A Robust Visual Cryptography Technique for Photographic Grayscale Images Using Block Optimization and Blind Invisible Watermarking

Ayan Banerjee and Sreya Banerjee

***Abstract*—In this paper, we have proposed a new approach for Visual Cryptography of Photographic Grayscale images. Also we have addressed the issue of preventing cheating attacks in the proposed Visual Cryptography Scheme by invisibly watermarking the shares onto Host Images. This scheme not only provides Authentication for the VC shares but also makes these secret shares invisible by embedding them into not so significant Host images. Experimental results show that the proposed method is secure from attacks such as filtering, JPEG compression and fake share creation. The proposed method give high quality visually recognizable reconstructed images.**

***Index Terms*—Blind invisible watermarking, block preparation, host image, shares, visual cryptography.**

I. Introduction

Visual Cryptography (VC) was first introduced by Moni Noar and Shamir at Eurocrypt' 94 [1]. It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. Shares are binary images. They are usually, but not necessarily, presented in transparencies. Unlike conventional cryptographic methods, classical VC needs no complicated computation for recovering the secret. The act of decryption is to simply stack shares and view the Secret image that appears on the stacked shares.

However, the proposed VC method differs from the classical VC methods in that the proposed method generates shares that are binary images but not represented on transparencies. Hence the secret image recovery process requires significant processing.

The proposed VC method, however, is capable of encrypting 7bit grayscale images. Thus unlike classical VC, which is being used by several countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc., the proposed scheme can be used to transfer Photographic Grayscale Images.

Watermarking is the technique of embedding a secret image into a cover image without affecting its perceptual quality so that the secret image can be revealed by some process. One significant advantage of watermarking is the inseparability of the watermark (secret image) from the cover image. Some of the vital characteristics of the watermark are: hard to perceive, resists ordinary distortions, endures malevolent attacks, carries numerous bits of information, capable of coexisting with other watermarks, and demands little computation to insert and extract Watermarks. Generally, robust watermarking is used to resist un-malicious or malicious attacks like scaling, cropping, lossy compression, and so forth. Watermarking techniques can be categorized into different types based on a number of ways. Watermarking can be divided into Non-blind, Semi-Blind and Blind schemes [2], [3] based on the requirements for watermark extraction or detection. Non-blind watermarking schemes necessitate the original image and secret keys for watermark detection. The Semi-Blind schemes require the secret key(s) and the watermark bit sequence for extraction, whereas, the Blind schemes need only the secret key(s) for extraction.

Another categorization of watermarks based on the embedded data (watermark) is: visible and invisible. With visible watermarking of images, a secondary image (the watermark) is embedded in a primary image in such that it is perceptible to a human observer, whereas the embedded data is not detectable in case of Invisible watermarking; nevertheless, it can be extracted by a computer program.

Here our proposed scheme will add the merits of both visual cryptography as well as Invisible and Blind watermarking techniques , where we will generate the secret shares using basic visual cryptography model and then we will watermark these shares into some host image using invisible and blind watermarking. Thus the secret shares are protected from cheating attacks. The decryption will be same as in the visual cryptographic model i.e. by stacking of the shares after the secret shares have been extracted by a simple watermark extraction technique. The proposed watermarking scheme doesn't necessitate the original image or any of its characteristics for the extraction of watermark, and hence the proposed scheme is blind. The experimental results have demonstrated the efficiency of the proposed scheme [4], [5].

The rest of this paper is organized as follows: - Section II, the concept of block optimization is provided. Section III describes the proposed Visual Cryptography Scheme. Section IV describes the proposed Watermarking technique. Section V gives the concept of cheating in Visual Cryptography. Section VI describes the proposed method, section VII gives Experimental Results and Section VIII concludes the paper.

II. Block Preparation

In an image there is usually a likelihood of high correlation between neighbouring pixels [7], [8]. Let us consider an image of m×n resolution - that is, there are m numbers of rows,

Manuscript received February 20, 2012; revised March 26, 2012.

The authors are with the Cognizant Technology Solution, Kolkata, India (e-mail: ayan_cbs@yahoo.com).

each row containing n number of pixels in the digitally coded image. The basic approach we have formulated for reducing dimension of the Secret Image has been derived from the concept of block optimization. The first step is applying averaging filter to reduce the color space of the image. Consider an m×n image; also consider a 3×3 or larger window Wk for masking. The filter can be simple averaging filter or a weighted average filter, depending on requirements. For every position of the filter the following steps are performed:

- The average value (A_k) is calculated from the pixel values in the image corresponding to the position of the filter.
- Calculate average value (A_k) from the elements belonging to W_k.

$$A_K = \frac{1}{9} * \sum_{i=i(init)}^{i(init)+2} \sum_{j=j(init)}^{j(init)+2} X_{i,j} \ ,$$

where i(init) and j(init) are initial values of i and j respectively for the masking window W_k.

