AN EXTENDED VISUAL CRYPTOGRAPHY SCHEME WITHOUT PIXEL EXPANSION FOR HALFTONE IMAGES

N. Askari, H.M. Heys, and C.R. Moloney

Electrical and Computer Engineering
Faculty of Engineering and Applied Science
Memorial University of Newfoundland

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 share 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 share images and the recovered secret image in an extended visual cryptography scheme for which the size of the share 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 cryptography approach.

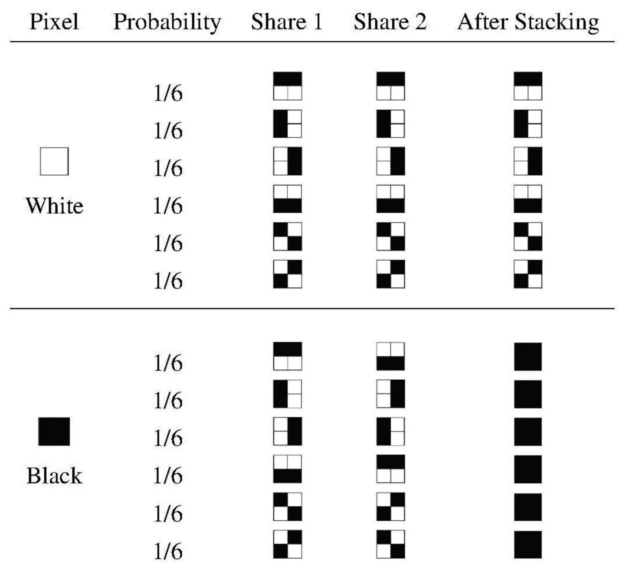
Index Terms— cryptography, image processing, visual cryptography, secret sharing

1. INTRODUCTION

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 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 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.

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 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 subpixels. 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 subpixels) [3]. It may also

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



This research was funded in part by the Natural Sciences and Engineering Research Council of Canada (NSERC).

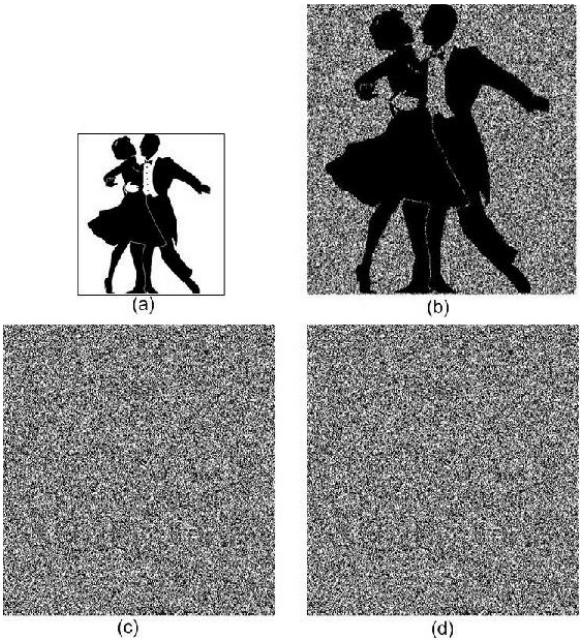


Fig. 1. Example of a $(2, 2)$ VC Scheme with 4 Subpixels: (a) secret Dancers image; (b) reconstructed Dancers image; (c) first share; (d) second share

be noted that the recovered image has a degradation in visual quality (specifically, the contrast between white and black is decreased) since a recovered white pixel is actually comprised of 2 white and 2 black subpixels, while a black pixel is represented by 4 black subpixels in the recovered image.

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 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 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 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.

Although visual cryptography operates on binary images, it can be applied to grayscale images by using a halftoning

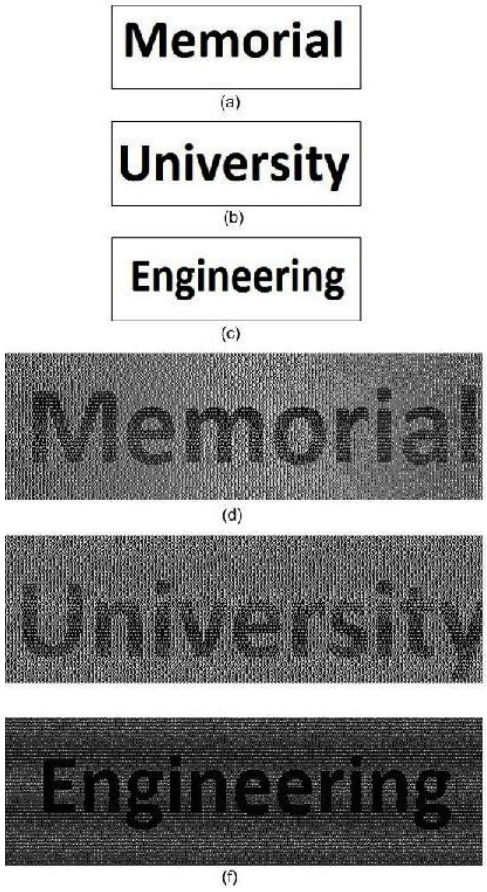


Fig. 2. Example of $(2, 2)$ EVC Scheme: (a) first cover image; (b) second cover image; (c) secret image; (d) share 1; (e) share 2; (f) recovered secret image

algorithm to first convert the grayscale image to a binary image [5]. This allows for 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. However, 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. Previous schemes 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) [6] and compromise of the security of the scheme [7].

