

ANAGLYPH 3D IMAGE ENCRYPTION USING MULTIPLE MEANINGFUL SECRET HIDING SCHEME AND MODIFIED ERROR DIFFUSION

Joseph James S* Haribaabu V* Manikandan K* and Selvakumara Samy S*

Abstract: Visual cryptography is a method in which decryption is performed with less computational devices or human visual system. In the traditional visual cryptography scheme, one secret image is divided into two shares so that by stacking the two shares secret image appears. Drawback of this scheme is more number of shares to hide one secret image. This paper presents a new scheme for hiding multiple color secret images into meaningful color cover images. Meaningful shares generation requires less number of cover images than the secret image which reduces the storage space, more desirable for security and less vulnerable to attack. This paper also provides a scheme to create meaningless shares to encrypt multiple secrets and combines the use of anaglyph 3D images and modified halftone error diffusion process for encryption. Anaglyph image gives dual edges and improves perception ability of human visual system and Modified halftone error diffusion process produces the halftone image more similar to original grayscale image.

Keywords: Visual Cryptography, Halftone , Multi Secret Sharing, Meaningful Shares, Anaglyph 3D image.

1. INTRODUCTION

The rapid growth in the information technology, Internet, mobile communication, and Digital multimedia applications has opened new opportunities in scientific and commercial applications that involve large volume of digital data including military application. But this progress has also led to many serious security problems such as hacking, duplications and misuse of data by unauthorized people. Now a day's security of data is a big issue. There are many schemes available to deal with this security problem. Among the existing methods the Visual cryptography Scheme (VCS) is a simple and an emerging cryptographic technology which uses the characteristics of human visual system to encrypt and decrypt images without involving complex computation. Being a type of secret sharing scheme, visual cryptography can be used in a number of applications such as credit card transaction, biometric image authentication and secure storage and transmission of secret messages.

Naor and Shamir proposed the basic model of visual cryptography [1] for binary images. In a K-out-of-N scheme of VC, a secret binary image is cryptographically encoded into N shares of random binary patterns. The N shares are Xeroxed onto N transparencies, respectively, and distributed amongst participants, one for each participant. No participant knows the share given to another participant. Anyone or more participants can visually reveal the secret image by superimposing any K transparencies together. The secret cannot be decoded by any K-1 or fewer participants; even if strong computational power is available with them. This scheme restricted to only binary images. VC for grayscale images [3][6] uses the halftone technique to convert multi-level pixel value into binary image values. Halftone technique [2] with error diffusion to convert grayscale into binary image provides pleasing and more similar halftone image as original image.

* Assistant Professor, SRM University,
Email: Josephjames.s@ktr.srmuniv.ac.in¹, Haribaabu.v@ktr.srmuniv.ac.in², manikandan.k@ktr.srmuniv.ac.in³,
selvakumarasamy.s@ktr.srmuniv.ac.in⁴

VC scheme for color images [3][5] separates the color channels which are grayscale passes through halftone process to get binary image. Classical VC scheme [1] applied to generate shares. The shares are stacked together to create color share. Secret hiding through meaningful image [8] uses cover image and its complimentary image. For decryption shares are stacked together, the complementary pixel value become zero, whereas other pixels reveals secret image. Extended VC scheme [4] provides a method to hide a secret through meaningful cover shares with threshold decryption. All these schemes restricted to hide a single secret image and pixel expansion to generate shares which requires more space to store a single secret image shares. Multiple secret sharing scheme [9][12] uses classical VC scheme to generate meaningless shares to hide multiple secrets. Shares are constructed based on angle of rotation of classical VC shares. Multiple secret hiding through meaningful cover image [11] hides secrets through mask constructed using meaningful cover image. Mask is common for all secrets. Without mask we cannot retrieve any secrets. All the above mentioned methodologies could hide one or two binary or grey scales images. More than two color secrets were not retrieved. In this paper, we propose a method capable of retrieving multiple color secrets with enhanced quality.

2. RELATED WORK

The classical (2, 2) VC scheme [1] for binary image share construction is illustrated in Fig.1. In black-and-white (2, 2) visual cryptography decomposes every pixel in a secret image into a 2x2 block in the two transparencies according to the rules given in figure 1, two of them black and white















Secret Image	Share 1	Share 2	Stacked Image
 White pixel			
 Black Pixel			
			
			

Figure 1. Classical (2, 2) VC Scheme construction.

For a pixel in secret image one of the above four rows corresponding to black and white of figure 1 is chosen to generate Share1 and Share2. Therefore, when stacking two transparencies the blocks corresponding to black pixels in the secret image are full black and those corresponding to white pixels are half-black-and-half-white. As a concern to information security, one of the two rows is selected with equal probability. In the decryption process the two shares are stacked together (OR operation) to recover the secret image. If all corresponding pixels are black then the stacked result is black (=0). If at least one pixel color is white (=1), the stacked result pixel is white (=1).The number of share can be generated depends on the rows of basic matrices. One secret pixel is replaced by four pixels in shares. So sizes of the shares are two times larger than secrets. The above process is illustrated in Fig.2. (a)- (d).

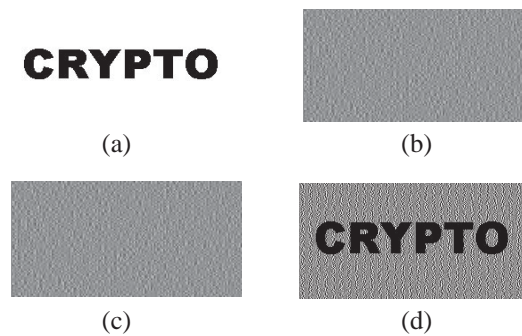


Figure 2 (a) Binary secret image. (b) Encrypted share 1. (c) Encrypted share 2. (d) Reconstructed image.

3. THE PROPOSED SCHEME

This paper provides two schemes to encrypt secret images through meaningless and meaningful share generation. In both the schemes certain changes are introduced for the quality enhancement of images explained in detail in the following section C and D. The schematic diagram of the proposed method is shown in Figure 4 and Figure 7.

3.1 2D image into Anaglyph 3D image

Anaglyph 3D is the name given to the stereoscopic 3D effect achieved by means of encoding each eye's image using a filter of different colors such as red and cyan. Anaglyph 3D images contain two differently filtered colored images, one for each eye. When viewed through the color-coded anaglyph glasses, each eye image reaches one eye, revealing an integrated stereoscopic image.

