A Survey on Cryptographic Authentication Scheme by enhanced Halftone Images

NitinNavale[*], SanketShinde[*], ShyamAndhale[*], MangeshLahamge[*], Prof. Pramod Patil[**]

[*] UG Student Department of Information Technology, Nutan Maharashtra Institute of Engineering and Technology; Talegaon, Pune.
[**] Assistant Professor Department of Information Technology, Nutan Maharashtra Institute of Engineering and Technology; Talegaon, Pune.

Abstract- Visual cryptography is a secret sharing scheme in which secret image is distributed in n number of shares such that, when this n shares are superimposed together, a hidden secret image is get. In extended visual cryptography, we use the cover image for share images, which will give integrating visual cryptography. In this paper, we propose a method for improving the quality of processing halftone images of the share images and the recovered secret image. In an extended visual cryptography scheme the size of the share images and the recovered image is the same as the original halftone secret image. The resulting scheme of extended visual cryptography maintains the quality of original secret image and its security.

Index Terms- image processing, visual cryptography, secret sharing, halftone algorithm.

I. INTRODUCTION

A visual cryptography (VC) is a secret sharing scheme introduce by Naor and Shamir. A basic 2-out-of-2 or (2; 2) visual cryptography scheme generates 2 share images from an original image and must combined both shares together to regenerate the original image. Generally, a (k; n) scheme generates n shares, but only k shares requires to recover the secret image. To maintain the aspect ratio for the recovered original secret image for a (2; 2)scheme each pixel of the original image is replaced in the share images by a 2 X 2 block of sub pixels. For both black and white pixels, six combinations of share pixels are randomly created as shown in fig.1. After stacking the shares with white transparent and black opaque, the original secret image will be recovered. Stacking can be done by using mathematically O Ring operation, where white pixel is consider as "0" and black pixel is consider as "1".As each pixel of original image is divided into 4 sub pixels, the resulting share images and the recovered secret image contain 4 times more pixels than the original image. It results into degradation of the recovered original secret image in visual. White pixelis a combination of 2 white and 2 black subpixels, while a black pixel is 4 black subpixels in the recovered image.

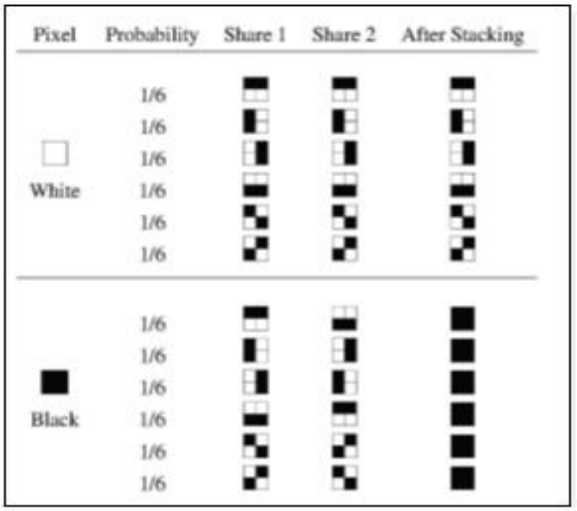
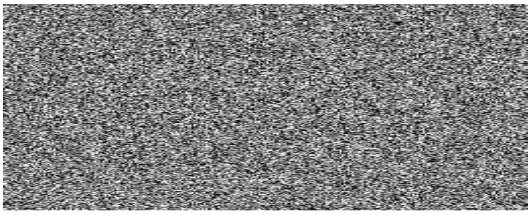


Fig.1 Illustration of a (2;2) VC Scheme with 4 Subpixels.

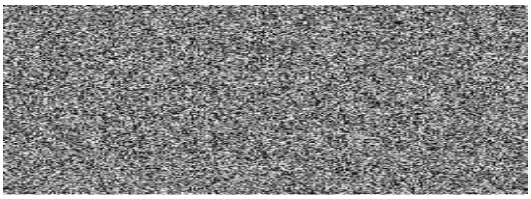
As the shares are generated randomly, the individual share does not provide any information about the secret image, to recover original image all shares must be required. It is might be helpful in a security context. For example, as shown in fig.2 the Hello image(a) is the original secret image, fig.2(b) shows the processed image of original image and fig.2(c, d) are shares generated the individual share (c) or (d) does not give any information of the original image(a).