The objective of the research outlined in this paper is to derive 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 im-

age. Our proposed scheme maintains the perfect security of the basic EVC scheme [4].

2. PRE-PROCESSING HALFTONE IMAGES

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. 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 [8]. In this paper, we refer to this basic approach as *simple block replacement* (SBR). The SBR scheme considers groups of four pixels from the halftone secret image in one 2×2 block, referred as a *secret block*, and generates the shares block by block (rather than pixel by pixel). As each secret block with four pixels encodes into two secret shares each containing four pixels, the size of the reconstructed 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 equal to 1, 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 cryptography schemes such as traditional VC or EVC.

The SBR approach is straightforward 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 details in the images. In our experiments applied to EVC, we shall see these effects in Figure 5.

3. AN IMPROVED PRE-PROCESSING SCHEME

We now present a novel and effective method for replacing the candidate blocks of a halftone secret image, which we refer to as the *balanced block replacement (BBR)* method. 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. 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 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.

3.1. 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 overlapping 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, then moves from left to right and top to bottom in raster format. When the first candidate block in a cluster is identified, the number 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 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

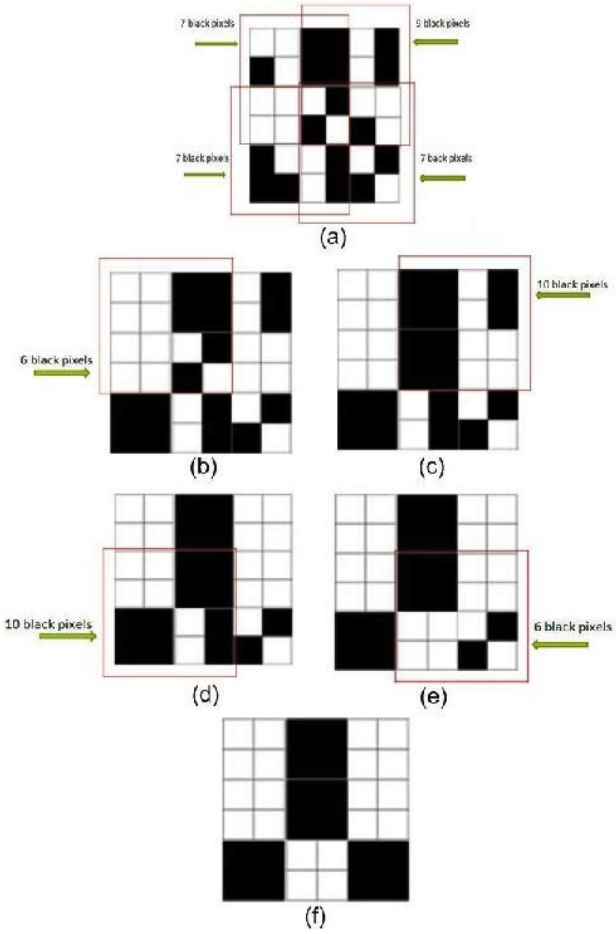


Fig. 3. Example of the BBR Method

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 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.

3.2. 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, or 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).

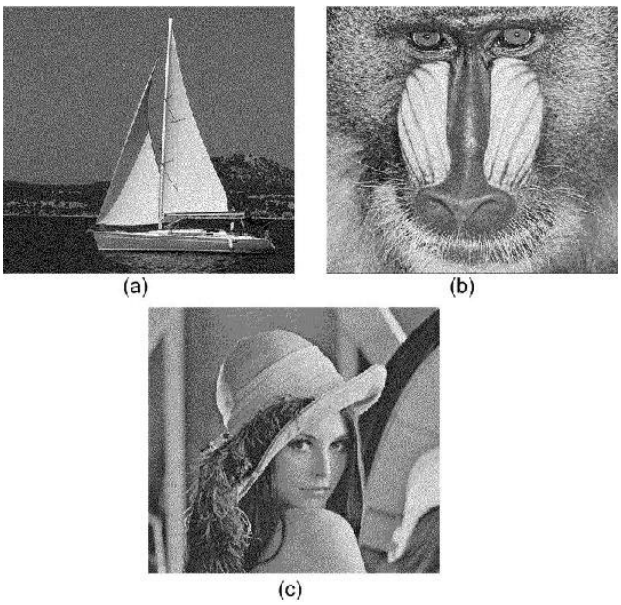


Fig. 4. Images Used for EVC Scheme: (a) halftone boat; (b) halftone baboon; (c) halftone Lena

4. 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 pre-processing scheme, SBR, of Section 2 or the more advanced BBR method of Section 3 to ensure that the share and recovered images 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 pre-processing 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 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 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 Figure 4, the halftone boat and the halftone baboon, both of size 512×512, 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].

