IJCTA, 8(4), 2015, pp. 1511-1519
© International Science Press

Optimal Grayscale Visual Cryptography using Error Diffusion to Secure Image Communication

A. John Blesswin* and G. Selvamary**

Abstract: With the emergence networks, accessing the multimedia information over the network is increased. Hence securing such information is the most important issue in communications. The traditional cryptography techniques encrypt the image, which was more difficult, time-consuming and tedious process. Visual cryptography (VC) is a special type of secret sharing scheme which hides secret images in shares such that, when the shares are superimposed, a hidden secret image is revealed. It does not require complex computational method to decode the secret information. The scope of proposed Optimal Grayscale Visual Cryptography (OGVC) affords a friendly situation to deal with images. OGVC uses two techniques, namely Error Diffusion and inverse halftoning to covert gray scale to binary and vice versa. While sharing the share images, the chance of guessing for an intruder is considerably reducing. Thus it provides an extra layer of security to the images while transferring. The experimental result shows that the proposed OGVC scheme provides robustness, high quality and less computational complexity.

1. INTRODUCTION

Multimedia information sharing over the internet increases vastly. This implies the pressure on securing such information. While securing the information the factors such as size of the information, type of the data and computational complexity are to be considered. Generally images are bigger in size and quantity of data in it. Visual cryptography is the new method to encrypt the image data in a better way. Naor and Shamir [1] scheme describes the principles of Visual Secret Sharing (VSS), as shown in Table 1., to generate two share images by the combinations of black and white pixels according to the secret image. G. Ateniese et al [2] designed a novel technique to bring k out of n visual cryptography schemes but unable to get any secret information by stacking a less number of favorable shares. Wu et al [3] scheme is to share more than one secret image in two random shadows. Ito et al [4] minimized the size of share images, by invariant visual secret sharing scheme. The schemes [1-4] are applied to binary images, which applies to carry out the work of generating shares with higher efficiency.

Table 1
Model of Naor and Shamir [1] scheme

Images	*White Pixel*	*Black Pixel*
Share 1	□■ ■□	□■ ■□
Share 2	□■ ■□	■□ □■
Share 1 × Share 2	□■ ■□	■■ ■■

Wang et al [5] found that the configuration of binary values in the halftone images, which resulted better quality of reconstructed images. Self-verifying visual secret sharing method [6] verifies the reliability of the secret image by halftone logos. Wang et al [7] applied the technique of error diffusion[12] to perform the halftone operation on

* Department of computer science and engineering,

** Department of information technology,

* ** SRM University, India, *Email: wjohnbless@gmail.com*

secret images by deriving the error values and distributed to their adjacent pixels, which increases the reconstructed image clarity. Shyong Jian Shyu [8], proposed minimizing the pixel expansion for a (k, n)-VCS into an integer linear program (ILP), to ensure that the constraints for GVCS can be satisfied. Hodeish [9], proposed a (2,2) VCS where two adjacent pixels are taken together as the one time input for generation of shares. Fatahbeygi [10], explains a master share that is constructed according to the block classification results and then owner share is generated by comparing master share together with binary watermark.

2. MATERIALS AND METHODS

The phases of the proposed system are explained in this section. The proposed system consists of two phases; Firstly, Share construction phase in which two shares S1 and S2 are generated from the given input image and two cover images. Secondly, in Revealing phase, the two share images SH1 and SH2 are generated from the shares S1 and S2 respectively. A reconstructed image is revealed by stacking the two share images using XOR operation.

The share images look like natural images, individual share image does not reveal any information about the secret pixels. To create this confusion to the intruder, share images will show that one cover image hides the other cover image. The chances of guessing the presence of secret image will be significantly reduced. In the proposed system, Halftoning process is done by Floyd Steinberg error diffusion technique [12] to convert the gray scale image into halftone image HI. The HI is given to the share construction phase to generate shares. In the revealing phase, reconstructed gray scale image GI' is obtained by inverse halftoning technique [11]. Block diagram of the proposed system is shown in Fig.1.

