ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

An EXTENDED VISUAL CRYPTOGRAPHY SCHEME WITHOUT PIXEL EXPANSION USING DITHERING

Amina Shereen O V[1], Lijina S S[2]

Student, M Tech CSE, Malabar Institute of Technology Anjarakandy, Kannur, India [1]

Assistant Professor, M Tech CSE, Malabar Institute of Technology Anjarakandy, Kannur, India [2]

Abstract: Visual Cryptography is secret sharing scheme which uses images distributed as shares such that when they are superimposed, the hidden secret image is revealed. In extended visual cryptography (EVC), the shares are constructed to contain meaningful cover images. Here, we propose a technique called dithering to block replacement methods of EVC, in order to improve the quality of recovered secret image. The size of share image and recovered image is same as that of original secret image. The resulting scheme also maintains perfect security by applying random number generation to the secret image.

Keywords: Extended Visual Cryptography, halftone images, Dithering, Pixel expansion

I. INTRODUCTION

Visual cryptography (VC) was first proposed by Naor and Shamir in 1994, which was based on black and white or binary images. Visual Cryptography is a secret sharing scheme, in which shares may be distributed to various parties, so that only by collaborating with an appropriate number, can resulting combined shares reveal the secret image. Recovery of the secret can be done with the help of human visual system. Visual Cryptography is of particular interest to biometric applications [6].

A basic 2-out-of-2 VC scheme produces two share images from an original image and must stack these two shares to reproduce the original image [5]. In order to preserve the aspect ratio for the recovered secret image for a (2; 2) scheme, each pixel in the original secret image can be replaced in the share images by a 2 x 2 block of sub pixels. As shown in Figure 1, if the original pixel is white, one of six possible combinations is randomly created. Similarly, the share combinations for black pixels are also shown. After stacking the shares with white transparent and black opaque, the original secret image will be reproduced. Stacking is done by mathematically ORing, where white is equivalent to 0 and black is equivalent to 1.

It may also be noted that the recovered image has degradation in visual quality, since a recovered white pixel is comprised of 2 white and 2 black sub pixels, while a black pixel is comprised of 4 black sub pixels in the recovered image. The process is illustrated in Figure 2 for a simple binary image.

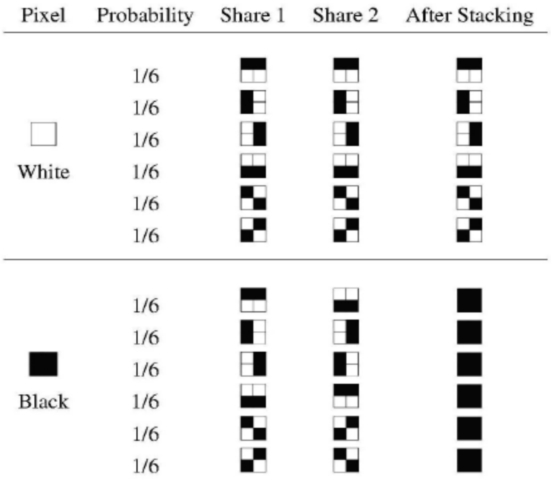

Fig 1. Illustration of a (2; 2) VC Scheme with 4 Sub pixels

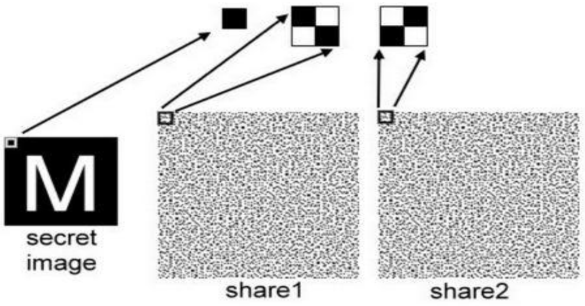

Fig 2. Example of a VC scheme

In 1996, Ateniese et.al. proposed extended visual cryptography (EVC) schemes that can construct meaningful share images. The (2; 2) EVC scheme proposed in [2] also required expansion of one pixel in the original image to 4 sub pixels. It can be shown that no share image leaks any information of the original secret image. Figure 3 illustrates a (2; 2) EVC scheme containing the binary secret image, Engineering, with two cover images, Memorial and University [1].