Figure 5 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 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 Figure 6(d) versus Figure 5(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 6(e), in comparison to the result for SBR of Figure 5(e). Similarly, the share image of the baboon shows improved clarity around the eyes for the BBR result versus the SBR result.

5. 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, we are able to produce good quality images in the shares and the recovered image. Note that other applications can also benefit from the pre-processing approach, such as multiple image visual cryptography, which hides multiple images in shares [9].

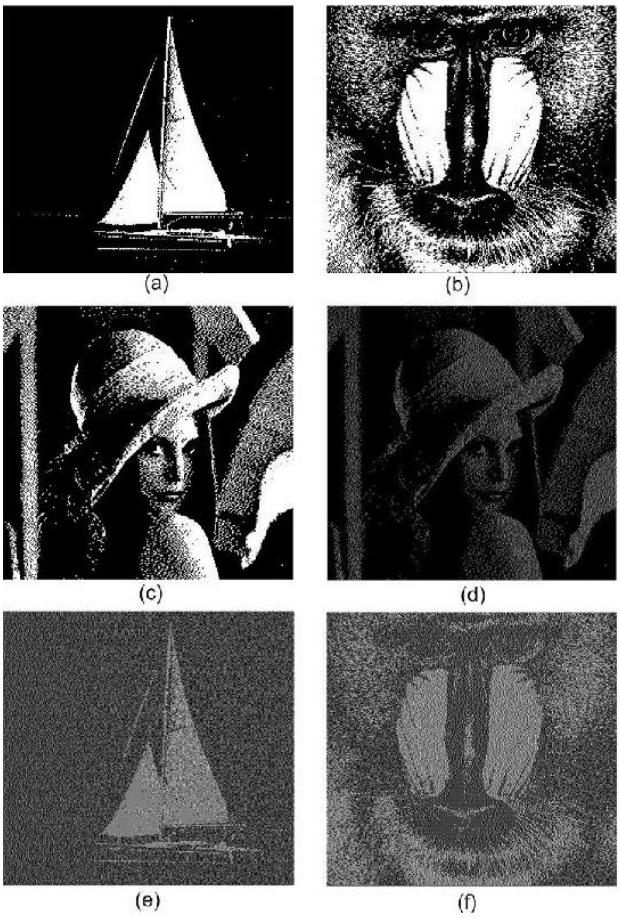


Fig. 5. Experimental Results of SBR Method Applied to EVC: (a) processed boat; (b) processed baboon; (c) processed Lena; (d) reconstructed Lena; (e) first cover image; (f) second cover image

6. 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

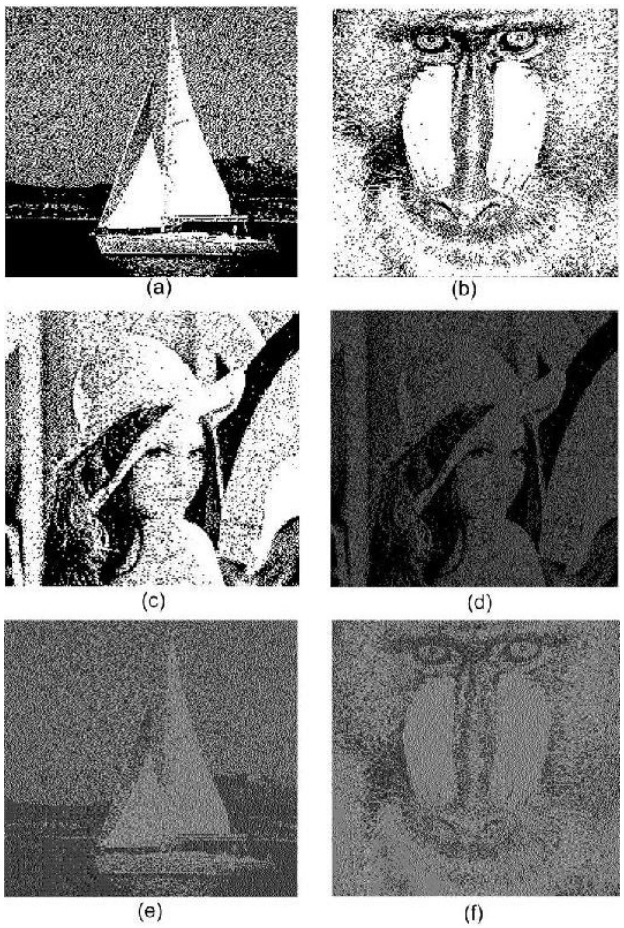


Fig. 6. Experimental Results of EVC with BBR Method Applied to EVC: (a) processed boat; (b) processed baboon; (c) processed Lena; (d) reconstructed Lena; (e) first cover image; (f) second cover image

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.