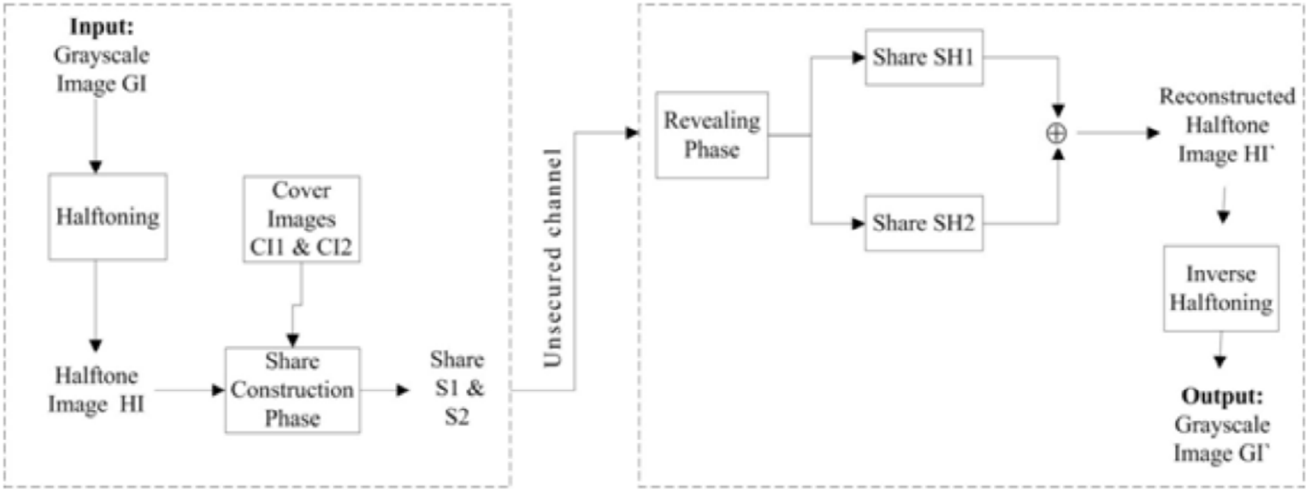


Figure 1: Block diagram of proposed scheme

3. SHARE CONSTRUCTION PHASE

Step 1. Consider a m × n secret grayscale image (GI) and two natural grayscale images as cover images (1); then

$$GI_{i,j} \in \{0,1,2,3\ldots,255\}$$

$$CI1_{i,j} \in \{0,1,2,3\ldots,255\}$$

$$CI2_{i,j} \in \{0,1,2,3\ldots,255\} \tag{1}$$

where *i* and *j* are varying from 1 to m × n.

Step 2. Generate a halftone image HI by applying the Error Diffusion (ED) technique on GI (2);

$$HI_{i,j} \in \{0,255\} \quad \leftarrow \quad ED(GI_{i,j}) \tag{2}$$

Step 3. Construct the shares $S1_{ij} \in \{0, 1, 2, 3 ..., 255\}$and $S2_{ij} \in \{0, 1, 2, 3 ..., 255\}$from HI by using SHARE_CONST algorithm; now, shares $S1$ and S2 will have the pixel expansion of 3 and also assures that the secret information can be completely restored after stacking from the shares. Shares are delivered to the receiver. Fig. 2 explains the share construction phase.