- All pixel values corresponding to the neighborhood of the mask in the image is replaced by the resultant average value computed in the previous stage.
- Finally, for all these 9 pixel values (which are same, after previous stage), a single pixel is created for the augmented image.
- The subsequent steps of the proposed scheme are carried on this augmented image.

For example, suppose the original 3×3 pixel neighbourhoods are:

19	21	23
17	22	23
21	24	16

Here, average value =21.

After averaging and replacement the neighbourhood pixels are:

21	21	21
21	21	21
21	21	21

As can be easily understood, the quality loss in the resultant image will depend largely on the size of the mask used for the averaging process. It is quite natural that for a 20×20 image, if a filter size of 3×3 is used, it will lead to objectionable loss in quality, but the same filter size will not affect an image of size 1024×768 as much; the situation will be more acceptable if the image size is even greater. In fact, for large images we can use filter of size greater than 3×3 and still maintain unobjectionable quality loss. For smaller images the filter size will be small and vice versa. In the proposed method we use a 4×4 filter.

III. Visual Cryptography

Visual cryptography (VC) is a method of encrypting a secret image into shares such that processing a sufficient number of shares reveals the secret image. Shares are usually presented in transparencies.

In the proposed method we encrypt the Augmented Secret Image into 4 shares in such a way that every pixel in the Secret image is represented by a (4x4) block (i.e. 16 pixels) in each of the 4 shares formed. The shares formed are themselves binary images. The pixel values of the blocks, in all the 4 shares, corresponding to a pixel in the Secret Image are such that:

$$\sum_{p=0}^{4} \sum_{\substack{x=a+1 \\ y=b+1}}^{\substack{y=b+4 \\ x=a+4}} f(x,y) = \left(\frac{g(i,j)}{4} \right)$$

$$\forall i : 1 \le i \le m$$

$$\forall j : 1 \le j \le n$$

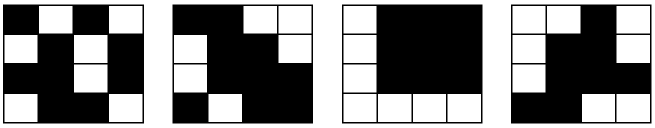
where,

a = 4(i-1) , b = 4(j-1)
(m,n) = dimension of Secret Image
f(x,y) = bit of share at (x,y) position
g(i,j) = pixel of Secret Image at (i,j) position
p = share number

Though there is the above constraint on the total number of black and white pixels in the blocks of the 4 shares combined, which pixel in which share will be back or white is completely random. Every pixel in the blocks of the 4 shares has the equal probability of being black or white (i.e. information or noise padding). This stems from the principle that a truly random selection will make the method more crypto secure.

In the proposed method we decrypt the Augmented Secret Image from the shares by counting the nos information pixels present in all the shares for a particular block and multiplying the value by 4. For every block we create a 8bit pixel in the Reconstructed Augmented Image with the pixel value as the value obtained in the above step.

An example of the decompression process is shown below:



Share 1 **Share 2** **Share 3** **Share 4**

Resultant Pixel Value =144

In the above example the Total Number of Information pixels (black) present in all four shares combined is :

9 + 10 + 9 + 8 = 36

Thus, pixel value in RAI = 36 * 4 = 144

IV. Watermarking

In the proposed method we watermark the shares, which actually are binary images, onto natural 24 bit RGB color or 8 bit Grayscale images. If the dimension of a share is m×n then the dimension of a cover image needs to be exactly m×n.

The watermarking method replaces the lsb of every pixel of the grayscale cover image by the pixel bit value of the share at the same position. In case of RGB color cover image, the watermarking scheme replaces the lsb of red component of every pixel of the cover image by the pixel bit value of the share at the same position.

Thus the Shares are watermarked into the cover images with little or no effect on the visual appearance of the cover image.

The watermark extraction principle is also very simple. The watermarked cover image is read and if the cover image is grayscale then lsb of every pixel is stored in a bitmap to get the corresponding embedded share. If the watermarked cover image is a 24 bit RGB color image then lsb of red component of every pixel is stored in a bitmap to get the corresponding embedded share.