The input 2D color image is duplicated, both images are separated into RGB (Red, Green and Blue) and CMY (Cyan, Magenta and Yellow) color channels. The CMY model can also be created by using the RGB color model by making appropriate color channels zero. For example, making the red channel zero in RGB will provide a cyan image. Red and cyan channels are taken out and these two images are superimposed (sum the corresponding pixel values in both images) with some pixel difference to produce an anaglyph 3D effect.



Figure 3. (a) 2D image



Figure 3. (b) Anaglyph 3D image

Anaglyph images provide double edges which increase the sustainability of edges during the halftone process, thereby increasing the perception of the human visual system. When these are viewed through filter glasses, they provide an exact stereoscopic effect.

3.2. Modified Halftone Error Diffusion Process

Halftone Technique

The halftone method transforms grayscale image into binary image that uses the density of the net dots to simulate the gray level is called “Halftone”. Every pixel of the transformed halftone image has only two possible color levels (black or white). Because human eyes cannot identify too tiny printed dots and, when viewing a dot, tend to cover its nearby dots, we can simulate different gray levels through the density of printed dots, even though the transformed image actually has only two colors—black and white. This halftone process produces more quantization error, these errors should be diffused to neighboring pixels to get good quality halftone image. Out of the well known error filters Floyd-Steinberg, Jarvis and Stucki, better results are produced by Floyd-Steinberg error filter.

Modified Error Diffusion

Floyd-Steinberg standard error diffusion [2] uses constant threshold 127.5 which is middle value of 0-255 grayscale image pixel values. Error calculation and error diffusion are performed based on following mathematical expression.

$$\begin{aligned}
 HI(x, y) &= \begin{cases} 255, & \text{if } GI(x, y) \geq TH \\ 0, & \text{Otherwise} \end{cases} \\
 E(x, y) &= GI(x, y) - HI(x, y) \\
 GI(x, y+1) &= \frac{GI(x, y+1) + 7 * E(x, y)}{16} \\
 GI(x, y,1) &= \frac{GI(x+1, y) + 5 * E(x, y)}{16} \\
 GI(x+1, y-1) &= \frac{GI(x+1, y-1) + 3 * E(x, y)}{16} \\
 GI(x+1, y+1) &= \frac{GI(x+1, y+1) + 1 * E(x, y)}{16}
 \end{aligned}$$

Where $GI(x, y)$ pixel in grayscale image, $HI(x, y)$ pixel in halftone image, $E(x, y)$ quantization error and TH Threshold value. If the grayscale pixel value is larger than threshold, 255 will be placed in the corresponding halftone image. Otherwise 0 will be placed. The quantization error $E(x, y)$ will be calculated based on formula given and those errors are diffused to neighboring pixels. The quantization errors diffused into neighboring pixel in the ratio of 7/16, 1/16, 5/16, 3/16. The above are modified to produce better halftone image than the existing one.

We know in the above scheme, a better halftone image are produced, in our work by introducing certain changes in, (i) threshold for halftone process, (ii) ratio of quantization error diffusion, obtained further improvement in the halftone images. In this new scheme, first one is image self dependent threshold for halftone process. Threshold is calculated based on middle value of mean of pixel values of an image. Second, the ratio of quantization error diffusion coefficients are changed to 6/16, 2/16, 4/16, 4/16 from Floyd and Steinberg error diffusion. These values are obtained from the experimental results of standard test images. This modified error diffusion process reduces quantization error thereby reasonably improves PSNR values of halftone image.

3.3 Scheme1: Meaningless Share Construction

This scheme hides three secret images using three meaningless share generation. In decryption process, two share are stacked to get temporary share. Stacking share1 and temporary share reveals first secret. Rotating

share1 to 90° clockwise(CW) then stack with temprary share reveals second secret. Rotating share1 to 90° counter clockwise(CCW) then stack with temprary share reveals third secret.The schematic diagram of this method is shown in **Figure 4**. Each pixel from the secret is replaced by a matrix of size 2X2 in shares. So the shares generated are two times larger than secret image.

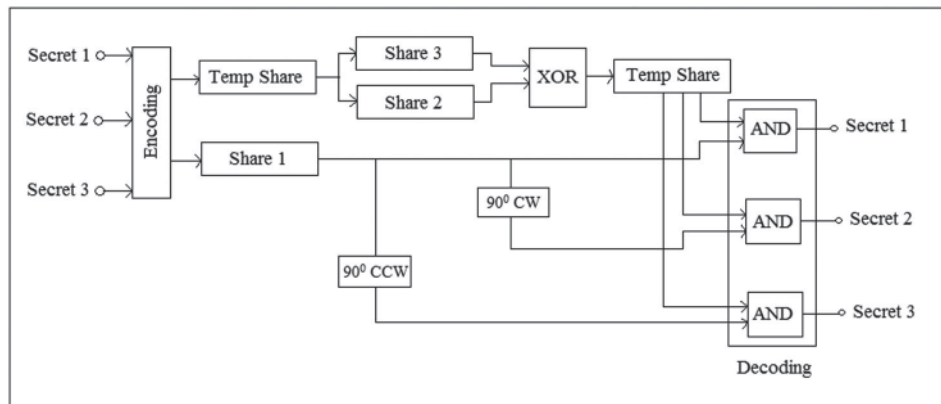


Figure 4. Schematic diagram of proposed meaningless share construction

Color secret images are passed through edge enhancement filter to sharpen edges to reduce destruction of edges during halftone process. Then the color 2D images are converted into anaglyph 3D images and separated into RGB color channels. Secret image1 is converted into three channel images SR1 (Red), SG1 (Green), and SB1 (Blue). Similarly Secret2 and Secret3 are converted into three channel images SR2, SG2 and SB2, SR3, SG3, SB3 respectively. Modified halftone error diffusion is applied to all nine channel images. Thus halftone images HSR1, HSG1, HSB1, HSR2, HSG2, HSB2 HSR3, HSG3 and HSB3 are generated. HSR1, HSR2 and HSR3 are processed based on the following pixel pattern given in Fig.5 and two final shares FSR1 and FSRTemp are obtained. To split the share Temp into two shares FSR2 and FSR3, the coding rules are designed carefully. Splitting the share FSRTemp into two shares should be, such that the original share (FSRTemp) is reproduced when two shares (FSR2 and FSR3) stacked together. To reproduce FSRTemp from FSR2, FSR3 XOR logical operation is used.

Similarly HSG1,HSG2,HSG3 and HSB1,HSB2,HSB3 processed using the code pattern and final share FSG1,FSG2,FSG3 and FSB1,FSB2,FSB3 are generated respectively.Merging FSR1,FSG1and FSB1 we get FS1. Similarly by merging FSR2, FSG2, FSB2 and FSR3, FSG3, FSB3 we get FS2 and FS3 respectively. FS1, FS2 and FS3 are the final shares obtained. Thus the color shares generated (FS1, FS2 and FS3) are meaningless. Shares generated based on the following code pattern shown in Figure 5.