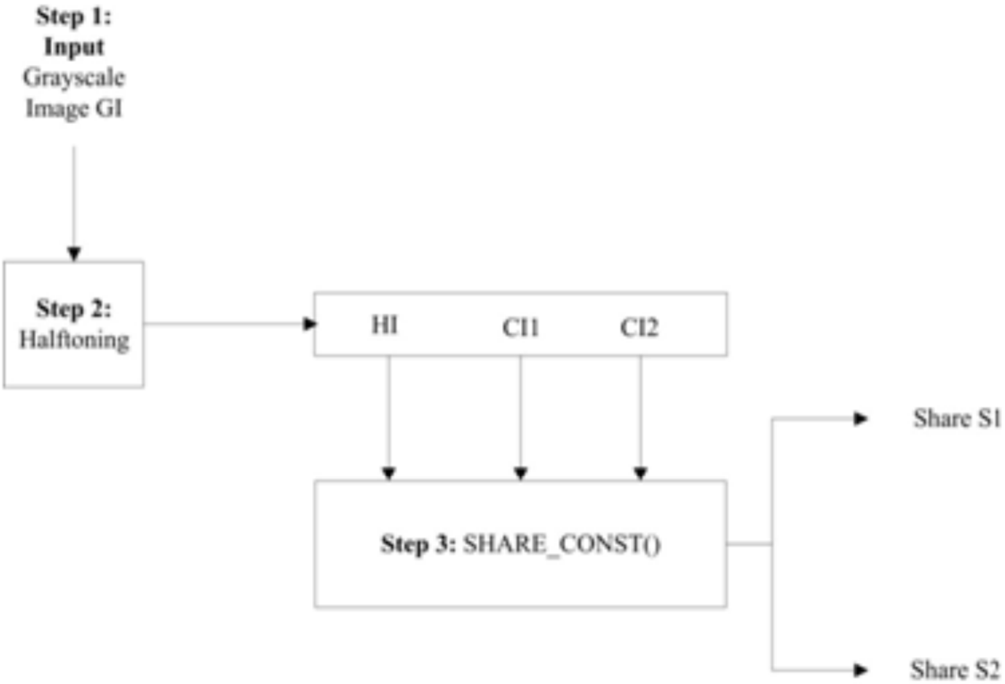


Figure 2: Share Construction Phase

Algorithm:

For given matrices CI^1, CI^2 and HIof size ($m \times n$).

Let shares S^1 and S^2 be empty as size of $m \times 3n$.

```
procedure SHARE_CONST (HI, $CI^1{}_{,}CI^2$)
    for $i$ = 1 to $m$ do
        for $j$ = 1 to $n$ do
            $PA_{i,j} \leftarrow AVG\ (CI1_{i,j} + CI2_{i,j})$
            if $HI_{i,j}$ = = 255 then
                $Wa \leftarrow [PA_{i,j}, PA_{i,j}-1, PA_{i,j}, PA_{i,j}-1]$
                $Wb \leftarrow [\ PA_{i,j}-1, PA_{i,j}, PA_{i,j}-1, PA_{i,j}]$
                $Pi \leftarrow$ RANDOM(Wa,Wb)
            end if
            if $HI_{i,j}$ = = 0 then
                $Ba \leftarrow [PA_{i,j}, PA_{i,j}-1, PA_{i,j}-1, PA_{i,j}]$
                $Bb \leftarrow [PA_{i,j}-1, PA_{i,j}, PA_{i,j}, PA_{i,j}-1]$
                $Pi \leftarrow$ RANDOM(Ba, Bb)
            end if
            $S^1_{(i,3*j-2)} \leftarrow CI1_{i,j}$
            $S^1_{(i,3*j-1)} \leftarrow Pi(1)$
            $S^1_{(i,3*j)} \leftarrow Pi(2)$
            $S^2_{(i,3*j-2)} \leftarrow CI2_{i,j}$
            $S^2_{(i,3*j-1)} \leftarrow Pi(3)$
            $S^2_{(i,3*j)} \leftarrow Pi(4)$
        end for
    end for
end procedure
```

4. REVEALING PHASE

Step 1. Let the share images $S1_{ij} \in \{0, 1, 2, 3 ..., 255\}$and $S2_{ij} \in \{0, 1, 2, 3 ..., 255\}$

Step2. The share images $SH1_{ij} \in \{0, 1, 2, 3 ..., 255\}$and $SH2_{ij} \in \{0, 1, 2, 3 ..., 255\}$ can be derived from $S1_{ij}$, $S2_{ij}$ using SHARE_REVEAL algorithm. Now, SH1 and SH2 have the pixel expansion of 2 as of GI.

Step 3. To generate the reconstructed Halftone Image HI’, digitally stacking the share images SH1, SH2 by XOR operation.

Step 4. The inverse halftoning technique is applied to HI’ to generate the reconstructed Gray scale Image GI’.

However, HI extracted during the revealing phase could be either an original image or a noise-like image depending on whether the received shared images are original or fake.

Let d is the difference between the GI and GI’, d=GI-GI’. If the value of d is equal to zero, it implies that the GI is completely restored from HI’ by inverse halftoning technique [11].

This method can be expanded to color images. First, divide the color image (RGB) into three individual images: Red(R), Green (G) and Blue(B). Then, the method is applied separately to each individual image, independently. Finally, the reconstructed secret color is generated by stacking the three reconstructed channels together.