(a)

(b)



(c)



(d)

Fig. 2 Example of a VC Scheme with 4 Subpixels: (a) hello; (b) processed hello image; (c)first share; (d) second share.

Figure.2 illustrates a (2;2) scheme containing the original binary secret image hello", with processed hello imageand two shares. To recover original secret image both shares are necessary. In Visual cryptography the image is first converted in a grayscale then binary image by using halftone algorithm. 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. This halftoning process applied to a grayscale image results in degradation of the image quality and since visual cryptography schemes also result in degradation in image quality, so image degradation becomes an important factor in a visual cryptography scheme. Hence, previous visual cryptography schemes suffered from issues of image expansion (as each pixel is divided into 4 subpixels) and compromise of the security of the scheme. The main objective of this paper is to improve the quality of resulting images and security. In extended visual cryptography scheme, the original size of pixels remains as it is, it does not produce more pixels in the shares and recovered image than the original secret image and maintains a good quality image for both the shares and the recovered image.Our proposed scheme maintains the quality and perfect security of the basic EVC scheme.

II. PRE-PROCESSING HALFTONE IMAGES

In this, we consider the application of visual cryptography for grayscale images first we converting the image to a binary image using a halftoning algorithm. After creating a halftone image, in order to maintain the image size and quality we applying simple methods of visual cryptography and extended visual cryptography. A basic, secure method is easy to implement which is based on a block-wise approach to pre-processing the binary halftone image.

III. SIMPLE BLOCK REPLACEMENT (SBR)

In SBR scheme we considersfour group of pixels from the halftone secret image and generates the shares block by block (instead of pixel by pixel). Block replacement in SBR is based on the number of black and white pixels present in block. If a black pixel in one block is greater than or equal to two then block becomes black and if black pixels is less than two the block becomes white. It will generate the new image which has only white and black blocks; this image is called as pre-processed secret image. This image is now ready to use as a secret image in visual cryptography or in extended visual cryptography. But the disadvantage of this system is, it produces more black or white images.

IV. BALANCED BLOCK REPLACEMENT

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. In this method blocks of two white and two black pixels consider 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.

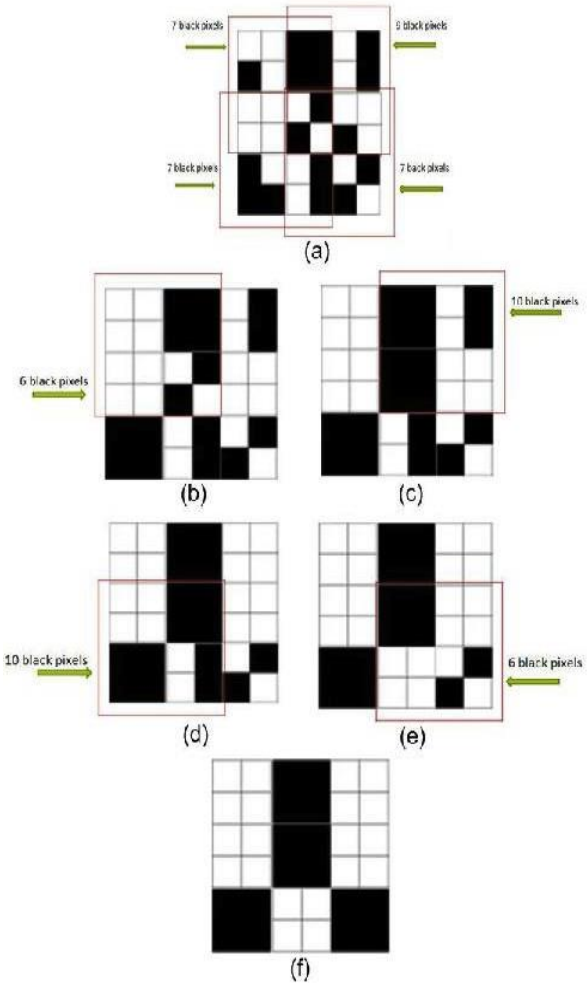


Fig.3 Example of BBR.

V. EXTENDED VC

In an extended VC scheme, each share have some meaningful cover image .An extended VC scheme image expansionis necessary to exactly preserve the information from the pixelsof the original secret image in the recovered secret image, we can use the basic pre-processing scheme, SBR or the more advanced BBR method toensure that the share and recovered images use the same numberof pixels as the original halftone secret image. Absolutely, the trade-off in such an approach is a decline in image quality.