As an example, if the pixel value of watermarked grayscale image are:

Pixel 1: 10110011
Pixel 2: 00110110

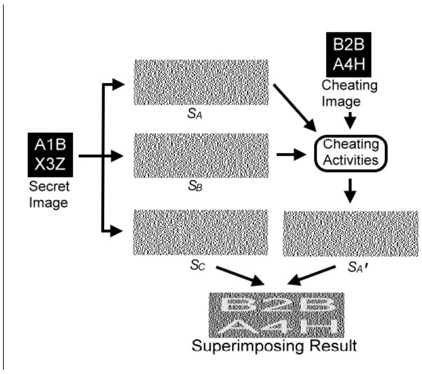
Then the pixel value of the share at the same co-ordinate is 1 and 0 respectively.

V. Cheating

A cheating process against a VCS [9] consists of the following two phases:

- Fake share construction phase where the cheater participant generates the fake shares;
- Image reconstruction phase where the Fake image appears on the decryption of genuine shares and fake shares.

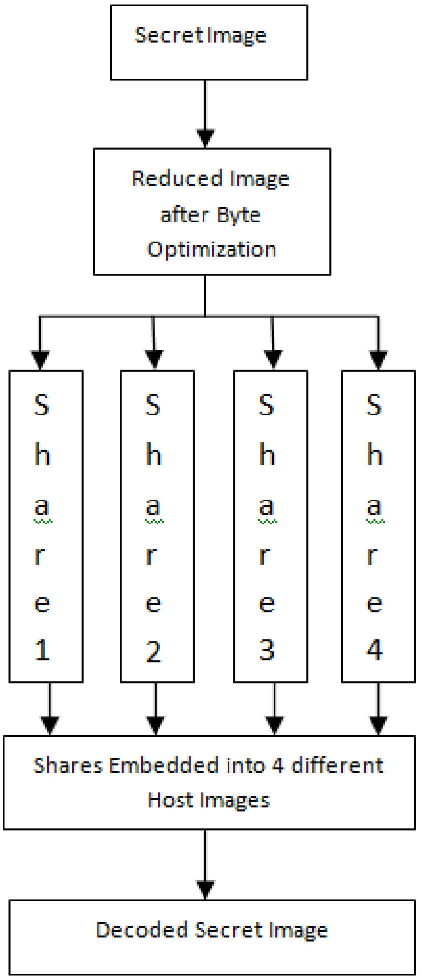
In the case of cheating, honest participants who present their shares for recovering the secret image are not able to distinguish fake shares from genuine shares. A reconstructed image is perfect image indistinguishable from the original. The key point of cheating is how to predict and rearrange the positions of black and white sub pixels in the victim's and cheater's share. Fig. 3 shows the whole cheating process and Table 1 shows how the cheaters create fake shares to change the decoded image.



VI. Proposed Method

In the proposed scheme we shall first generate the augmented secret image using Block Optimization. Then we shall generate the VC shares using the visual cryptography model proposed and then embed them into 4 different cover images using an Invisible Blind Watermarking technique, so that the shares will be more secure and meaningful. And the shares are protected from the malicious adversaries who may alter the bit sequences to create the Fake shares. During the Decryption phase, the secret shares are extracted from their cover images without needing any of the cover image characteristics.

The Schematic diagram of the entire process is as follows:


Secret Image
Reduced Image after Byte Optimization
Share 1
Share 2
Share 3
Share 4
Shares Embedded into 4 different Host Images
Decoded Secret Image

The Encryption process is as follows:

Step 1: Subject the Secret Image to Block Optimization to reduce its dimensions. This step Results in the formation of the Augmented Secret Image (ASI).

Step 2: Subject the ASI so formed to the proposed Visual Cryptographic Method. This step results in creation of 4 Shares.

Step 3: Embed each of the 4 shares onto different cover images using blind invisible watermarking scheme.

The Decryption process is as follows:

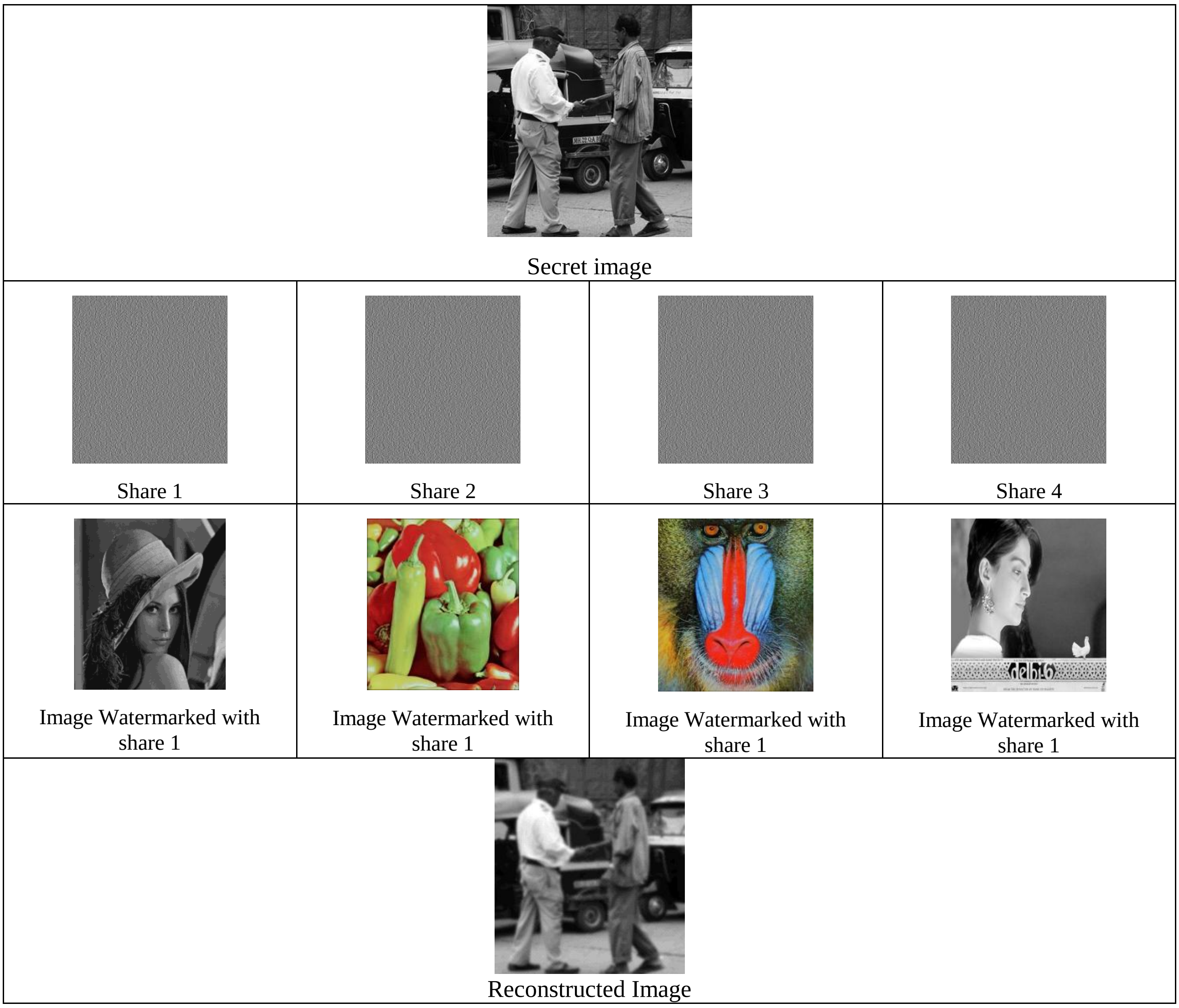
Step 1: Extract the shares from the watermarked images using the proposed watermark retrieval technique.

Step 2: Combine the 4 shares thus obtained using the proposed Visual Cryptographic Decription Method to form the Reconstructed Augmented Image(RAI)

Step 3: Repeat each pixel in the RAI 16 times in a 4×4 format to get back the original dimension Secret image

VII. Experimental Results

The proposed scheme has been simulated in MATLAB. The Secret Images are considered to be 8 bit grayscale bitmap images. The cover images used are both 8bit grayscale and 24bit RGB bitmap images. The experimental results are shown in Fig. 1. The PSNR value of the Reconstructed Secret Image for some of the test images is tabulated in Table1.