Algorithm:

For given matrices S^1, S^2 of size ($m \times n$).

Let shares SH^1 and SH^2 be empty as size of $m \times n/3$.

```
    procedure SHARE_REVEAL ($S^1$,$S^2$)
        for $i = 1$ to $m$ do
            for $j = 1$ to $n$ do
                R1= $S^1_{(i,3*j-1)} - S^1_{(i,3*j)}$
                R2= $S^2_{(i,3*j-1)} - S^2_{(i,3*j)}$
                If (R1==1and R2==1)
                    $SH^1_{i,(2*j-1)}$=255
                    $SH^1_{i,(2*j)}$=0
                    $SH^2_{i,(2*j-1)}$=255
                $SH^{2}_{i,(2*j)}=0$
            else if(R1==-1and R2==-1)
                $SH^{1}_{i,(2*j-1)}=0$
                $SH^{1}_{i,(2*j)}=255$
                $SH^{2}_{i,(2*j-1)}=0$
                $SH^{2}_{i,(2*j)}=255$
            else if(R1==1and R2==-1)
                $SH^{1}_{i,(2*j-1)}=255$
                $SH^{1}_{i,(2*j)}=0$
                $SH^{2}_{i,(2*j-1)}=0$
                $SH^{2}_{i,(2*j)}=255$
            else if(R1==-1and R2==1)
                $SH^{1}_{i,(2*j-1)}=0$
                $SH^{1}_{i,(2*j)}=255$
                $SH^{2}_{i,(2*j-1)}=255$
                $SH^{2}_{i,(2*j)}=0$
        end for
    end for
    RI=BITXOR($SH^{1}$, $SH^{2}$)
end procedure
```

EXPERIMENTAL RESULTS

Experimental results demonstrate on three objectives. First, robustness of the algorithm; secondly, construct the original secret image with high quality and lastly, less computational time. The proposed OGVC allows no limitation on the size of the secret images. The set of test images shown in Fig. 3 illustrates that OGVC can perform well on grayscale images. The set contains eight 512 × 512 grayscale images: Apple, Batman, BMW, Motorola, Number, SRM, Twitter and YouTube. The efficiency of the proposed method outlined in this paper is tested by coding and running the algorithm in MATLAB 7.10 Tool. The image quality measures [13] such as Peak Signal to Noise Ratio (PSNR),Mean Absolute Error (MAE)Structural Similarity Index (SSIM)and Normalized Correlation (NC) are evaluated between reconstructed images and original secret images using following equations;