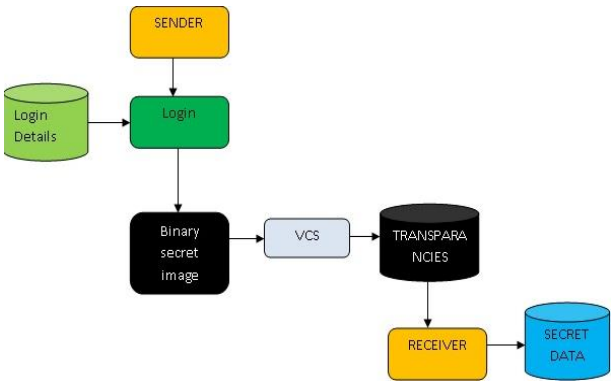


Fig.4 Architecture.

VI. 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 eachcluster 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 initialprocessed image.The third step starts from the first block in the top left ofthe first cluster of the initial processed image. The processingof the blocks in each cluster starts from the top left block,then movesfrom 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. Theidea is to keep the number of black and white pixels in eachcluster of the initial processed image as close as possible tothe corresponding threshold value from the cluster of the originalhalftone image. Therefore the number of black pixels inthe case of changing the candidate block to a black or whiteblock is computed and is compared to the threshold value thatwas derived for the same cluster in the original halftone image.

If the corresponding candidate block converts to a blackblock, 2 pixels will be added to the number of black pixelsin a cluster and if the candidate block turns to white block, 2black pixels will be reduce from a cluster.The conversionis based on the difference between threshold and the number of black pixels in the processed image. Ifchanging the candidate block to black the difference issmall, the candidate block is converted to a black block. Similarly, if the candidate blocks to white the difference small, 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 blackor white block.

An Example of the Scheme

Fig3 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 overlappingclusters 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. Sequentially, blocks with 0, 1, 3, or 4 black pixels are converted; leave only black, white 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 to4. 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).

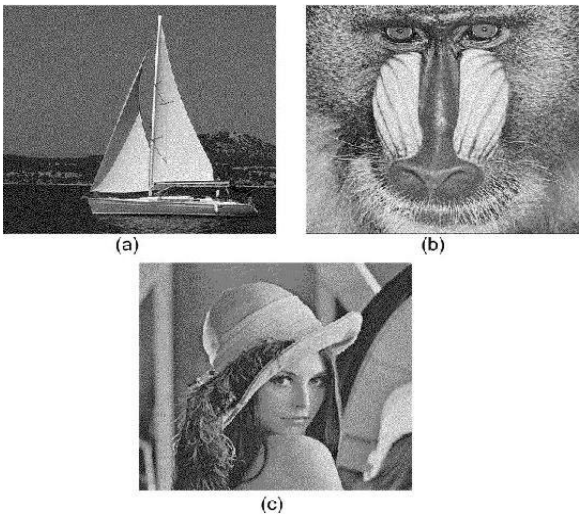


Fig. 5. ***Images Used for EVC Scheme: (a) halftone boat; (b) halftone baboon; (c) halftone Lena***

VII. APPLICATION TO EXTENDED VC

Biometric Security
Watermarking
Steganography
Bank Customer Identification

VIII. CONCLUSION

In this paper, we have explored extended visual cryptography without expansion. We have shown that using an intelligentpre-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, whichhides multiple images in shares.

REFERENCES

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

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

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

[4] AnkitaGharat, PreetiTambre, Yogini Thakare, Prof. S.M. Sangave, International Journal of Advanced Research in Computer Engineering and Technology(IJARCET), vol. 2, 2013.

AUTHORS

First Author – NitinNavale, UG Student
Second Author – SanketShinde, Department of Information Technology, Nutan Maharashtra Institute of Engineering and Technology; Talegaon, Pune.
Third Author – ShyamAndhale, Department of Information Technology, Nutan Maharashtra Institute of Engineering and Technology; Talegaon, Pune.
Fourth Author – MangeshLahamge, Department of Information Technology, Nutan Maharashtra Institute of Engineering and Technology; Talegaon, Pune.
Fifth Author – Prof. Pramod Patil, Assistant Professor Department of Information Technology, Nutan Maharashtra Institute of Engineering and Technology; Talegaon, Pune.