Pixel of first secret image	W	W	W	W	B	B	B	B
Pixel of second secret image	W	W	B	B	W	W	B	B
Pixel of third secret image	W	B	W	B	W	B	W	B
2x2 block of share1								
2x2 block of share 2								

Figure 5. Pixel code pattern for encryption

In decryption process, color meaningless shares are converted into color channels R1, G1, B1, R2, G2, B2 and R3,G3,B3.Stacking R2and R3 will give RTemp.By stacking R1 and RTemp as such Red channel of first secret(SR1) will revealed. Rotating R1 by 90° clockwise and stacking with RTemp will reveal Red channel of second secret (SR2). Rotating R1 by 90° anti-clockwise and stack with RTemp will reveal Red channel of third secret(SR3).Similarly performing decryption on G1,G2 and B1,B2 will reveal secret color channels SG1,SG2,SG3 and SB1,SB2,SB3 respectively. By merging SR1, SG1 and SB1 color channels we will get the original color secret image1.Similarly secret2 and secret3 can be obtained from corresponding color channels. Each pixel is substituted by 4 pixels in the shares. The shares generated are twice the size of the input color secrets.

3.4 Scheme2: Meaningful Share Construction

In this method, four secret images are encrypted using three meaningful cover images. Generated shares will look like cover images. Secrets will be revealed only when shares are stacked together.Secret1 will be revealed by stacking share1 and share2.Rotating share1 by 90° CCW and stack with share2 will reveal secret 2.Third secret will be revealed by stacking share2 and share3.Rotating share2 by 90° CCW and stack with share3 will reveal secret4. Share1 and share2 are created by referring the pixel values of secret1, secret2, cover1 and cover2 in the corresponding pixel positions.Share3 is constructed by referring the pixel values of share2, secret3, secret4 and cover3 in the corresponding pixel position. The shares are twice the size of secret image. Each pixel in secret is replaced with 2x2 pixel block in shares. Schematic diagram of this method is shown in figure 7.

Input color secret and cover images are converted into anaglyph 3D images and then separated to RGB color channels. Cover images are used for generating meaningful shares. As a result we will get seven Red, seven Green and seven Blue channel images. Encryption is carried out on single color channel of 4 secrets and 3 cover images at the same time. Let SR1, SR2, SR3, SR4, CR1, CR2 and CR3 are Red channels of secrets and cover images respectively. Modified halftone error diffusion applied on these and halftone images HSR1, HSR2, HSR3, HSR4, HCR1, HCR2 and HCR3 are obtained.

To proceed further before encryption, we first define two different pattern groups, namely, P_b, P_w , to be used during share generation process. Pattern groups are the basic constituents of the shares. There are one white and three black pixels in each pattern of the P_b , and two white and two black pixels in P_w which results in six different combinations for P_w and four different combinations for P_b exist. Possible combination of extended blocks in P_b, P_w is shown Figure.6.

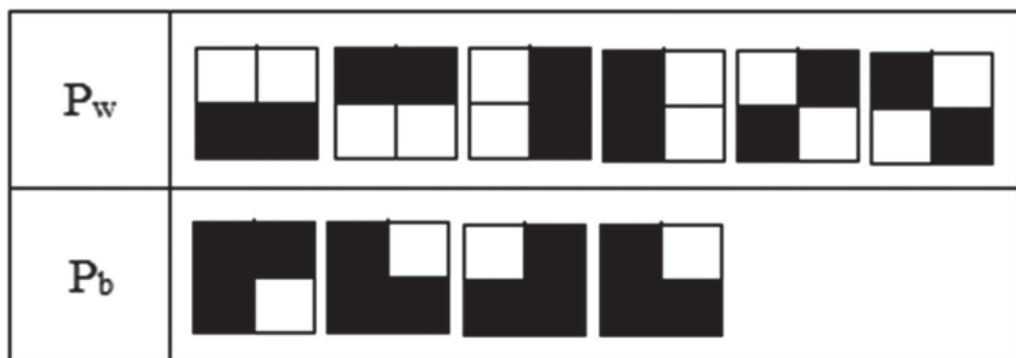


Figure 6. Pixel pattern for Black and White

Each extended block of shares is filled according to these patterns by checking the corresponding pixels of both cover images. For instance, if the cover-image pixel value is black, then the extended block type in a share can be selected from P_b . Otherwise, block type is determined among the patterns in P_w .

This will guarantee generation of meaningful shares at the cost of reduced contrast of cover images. The proposed secret hiding scheme through meaningful share encryption and decryption is shown in Fig.7.

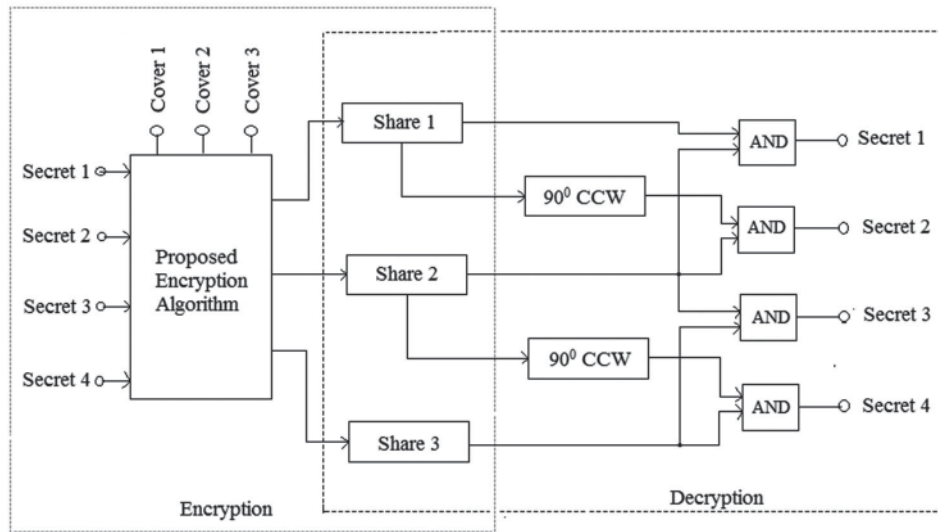


Figure 7. Proposed meaningful share scheme encryption and decryption

3.5 First Share Construction

Let A, B and C be first, second and third share and a, b and c are extended blocks of A, B and C respectively. $S_1, S_2, C_1,$ and C_2 are pixel value of HSR1, HSR2, HCR1 and HCR2 respectively shown in Figure 9. Let A1 be the 90° CCW rotated image of A. A should reveal second secret when it is rotated 90° CCW and stacked with share2. So the pixel values of A is determined by considering corresponding pixel values in A1. Here pixel processing starts at first row (1,1) then the next pixel position to be processed is the place where (1,1) will be in A1 when A is rotated 90° CCW. In each iteration four pixels will be processed shown in Fig.8.(1)-(3). Next iteration starts at second row and goes row by row.