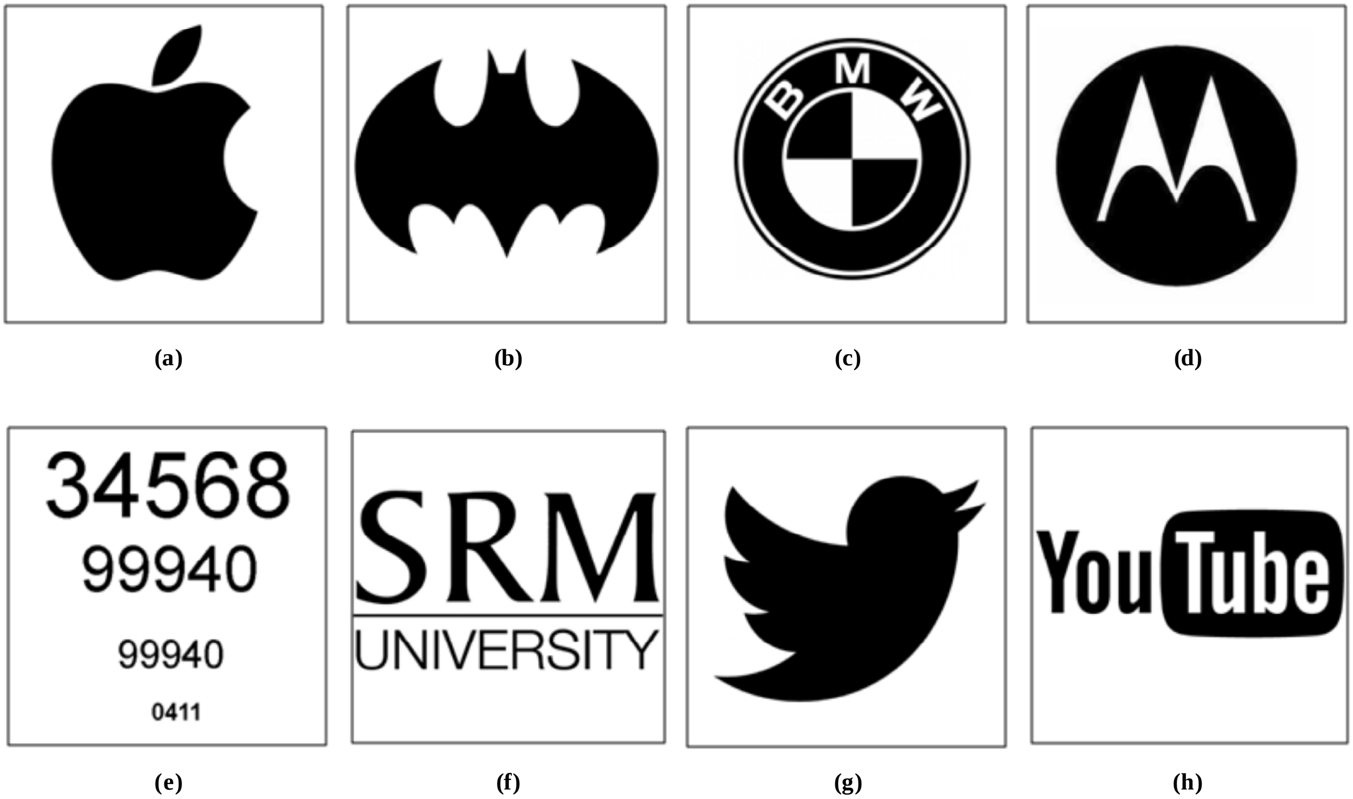
Peak Signal to Noise Ratio (PSNR): It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is expressed in terms of the logarithmic decibel is given by (3),

$$PSNR = \log\frac{(2^{n}-1)^{2}}{MSE} \tag{3}$$

Mean Absolute Error (MAE): It is a capacity used to measure how nearby predictions are to the eventual consequences. The mean absolute error is given by (4),

$$MAE = \frac{1}{n}\sum_{i=1}^{n}\left| f_i - y_i \right| = \frac{1}{n}\sum_{i=1}^{n}\left| e_i \right| \tag{4}$$

Here, mean absolute error is an average of the absolute errors $e_i = |f_i - y_i|$, where f_i is the prediction and y_i the true value.



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig 3. Eight 512 × 512 images
(a) Apple (b) Batman (c) BMW (d) Motorola (e) Number (f) SRM (g) Twitter and (h) YouTube

Structural Similarity Index (SSIM): It measures the similarity of two images, based on an initial uncompressed or distortion-free image (5).

$$SSIM(x, y) = \frac{2 \times \mathrm{m}_1(\mathrm{P}) \times \mathrm{m}_2(\mathrm{P}) + \mathrm{C}_1}{\mathrm{m}_1(\mathrm{P})^2 + \mathrm{m}_2(\mathrm{P})^2 + \mathrm{C}_1} \times \frac{2 \times \mathrm{c}(\mathrm{P}) + \mathrm{C}_2}{\mathrm{s}_1(\mathrm{P})^2 + \mathrm{s}_2(\mathrm{P})^2 + \mathrm{C}_2} \tag{5}$$

Where m_1(P) and m_2(P) are mean values, s_1(P) and s_2(P) are standard deviations of seq1 and seq2, c(P) is the covariance between seq1 and seq2 computed over the same window, C_1 = (K1*L)^2: regularization constants, C_2 = (K2*L)^2, K1, K2: regularization parameters, L = 255 and the default window is a Gaussian window with standard deviation 1.5 along both the X and the Y axis.

Normalized Correlation (NC): It measures the similarity representation between the original image and decrypted image (6).

$$NC = \frac{\Sigma_{i=1}^{M}\Sigma_{j=1}^{N}(I[i, j]I'[i, j])}{\Sigma_{i=1}^{M}\Sigma_{j=1}^{N}(I[i, j])^2} \tag{6}$$

Where $I(i, j)$ is original image and $I'(i, j)$ is decrypted image, M is height of image and N is width of the image.