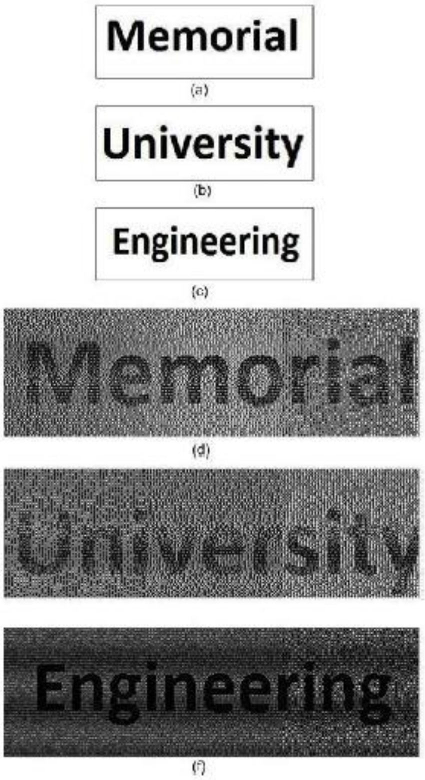

Fig 3. Example of an EVC scheme [1]

Visual cryptography operates on binary images. It can also be applied to grayscale images by using a half toning algorithm to first convert the grayscale image to a binary image [9]. Hence, using half toning techniques to convert grayscale images to binary images is a useful pre-processing 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 schemes also result in a reduction in image quality, mitigating image degradation becomes an important objective in a visual cryptography scheme. Previous schemes integrating half toning 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) [7] and compromise of the security of the scheme [4].

The objective of this paper is to produce an EVC scheme which gives more clarified share image and recovered secret image without pixel expansion using a technique called dithering. Our proposed scheme maintains the perfect security of EVC scheme.

II. PRE-PROCESSING HALFTONE IMAGES

The application of visual cryptography to gray scale image can be considered by first converting the text password to a binary image. After creating the halftone image, it is the processed and in order to preserve the image size when applying extended visual cryptography, simple methods can be applied. One such method is Balanced Block Replacement method or BBR.

It is an improved scheme for processing halftone images. It is an effective method for replacing the candidate blocks of a halftone secret image. The purpose behind BBR is to perform the block replacement such that there is a better balance of black and white in the processed secret image. The image which contains only white and black block is referred to as 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 [1].

III.DITHERING IN BBR

Dithering is the attempt by a computer program to approximate a color from a mixture of other colors when the required color is not available. It works by approximating unavailable colors with available colors, by mixing and matching available colors in a way that mimics unavailable ones.

In a simple case, a gray scale image can be represented by different patterns of black and white pixels. Take for instance, an image that is pure white; we would like the dithered result to be nothing but white pixels. Likewise, for a pure black image we would like just black pixels. However, if we consider an image that has a mid gray level (I.e. 50% black); the best representation of that tone would be an interlaced image of black and white pixels, more commonly known as a checkerboard pattern [8].

Through this exploitation of the human eye, we can make a variety of intensities by closely pairing intensities, or even colours, together.

Dithering is applied to the block replacement method called Balanced Block Replacement (BBR) thereby overcoming the problem of pixel expansion. BBR approach is to perform the block replacement such that there is a better balance of white and black in the processed secret image. We balance white and black in the processed image by assigning some candidate blocks to black and others to white [1].

The representation of midtone gray to dither is as shown in Figure 3.

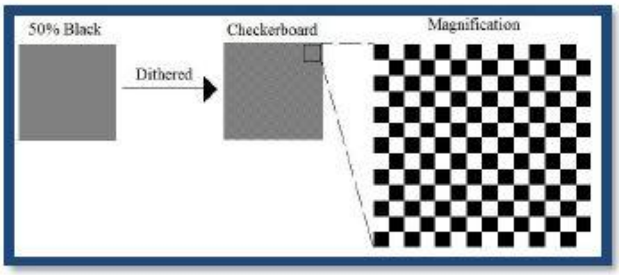

Fig 3. Midtone Gray to Dithered Representation

Here, we propose a block replacement method; BBR 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.

IV. General Description of the Scheme

The preparation of a grayscale image in visual cryptography involves 3 steps [1]. 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 x2 pixels. Then, the halftone image is divided into a number of overlapping squares of four 2 x 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 number of black pixels in the cluster is 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.

V. An Example of BBR Scheme

Figure 4 is an example of how the proposed algorithm works. A halftone image of size 6 x 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 4(a), we can see 7 black pixels in the first block. 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 4(b) is the resulting initial processed image. Next, the algorithm starts with partitioning the initial processed image into overlapping clusters. Figure 4(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 4(f).