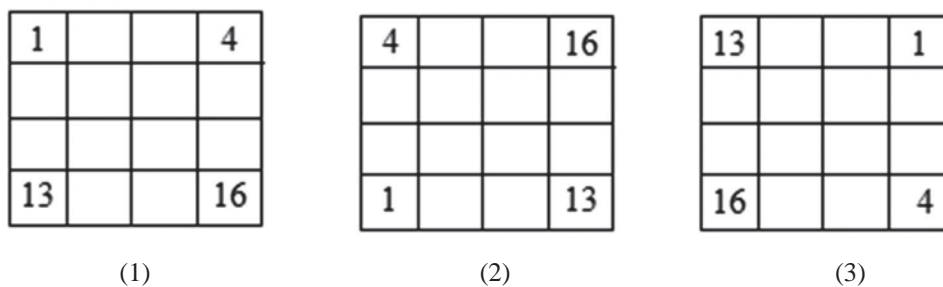


Figure 8. Pixel sequence of A (1) Original pixel position (2) After rotating 90° CCW (3) After rotating 90° CW

During each iteration, first extended block (a) of A can be selected randomly based on cover image pixel value, then extended block of A1 (a1) can be determined based on the rule set. The rule set can be defined as follows by using the pixel values at secret images and cover images. Which pattern group P_b or P_w to be tested with this rule set is determined by the corresponding pixel value at first cover image. Hamming weight of the OR'ed vectors a and b is denoted by $H(OR(a, a1))$, like the hamming weight of AND'ed vectors that denoted by $H(AND(a, a1))$

Rule 1. If S_1 is black, S_2 is black, $H(OR(a, a1))$ is less or equal to 3, and $c2$ is black, then it is an appropriate pattern.

Rule 2. If S_1 is black, S_2 is black, $H(\text{OR}(a, a1))$ is less or equal to 2, and $c2$ is white, then it is an appropriate pattern.

Rule 3. If S_1 is white, S_2 is white, $H(\text{AND}(a, a1))$ is greater or equal to 1, and $c2$ is black, then it is an appropriate pattern.

Rule 4. If S_1 is white, S_2 is white, and $c2$ is white, then it is an appropriate pattern.

Rule 5. If S_1 is white, S_2 is black, and $H(\text{XOR}(a, a1))$ is greater than 1, then it is an appropriate pattern.

Rule 6. If S_1 is black, S_2 is white, and $H(\text{XOR}(a, a1))$ is greater than 1, then it is an appropriate pattern.

The $a1$ value placed in the rotated pixel position in $A1$ and corresponding position extended block of A will be determined. Likewise all secret image pixels are processed and corresponding extended blocks of A and $A1$ are determined. This process continued for all pixel values of secrets $HSR1$, $HSR2$ and cover images $HCR1$, $HCR2$. Now Red channel of two meaningful shares are created.

3.6 Second Share Construction

Extended blocks of second share are determined based on extended blocks of A , $A1$ and pixel values of secrets $HSR1$, $HSR2$ and second cover $HCR2$. Relative pixel values at two secret images must be obtained when b is stacked with a and $a1$, respectively. Therefore, b should be selected according to both a and $a1$. Appropriate patterns for b can be selected among the patterns at P_b or P_w shown in Figure 6. Relative pixel value at the second cover image determines pattern group to be used in order to create shares that look like cover images.

Initially all patterns that belong to a selected pattern group (P_b or P_w) are candidate for b . Only a set of appropriate patterns could reveal original pixel values of both secret images. A rule base is defined to find this appropriate pattern set as follows.

Rule 1. If S_1 is black, S_2 is black, $H(\text{AND}(a, b))$ is 0, and $H(\text{AND}(a1, b))$ is 0, then it is an appropriate pattern.

Rule 2. If S_1 is black, S_2 is white, $H(\text{AND}(a, b))$ is 0, and $H(\text{AND}(a1, b))$ is not 0, then it is an appropriate pattern.

Rule 3. If S_1 is white, S_2 is black, $H(\text{AND}(a, b))$ is not 0, and $H(\text{AND}(a1, b))$ is 0, then it is an appropriate pattern.

Rule 4. If S_1 is white, S_2 is white, $H(\text{AND}(a, b))$ is not 0, and $H(\text{AND}(a1, b))$ is not 0, then it is an appropriate pattern.

Patterns selected according to these rules are appropriate for painting the corresponding extended block at B . A random selection can be made among this pattern set. Second share created by the procedure outlined above looks similar to second cover image Red channel, because pattern groups to be tested are selected according to the relative pixel values of second cover image Red channel. Now second shares of Red channels are created.

3.7 Third Share Construction

Third share should reveal secret3 and secret4 when it is stacked with share2. So the construction of third share is based on the pixel values of share2 (B), secret3, secret4 and cover image 3. Let $s3, s4$ and C are pixel values of secret3, secret4 and share3. B and $B1$ be second share and 90° CCW rotated image of B and their extended blocks are b and $b1$ respectively. All extended blocks of P_w and P_b are suitable for third share (C), but appropriate blocks are selected based on pixel value of cover 3 using following rule set.

- Rule 1.** If S_3 is black, S_4 is black, $H(AND(c, b))$ is 0, and $H(AND(c, b1))$ is 0, then it is an appropriate pattern.
- Rule 2.** If S_3 is black, S_4 is white, $H(AND(c, b))$ is 0, and $H(AND((c, b1)))$ is not 0, then it is an appropriate pattern.
- Rule 3.** If S_3 is white, S_4 is black, $H(AND(c, b))$ is not 0, and $H(AND(c, b1))$ is 0, then it is an appropriate pattern.
- Rule 4.** If S_3 is white, S_4 is white, $H(AND(c, b))$ is not 0, and $H(AND(c, b1))$ is not 0, then it is an appropriate pattern.

Appropriate extended block (c) is placed in the corresponding pixel positions of share 3(C). Now third share of Red channels is created. Similarly Green and Blue channel shares are created using corresponding color channels of secret and cover images. By merging color channels of share1 will give the color meaningful share1. Similarly color meaningful share2 and share3 are obtained.

