed Lena; (e) first cover image; (f) second cover image

Figure 5 shows the results of using the BBR pre-processing method proposed in [10], an EVC scheme. The shares and the recovered secret image have the same size as the original halftoned images; however, compared with the original halftone images, the recovered image have a visual quality that is very poor with a severe darkening effect. Figure 6 demonstrates the effect of using the proposed EVC scheme. A significant improvement can be observed in the visual quality of the reconstructed image in comparison to the previous method result.

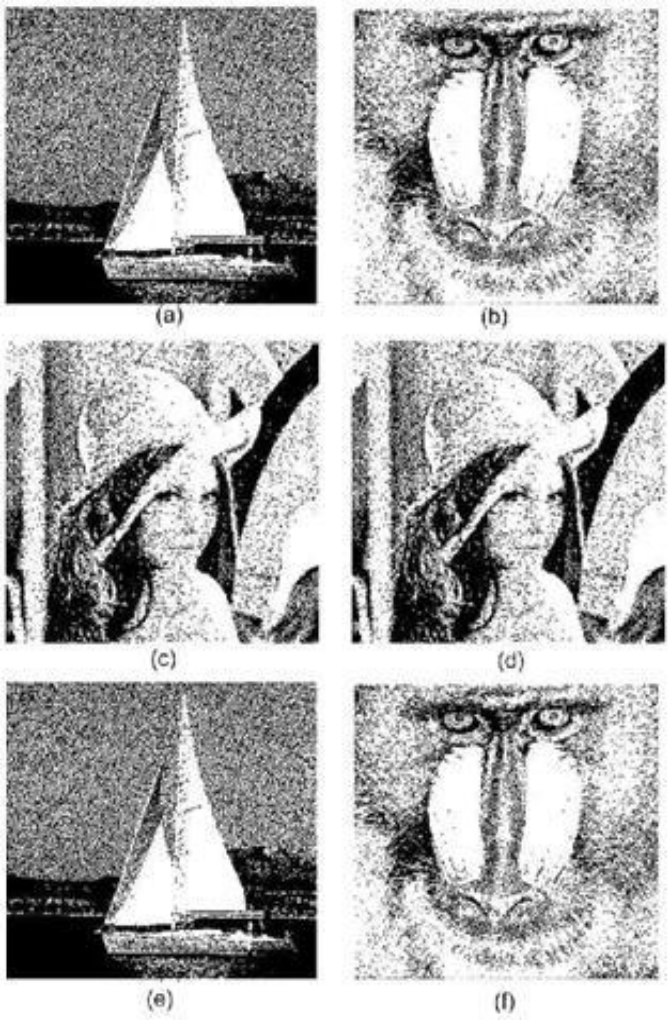


Fig. 6. Experiment Result of the proposed scheme applied in EVC: (a) Processed Boat; (b) Processed Baboon; (c) Processed Lena; (d) Recovered Lena; (e) Recovered Boat; (f)Recovered Baboon

.

The recovered image of Lena proposed in this scheme gives better image quality proposed in [10] and this can be seen from the Figure 5 and 6.

6 Conclusion

In this paper, we have explored extended visual cryptography without expansion. We have shown that using an intelligent pre-processing of halftone images based on the characteristics of the original secret image, and by XORing, we are able to produce good quality images in the recovered image. The principle of this scheme is to encode the block with four pixels into two share blocks according to the number and distribution of black and white pixels, thereby allowing the secret image to be clearly restored by sing XOR operation. This scheme can be applied to both binary and halftone images. Although this scheme introduces some noise into the recovered image, the recovered image is substantially clearer than in other proposed non-expansion scheme. Note that the other application can be benefited from pre-processing scheme such as multiple image visual cryptography, which hides multiple images in share[9].

ACKNOWLEDGMENT

The authors wish to thank all those who provided the information and to those who helped.

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] A. Ross and A. A. Othman, “Visual Cryptography for Biometric Privacy”, IEEE Transactions on Information Forensics and 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 Santis and D.R. Stinson, “Extended Capabilities for Visual Cryptography”, Theoretical Computer Science, vol. 250, pp. 143-161, 2001.

[5] 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.

[6] 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.

[7] M. Nakajima and Y. Yamaguchi, Extended Visual Cryptography for Natural Images, in Proceeedings 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, Taiwan, 2002.

[9] 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.

[10] N. Askari, H.M. Heys, C.R. Moloney, “An extended Visual Cryptography Scheme without Pixel Expansion for Halftone Images” IEEE Canadian Conference on Electrical and Computer Engineering (CCECE),2013.