Table 2
Statistical analysis

Image	*PSNR*	*MAE*	*SSIM*	*NC*
Apple	+32.45	0.25	0.92	0.98
Batman	+29.84	0.41	0.87	0.97
BMW	+24.57	1.28	0.756	0.91
Motorola	+24.54	1.27	0.73	0.92
Number	+25.09	0.94	0.87	0.82
SRM	+23.88	1.40	0.79	0.84
Twitter	+30.92	0.34	0.89	0.98
YouTube	+27.90	0.61	0.83	0.95

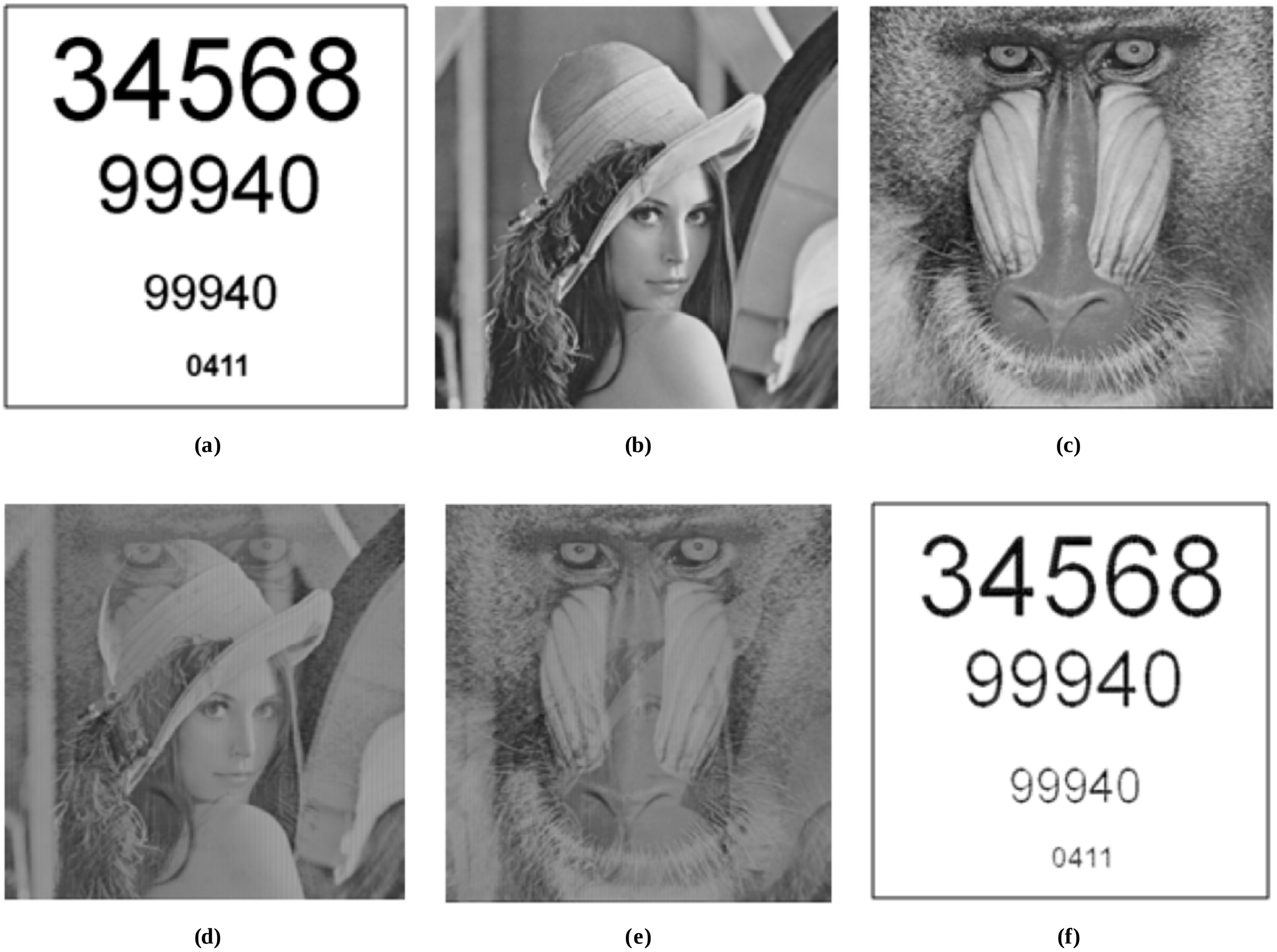
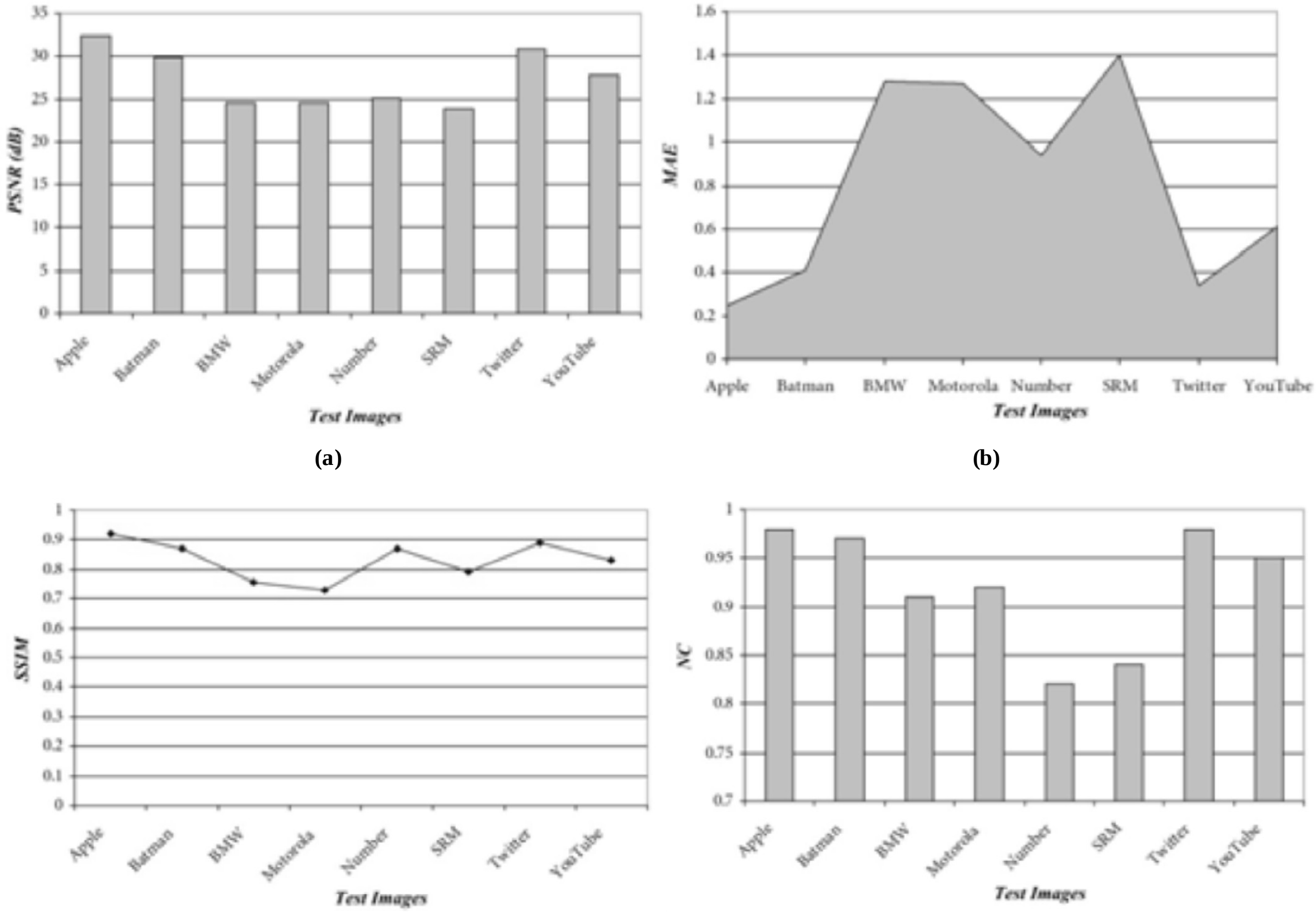


Figure 4: (a) Secret image, Number (b) Cover image, Lena (c) Cover image, Baboon (d) Share1 (e) Share2 (f) Reconstructed secret image, Number

Fig.4(a), 4(b), 4(c), 4(d), 4(e) and 4(f) shows secret image Number, cover images Lena and Baboon, Share1, Share2 and reconstructed secret image number. Share images are looking completely different from secret image; therefore, this method can show the robustness.