For the purpose of illustration, assume that two corresponding pixel values at two secret images are $S_1 = 0$ and $S_2 = 1$ and pixel values at cover images are $C_1 = 0$ and $C_2 = 1$. Because $C_1 = 0$ anyone extended block from P_b can be selected randomly and placed in share1 (A). Appropriate pattern is selected by applying rule set. Now by using extended blocks of share 1 (a) and (a1) and pixel values of secret images and second cover image appropriate pattern should be selected for B. Here, Extended block for B selected from P_w because $C_2 = 1$. Appropriate pattern selected based on the rule set. Inappropriate patterns are marked as x in below Figure 9. Appropriate extended block patterns are unmarked, these can be selected randomly. In figure. 9 extended blocks for A can be selected from three pattern of P_b corresponding to the XOR results of unmarked patterns. Extended blocks of B is determined by using pixel blocks of A and A1. By applying rule set on P_w , possible outcomes are listed in figure 9. Inappropriate patterns are marked as X. Remaining appropriate patterns corresponding to the unmarked patterns can be selected randomly from P_w .

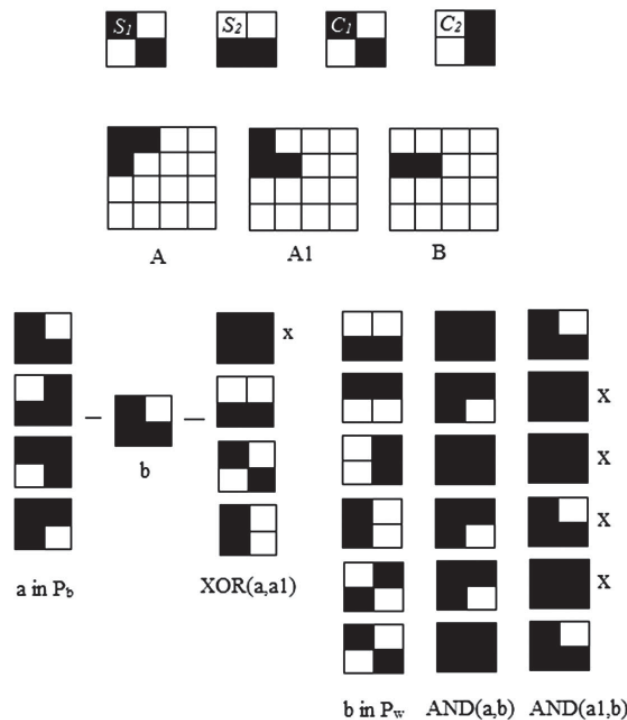


Figure 9. Extended blocks of shares determination

4. EXPERIMENTAL RESULTS

Here the proposed scheme is demonstrated by using images Lena, Baboon, Pepper and Flower of size 225x225 shown in figure 10 (a-d) are taken as input and converted into anaglyph 3D images. Modified Halftone error diffusion process applied on those images to get halftone image. Since each secret image pixel is represented by a 2×2 extended block at meaningful shares, the expansion factor is 4. It is recommended to view images in 60% resolution for visual clarity. Figure 10 to 13 represent the results of each step of the system. Size of images is resized to fit in the paper.

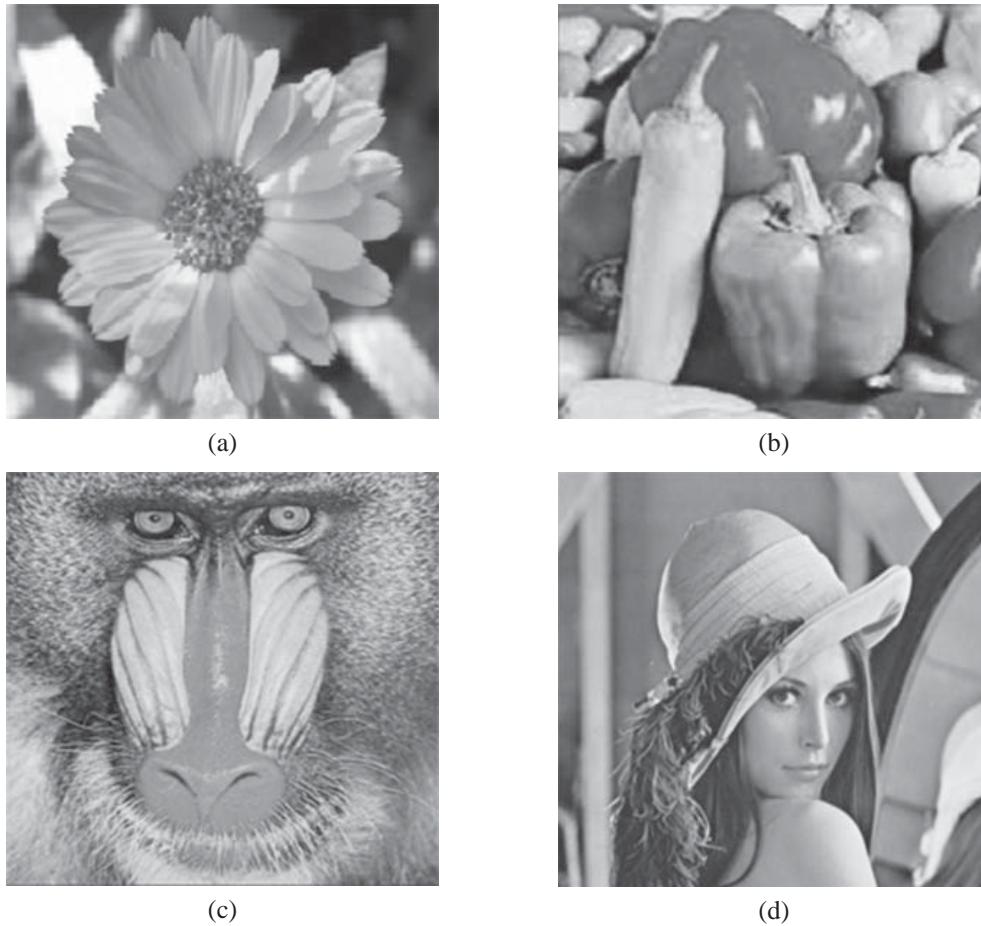
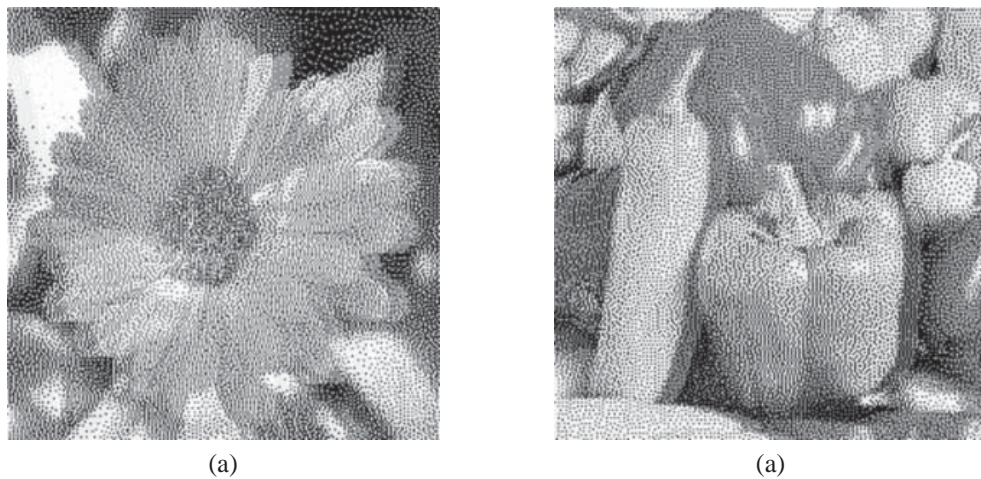