DOI 10.17148/IJARCCE

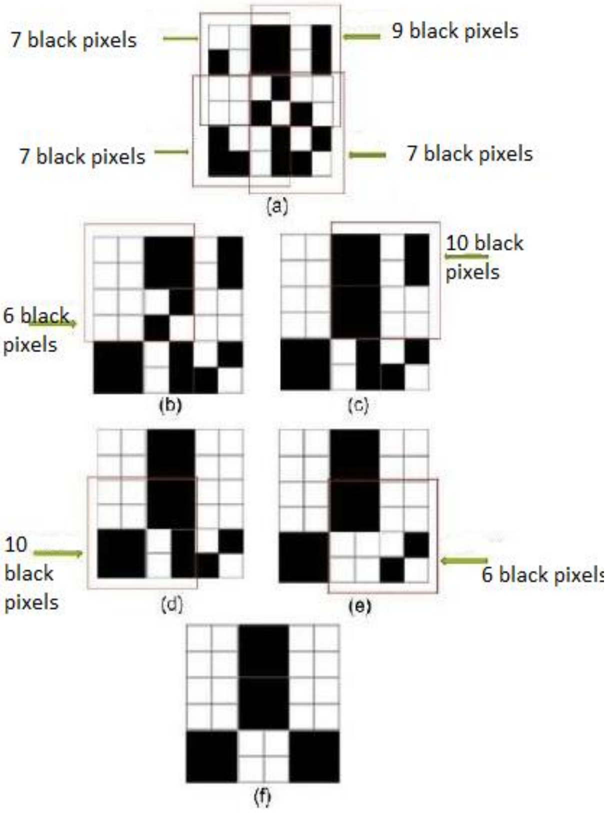

Fig 4. Example of BBR method

VI. Conclusion

In this work, we explored extended visual cryptography without pixel expansion using halftone images. We overcome the problem of visual cryptography by integrating it with bio-metric privacy thereby constructing meaningful cover images. Share images and cover images are constructed.

The work proposed a technique called dithering to a block replacement method, which is the Balanced Block Replacement to halftone images that improves the quality of share image and recovered secret image. So the size of share image and recovered image is same as that of original halftone secret image. The resulting scheme maintains perfect security of extended visual cryptography approach.

ACKNOWLEDGMENT

We take this opportunity to express my gratitude to all of the Department faculty members for their help and support.

We also place on record, my sense of gratitude to one and all, who directly or indirectly, have lent their hands in this venture.

References

[1] Nazanin Askari, Howard M Heys, and CR Moloney, *An extended visual cryptography scheme without pixel expansion for halftone images*, Electrical and Computer Engineering (CCECE), 2013 26th Annual IEEE Canadian Conference on, IEEE, 2013, pp. 1–6.

[2] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R Stinson, *Extended capabilities for visual cryptography*, Theoretical Computer Science **250** (2001), no. 1, 143–161.

[3] Thomas Funkhouser, *Image quantization, half toning, and dithering*, Princeton University.¡ http://www. cs. Princeton. Edu/courses/archive/-fall99/cs426/lectures/dither/index. htm (2000).

[4] Mizuko Nakajima and Yasushi Yamaguchi, *Extended visual cryptography for natural images*, (2002).

[5] Moni Naor and Adi Shamir, *Visual cryptography*, Advances in CryptologyEUROCRYPT'94, Springer, 1995, pp. 1–12.

[6] Arun Ross and Asem Othman, *Visual cryptography for biometric privacy*, IEEE transactions on information forensics and security **6** (2011), no. 1, 70–81.

[7] Zhi Zhou, Gonzalo R Arce, and Giovanni Di Crescenzo, *Halftone visual cryptography*, Image Processing, IEEE Transactions on **15** (2006), no. 8, 2441–2453.

[8] Jonathan Carrier, *Digital Halftone (Dithering) Methods and Applications Digital Image Processing* University of New Hampshire (2008)

[9] Floyd, Robert W. "*An adaptive algorithm for spatial gray-scale*." *Proc. Soc. Inf. Disp.* Vol. 17. 1976.

BIOGRAPHY

Amina Shereen O V is an M Tech student of Malabar Institute of Technology, Anjarakandy in Computer Science and Engineering department at the University of Kannur. She completed her B Tech from MES College of Engineering, Kuttippuram. She can be contacted at amina.sherin@gmail.com. You can also reach her at the mobile number +919633996102. She dwells at Thalassery.