The graph representation of the various image quality measures shown in Fig. 5. The PSNR values of the reconstructed secret images and the original images range from 23.88 to 32.45 dB. From the obtained PSNR, MAE, SSIM and NC values [13], the quality of the reconstructed grayscale image is maintained as original secret image.



(a) (b)

(a) (b)

Figure 5: Graph representation of reconstructed image quality measures (a) PSNR (b) MAE (c) SSIM (d) NC

Table 3
Computational analysis

Images	*Execution time(Seconds)*
Apple	8
Batman	7
BMW	9
Motorola	7
Number	8
SRM	9
Twitter	8
YouTube	7

The Table 3 shows the time taken to execute the algorithm on different images and the result shows that the method is less computational and efficient.

CONCLUSION

The Proposed OGVC, which uses the error diffusion. The use of error diffusion technique improves the quality of encrypted image and decrypted image. The proposed method helps to generate high quality share images. An individual shares does not show the secret information. Future studies should therefore investigate on 3D visual secret sharing with higher visual quality of the reconstructed secret images.

References

[1] M. Naor and A. Shamir, "Visual cryptography", *Proc. Advances in Cryptology (Eurprocrypt'94)*, pp.1 -12, 1994.

[2] G. Ateniese, C. Blundo, A. DeSantis, D. R. Stinson, Visual cryptography for general access structures, *Proc. ICALP 96*, Springer, Berlin, pp. 416-428, 1996.

[3] C.C. Wu, L.H. Chen, *A Study On Visual Cryptography*, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, R.O.C, 1998.

[4] R. Ito, H. Kuwakado, H. Tanaka, Image Size Invariant Visual Cryptography, *IEICE Transactions on Fundamentals*, Vol. E82-A, No. 10, pp. 2172-2177,1999.

[5] Zhongmin Wang, Gonzalo R Arce and Giovanni Di Crescenzo, Halftone Visual Cryptography Via Direct Binary Search, *14th European Signal Processing Conference*, Florence, Italy, 2006.

[6] Chin-Chen Chang, Chia-Chen Lin, Le, T.H.N, Hoai BAC Le, Self-Verifying Visual Secret Sharing Using Error Diffusion and Interpolation Techniques,*IEEE Information Forensics and Security*, Issue Date: Dec. 2009, Volume: 4 Issue: 4 on page(s): 790 - 801, 2009.

[7] Zhongmin Wang, Gonzalo R. Arce and Giovanni Di Crescenzo, Halftone Visual Cryptography Via Error Diffusion, *Information Forensics and Security IEEE*, Issue Date: Sept, Volume: 4 Issue:3, On page(s): 383 – 396, 2009

[8] Shyong Jian Shyu, Ming Chiang Chen, Minimizing Pixel Expansion in Visual Cryptographic Scheme for General Access Structures, Circuits and Systems for Video Technology, IEEE Transactions on Volume: 25, Issue: 9, 2015.

[9] Hodeish,Humbe, A (2, 2) secret sharing scheme for visual cryptography without Pixel Expansion, Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015.

[10] Fatahbeygi, A., Akhlaghian, F.,A new robust semi-blind image watermarking based on block classification and visual cryptography Pattern Recognition and Image Analysis (IPRIA), 2015.

[11] K. L. Chung and S. T. Wu, "Inverse halftoning algorithm using edge based lookup table approach," IEEE Trans. Image Process., vol. 14, no.10, pp. 1583–1589, Oct. 2005.

[12] R. W. Floyd and L. Steinberg, "An adaptive algorithm for spatial gray scale," Proc. Soc. Image Display, vol. 17, no. 2, pp. 75–77, 1976.

[13] A. John Blesswin, P.Visalakshi, "A Novel Visual Image Confirmation (VIC) Protocol Using Visual Cryptography for Securing Ubiquitous Bluetooth Mobile Communications", Research Journal of Applied Sciences 9(8): 503-510, 2014.