Figure 10. Secret images (a) Flower (b) Pepper (c) Baboon (d) Lena Natural 2D images



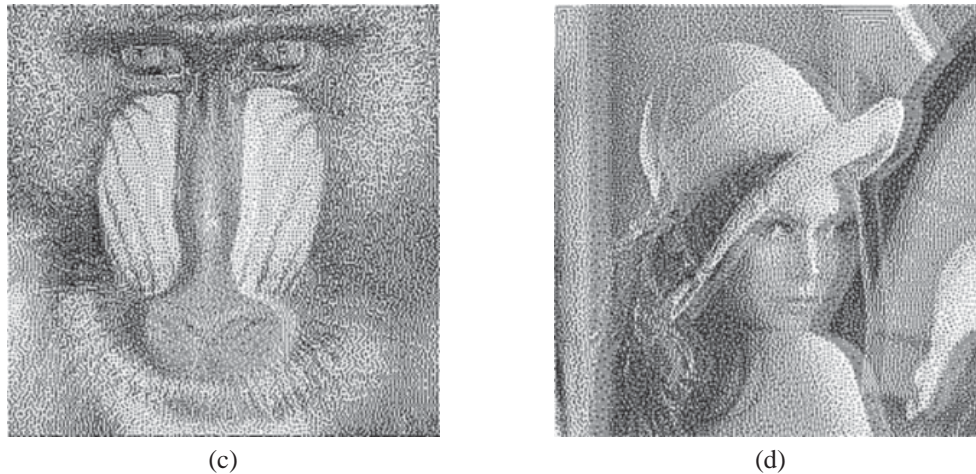


Figure 11. Halftone Anaglyph 3D images (a)-(d) of figure 10.

For three secret image encryption through meaningless share generation, Pepper, Lena, Baboon and Flower are taken as secrets. Three meaningless shares are generated shown in Fig.12.(a)-(c) and the decrypted secrets are shown in Fig.12.(d)-(f).

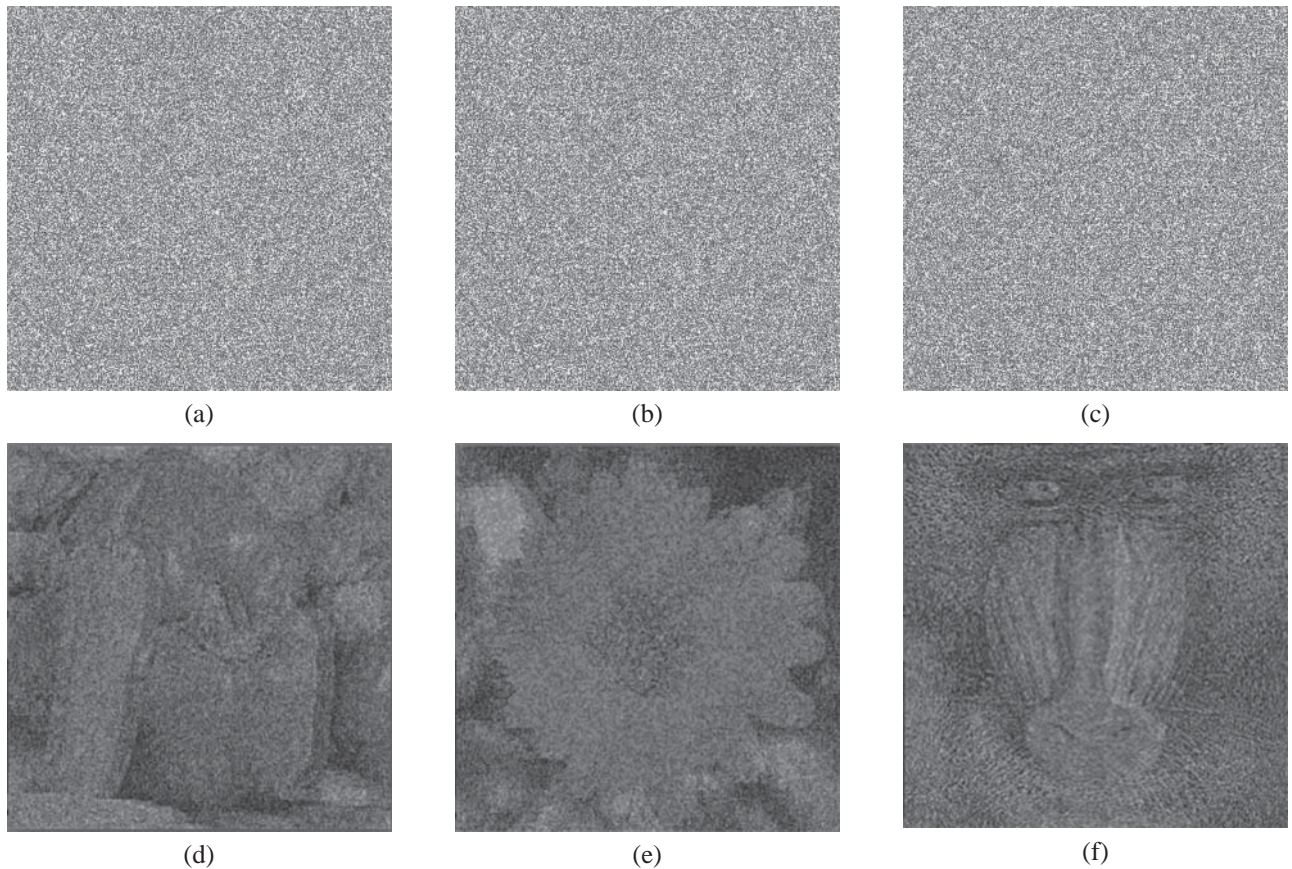


Figure 12. Encrypted Meaningless Shares (a)-(c) and Decrypted Secrets (d)-(f)

For meaningful share generation Lena, Baboon, Pepper and Baboon images are taken as secrets and Parrot, House and Eagle taken as cover images. The meaningful shares generated by proposed scheme are shown in Fig.13.(a)-(c) looks like cover images.