Secret image

Share 1

Share 2

Share 3

Share 4

Image Watermarked with share 1

Image Watermarked with share 1

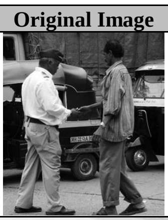
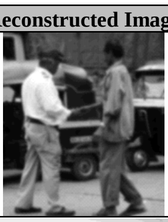
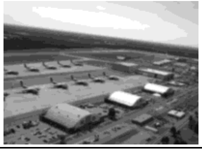
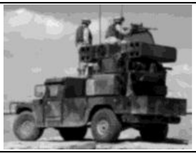
Image Watermarked with share 1

Image Watermarked with share 1

Reconstructed Image

Fig. 1. Experimental results

TABLE I: PSNR OF RECONSTRUCTED IMAGES

Name	Original Image	Reconstructed Image	PSNR(Reconstructed Image)
Bribe.bmp			**54.52**
Hangar.jpg			**48.64**
Humvee.bmp			**60.48**

VIII. CONCLUSION

In this paper, a modified image compression algorithm for still images that have been used to compress different type of images has been introduced. The main advantage of this compression scheme lies in the fact that it is applicable to a wide range of image file types some of which are incompatible with the JPEG compression scheme. Also in in case of Dual-color images this algorithm beats all other algorithms tested. This compression scheme is comparable to the other compression techniques in terms of compression ratio and corresponding quality.

REFERENCES

[1] M. Naor and A. Shamir, Visual Cryptography, "Advances in Cryptography," -EUROCRYPT'94, *Lecture Notes in Computer Science* 950, 1995, pp. 1-12.

[2] P. Tao and A. M. Eskicioglu, "A Robust Multiple Watermarking Scheme in the DWT Domain," Optics East 2004 Symposium, *Internet Multimedia Management Systems V Conference*, Philadelphia, PA, pp. 33-144, October 25-28, 2004.

[3] E. Elbasi and A. M. Eskicioglu, "A Semi-Blind Watermarking Scheme for Color Images Using a Tree Structure," in *proc. of IEEE Sarnoff Symposium*, March, 2006

[4] M. A. Dorairangaswamy, "A Novel Invisible and Blind Watermarking Scheme for Copyright Protection of Digital Images," I*nternational Journal of Computer Science and Network Security (IJCSNS)*, vol. 9, no. 4, pp. 71-78, 2009.

[5] M. A. Dorairangaswamy, "A Robust Blind Image Watermarking Scheme in Spatial Domain for Copyright Protection," *International Journal of Engineering and Technology (IJET)*, vol. 1, no.3, pp. 249 - 255, August 2009.

[6] S. Bhattacharjee, S. Das, D. Roy Choudhury, and P. Pal Chouduri, "A Pipelined Architecture Algorithm for Image Compression," *Proc. Data Compression Conference*, Saltlake City, USA, March 1997.

[7] A. Banerjee and A. Halder, "An Efficient Dynamic Image Compression Algorithm Based on Block Optimization, Byte Compressionand Run-Length Encoding along Y-axis," *IEEE ICCSIT 2010*, Chengdu, China, July 9-11.

[8] A. Halder, S. Dey, S. Mukherjee, and A. Banerjee, "An Efficient Image Compression Algorithm Based on Block Optimization and Byte Compression," I*CISA2010 International Conference*, Chennai Tamil Nadu, February 6.

[9] C. M. Hu and W. G. Tzeng, "Cheating Prevention in Visual Cryptography," *IEEE Transaction on Image Processing*, vol. 16, no. 1, Jan- 2007, pp. 36-45.

[10] A. Halder, D. K. Kole, and S. Bhattacharjee, "On-line Colour *Image Compression based on Pipelined Architecture* ," ICCEE-2009, Dubai, UAE, Dec 28 – 30.

[11] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, Pearson Education, 2002.

[12] T. Acharya and P.-S. Tsai, JPEG2000 Standard for Image Compression.

[13] S. Banerjee, A. Halder, and A. Banerjee "An Efficient Automatic Image Segmentation Algorithm based on Modal Analysis and Mutational Agglomeration," *IEEE ICCCT 2010*, Allahabad, India, September 17-19, pp 216 - 219.

[14] A. Banerjee and A. Halder, "An Efficient Image Compression Algorithm for almost Dual-Color Image Based on K-Means Clustering, Bit-Map Generation and RLE," *IEEE ICCCT 2010*, Allahabad, India, September 17-19, pp 200 - 205.

[15] J. Jiang, Image compression with neural networks -A survey, *Image Communication*, ELSEVIER, vol. 14, no. 9, 1999.

Ayan Banerjee was born in Kolkata, India. He received his Bachelor of Technology (B.Tech) degree, in Information Technology (IT), from West Bengal University of Technology, West Bengal, India, in 2010. Since July 2010, he has been working at Cognizant Technology Solution India, as a Programmer Analyst. His field of research, till date, includes Image Compression, Image Segmentation, Video Compression, Visual Cryptography, Skin Detection and Facial Recognition. He has published five papers in IEEE International conferences and two papers in International Journals, held and published in India, China, Singapore, UAE and USA.