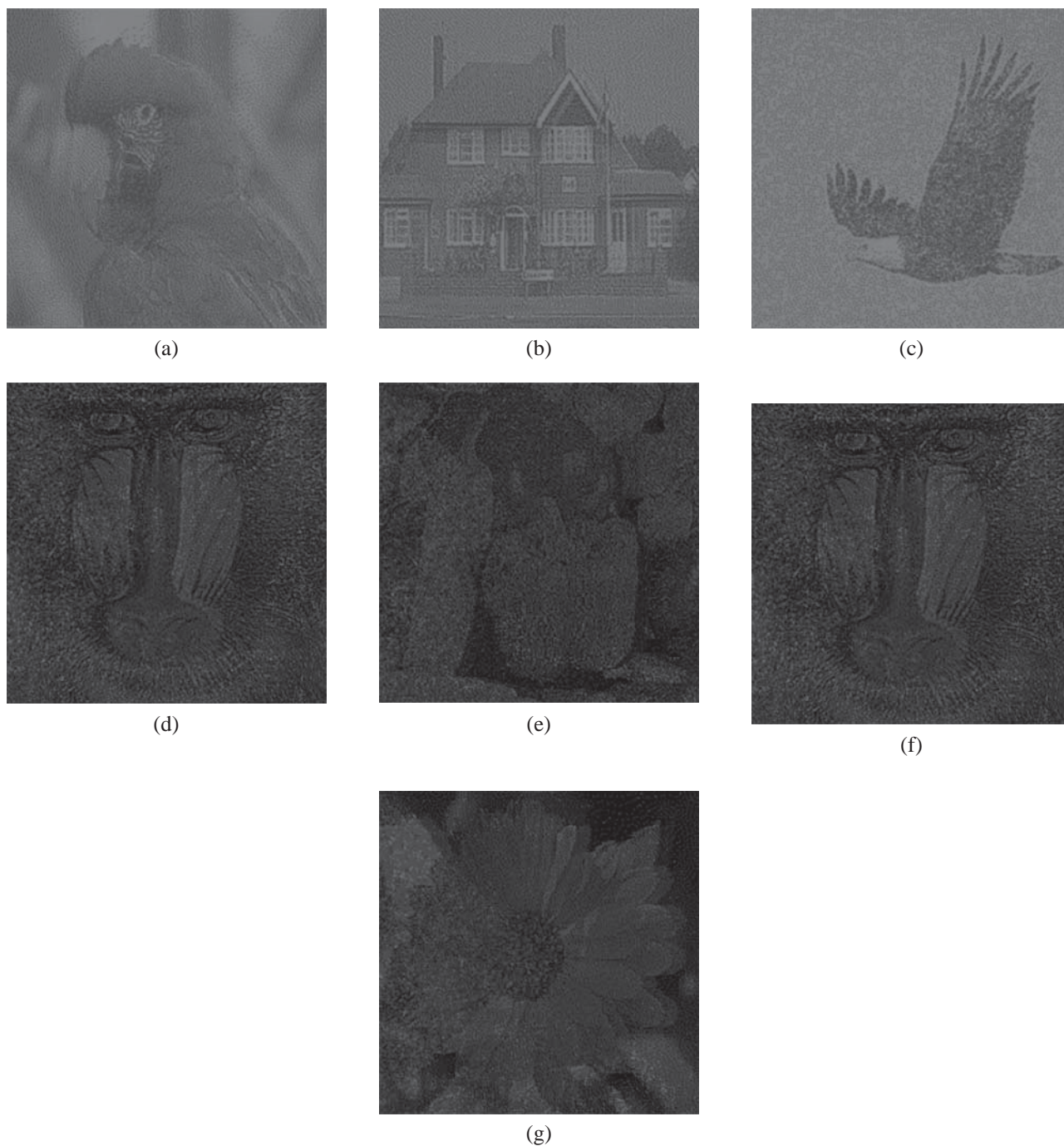


Figure 13. Meaningful shares (a)-(c) and Decrypted secrets (d)-(g)

First secret is revealed when first and second shares are stacked together whereas second secret is obtained if first share is rotated by 90° CCW and stacked with second share. Stacking share2 and share3 reveals secret 3 and forth share can be retrieved by stacking 90° CCW rotated image of share2 and share3 as shown in Fig.13.(d)-(g) respectively.

5. DISCUSSION

Many different halftone images, meaningful shares and decrypted secrets have been tested for quality improvement using proposed methods. The results of Modified halftone error diffusion, meaningless share and meaningful share generation are listed in table (1)-(4).The results bring out the following points.

1. For Halftone images of Lena, Baboon, Flower and Pepper, the PSNR values increased reasonably than the Floyd and Steinberg halftone method shown in Table.1 in which MSE (Mean Square Error) reduces in range from 100 to 167 and improvement in PSNR(Peak Signal to Noise Ratio) ranges from 0.10 db to 0.29 db.
2. By using meaningless share generation scheme, we can encrypt three different secret color images, which hide more number of secrets than single secret hiding of Extended VC schemes. The MSE reduces from 20 to 81 and 0.03 db improves in PSNR than the existing method listed Table.2.
3. For meaningful shares such as Parrot, Eagle and House image, MSE reduces in range from 4 to 36 and 0.05 db improves in PSNR are listed in Table.3.
4. For decrypted secret images from meaningful share the difference in MSE ranges from 26 to 45 and 0.03 db improves in PSNR values listed in Table.4, which is higher than existing method.

Table 1.
PSNR value comparison for Halftone images

<i>Images</i>	<i>Floyd & Steinberg Halftone Error Diffusion (Existing Scheme)</i>		<i>(Dependent threshold) + (New coefficients) (Proposed Scheme)</i>	
	<i>MSE</i>	<i>PSNR (db)</i>	<i>MSE</i>	<i>PSNR (db)</i>
Lena	4229.72	11.86	4149.79	11.96
Baboon	4387	11.70	4220.77	11.88
Pepper	2934.31	13.39	2841.54	13.60
Flower	3927.46	12.18	3822.34	12.31

Table 2.
PSNR value of different decrypted Secret from meaningless share (Using Halftone Image)

<i>Images</i>	<i>Existing Scheme</i>		<i>Proposed Scheme</i>	
	<i>MSE</i>	<i>PSNR(db)</i>	<i>MSE</i>	<i>PSNR(db)</i>
Gray Lena	5381.67	10.78	5359.76	10.81
Gray Baboon	6201.82	10.33	5989.31	10.36
Gray Flower	7300.54	9.49	7229.94	9.54
Gray Pepper	5978.04	10.19	5916.50	10.24
Color Lena	6091.05	10.28	6072.81	10.30
ColorBaboon	5869.47	10.45	5836.73	10.47
Color flower	6477.16	10.02	6438.74	10.04
Color Pepper	5973.05	10.37	5948.66	10.39

5. Shares' extended blocks corresponding to black pixels at cover images are represented by three black pixels and one white pixel whereas those corresponding to white pixels have only two black and two white pixels. Therefore, contrast of the cover images is reduced by two, since contrast is the difference between the revealed black and white pixels. Decrypted secrets' extended blocks corresponding to black pixel are represented by four black pixels whereas those corresponding to white pixels have only three black and one white pixel. Therefore, contrast of the decrypted secret images is reduced by

1/4.

6. Extended blocks of shares can contain one of the C_{10} $C_{10}=100$ possible pattern combinations. There exists at least one solution for any S_1 , S_2 , C_1 , and C_2 . Patterns used for coding the white secret pixels are also used for coding the black secret pixels with equal probability as in general VSS. In the proposed scheme, 10 different patterns are used in both shares to code four different possible combinations of the two secret pixels in regards of cover image pixels. Patterns existing in shares do not reveal any information about the two secret images encoded by them.

Table 3.
PSNR value of different decrypted Secret from meaningful shares (Using Halftone Image)

<i>Images</i>	<i>Existing Scheme</i>		<i>Proposed Scheme</i>	
	<i>MSE</i>	<i>PSNR(db)</i>	<i>MSE</i>	<i>PSNR(db)</i>
Gray Lena	4017.52	12.06	4013.51	12.06
Gray Baboon	6445.79	10.04	6412.04	10.06
Gray Pepper	9006.57	8.58	8970.42	8.60
Gray Flower	5532.79	10.52	5486.59	10.57
Color Lena	6151.38	10.24	6140.99	10.25
ColorBaboon	5725.14	10.55	5702.14	10.57
Color flower	5592.61	10.65	5571.65	10.67
Color Pepper	4973.12	11.17	4969.88	11.17

Table 4.
PSNR value of different meaningful shares (Using Halftone Image)

<i>Images</i>	<i>Existing Scheme</i>		<i>Proposed Scheme</i>	
	<i>MSE</i>	<i>PSNR(db)</i>	<i>MSE</i>	<i>PSNR(db)</i>
Gray Parrot	5760.33	10.52	5726.02	10.55
Gray Eagle	7219.31	9.54	7183.93	9.57
Gray House	6247.82	10.17	6215.65	10.20
Color Parrot	6011.69	10.34	5985.55	10.36
Color Eagle	7327.14	9.48	7285.47	9.51
Color House	5881.49	10.43	5853.49	10.46

6. CONCLUSION

This paper introduces a novel visual cryptographic scheme of generating both meaningful and meaningless shares to encrypt multiple color secret images. Meaningful share generation scheme requires three cover images to hide four secret images. However existing Extended Visual Cryptography scheme generates same kind of shares but it hides only one secret image. Modified halftone error diffusion technique reasonably improves quality of halftone images which is important for visual cryptography. Though this scheme is simple to implement secure transmission and storage of secret images, the experimental result shows the scheme enhances the following key areas of information transmission (i)Quality of meaningful shares and decrypted secret images (ii)Security of information (iii) Storage area requirement and (iv) Increasing perception ability of human visual system (HSV) using anaglyph 3D images.

7. FUTURE WORK

Multiple visual secret sharing schemes through meaningful shares proposed in this paper limited to hiding four secrets at negligible loss of quality of original images due to pixel expansion and random pixel patterns. In future work number of secret images hidden can be increased and without loss of quality of images can be addressed.

References

1. M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.
2. Chin-Chen Chang, Chia-Chen Lin, "Self-Verifying Visual Secret Sharing Using Error Diffusion and Interpolation Techniques" IEEE Trans. Info Forensics and security, vol. 4, no. 4, Dec. 2009.
3. Y. C. Hou, "Visual cryptography for color images," Pattern Recognit., vol. 36, pp. 1619–1629, 2003.
4. Inkoo Kang, Gonzalo R. Arce and Heung-Kyu Lee "Color Extended Visual Cryptography using Error Diffusion" IEEE Trans. Image Process., vol. 20, no.1, JAN. 2011.
5. Visual cryptography for color image using color error diffusion Nagaraj V Dharwadkar and B.B Amberker ICGST - GVIP Journal, ISSN: 1687-398X, Volume 10, Issue 1, February 2010.
6. Y. T. Hsu and L. W. Chang, "A new construction algorithm of visual cryptography for gray level images," in Proc. IEEE Int. Symp. Circuits Syst., 2006, pp. 1430–1433.
7. S. J. Shyu, "Efficient visual secret sharing scheme for color images," Pattern Recognit., vol. 39, no. 5, pp. 866–880, May 2006.
8. Z. M. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol.4, no. 3, pp. 383–396, Sep. 2009.
9. Multi Secret Sharing Scheme for Encrypting Two Secret Images into Two Shares Rezvan Dastanian and Hadi Shahriar Shahhoseini 2011 International Conference on Information and Electronics Engineering IPCSIT vol.6 (2011) © (2011) IACSIT Press, Singapore.
10. Securing Multiple Color Secrets Using Visual Cryptography Jenila Vincent M. a, E. Angeline Helenab Elsevier Proceedings 2012.
11. Hsien-Chu Wu¹, Hao-Cheng Wang, and Rui-Wen Yu "Color Visual Cryptography Scheme Using Meaningful Shares" IEEE Computer Society.
12. "Visual Secret Sharing Scheme for Hiding Three Secret Data" Pei-Fang Tsai, Ming-Shi Wang
13. "Digital Image Processing" Third Edition, by William K. Pratt. John Wiley & Sons Publication 2003.