

Enhanced Color Visual Secret Sharing Scheme using Modified Error Diffusion

Joseph James S
 M.E. Software Engineering
 Department of Computer Science & Engg.
 PSG College of Technology

Rajan S
 Assistant Professor (S.G)
 Department of Computer Science & Engg
 PSG College of Technology

ABSTRACT

In this paper a new visual cryptography scheme is proposed for hiding information in images which divide secret images into multiple shares. Secret information can be retrieved by stacking any k number of decrypted shares. This paper introduces the novel method of visual information pixel synchronization (VIP) and Modified threshold error diffusion to attain a color visual cryptography encryption that produces meaningful color shares with high visual quality. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channels and error diffusion generates shares pleasant to human eyes. Error diffusion method uses modified threshold value to improve the quality of shares and decrypted secret image. This paper also uses edge sharpening filters to enhance the edges of images.

Keywords

Visual cryptography (VC), meaningful shares, digital halftoning, error diffusion, secret sharing,

1. INTRODUCTION

Visual cryptography Scheme (VCS) is an emerging cryptography technology which uses the characteristics of human vision system to encrypt and decrypt images without involving complex computation. In a K-out-of-N scheme of VC [1], 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.

Previous VC schemes proposed for binary and grayscale images are not suitable for color images due to its various color levels. Some Color VC schemes produces meaningless shares[3] which are vulnerable to suspicion of shares and the pixel value of one share can be determined by scanning the pixel values of another share. Some color VC schemes[6] use complementary meaningful images for share generation which leads to suspicion of secret image and contrast loss in shares as well as decrypted secret image. The classical (2,2) VC scheme[1] for binary image share construction is illustrated in Fig.1. In this encryption process every pixel of secret image is transformed into two pixels, and each pixel take part in corresponding share image. In the decryption process the two shares are stacked together (OR operation) to recover the secret image.















Secret Image	Share1	Share2	Stacked Image
 White Pixel			
			
 Black Pixel			
			

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

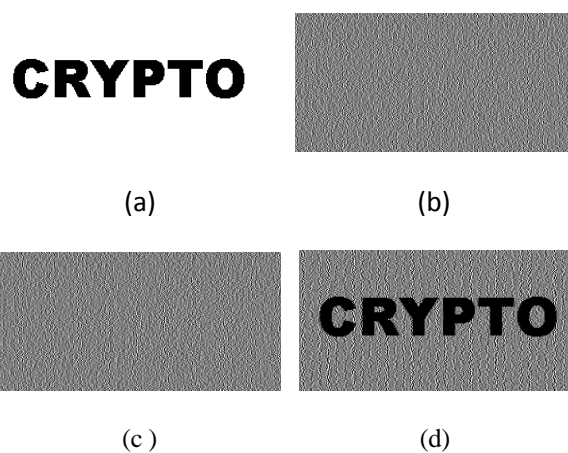


Fig .2.(a) Binary secret image.(b) Encrypted share 1. (c) Encrypted share 2. (d) Reconstructed image.

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. If pixel is white (black) one of the above four columns 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 concern to information security, one of the six columns is selected with equal probability.

This paper implements color VC scheme using modified error diffusion and meaningful images to generate secured and quality improved meaningful color share images.

2. Implementation

In this method, the secret image and meaningful images are taken as input for encryption process to generate meaningful shares. All color images are separated into RGB (Red, Green, and Blue) color channels [3]. These color channels passed to edge enhancement filter (Appendix A) to enhance the contrast of image edges. Then the RGB grayscale images are transformed to binary images using halftone technique [2]. The simple halftone method introduces more error in images during quantization. So to reduce these errors we use modified Floyd and Stein-burg error diffusion method.

2.1. Halftone Technique

Grayscale images will have pixel values in various level. This varying pixel values converted into binary values (0 or 1) using halftone technique [5]. Simple halftone method produces more errors during quantization of image. These errors will be distributed to neighboring pixels using Floyd and Stein-berg error diffusion method which easy and efficient among various error diffusion methods.

Algorithm For Halftone Error Diffusion

- [M,N] = Image size(inputimage);
 Threshold(T)=Mean(inputimage)/2
1. **Procedure Error diffusion(inimg,outimg)**
 2. **If** the actual pixel value > Threshold(T) **then**
 3. Replace pixel value with 255
 4. **Else** replace pixel value with 0
 5. Calculate the error value =actual value-new value
 6. Diffuse error into neighbor pixels using 7/16 ,1/16 , 5/16 , 3/16 values multiply with error and actual pixel values
 7. **For** left boundary pixels(row=1..M-1) **do**
 8. Diffuse error into (rows,1+1) , (rows+1,1+1), (rows+1,1+1) pixels using 7/16, 1/16 , 5/16.
 9. **For** Center image pixels(cols = 2.. N-1) **do**
 10. Diffuse error into (rows,cols+1), (rows+1,cols+1), (rows+1,cols), (rows+1,cols-1) pixels using7/16,1/16,5/16, 3/16.
 11. **End for**
 12. **For** (cols = N) **do**
 13. Diffuse error into (rows+1,N) , (rows+1,N-1) pixels using 7/16,1/16.
 14. **End for**
 15. **For** rows = M
 16. Diffuse error into (rows,1+1) using 7/16
 17. **For** cols = 2... N-1 **do**
 18. Diffuse error into(rows,cols+1) using 7/16
 19. **End for**
 20. **For** rows=M,cols=N
 21. Place the 0 or 1 accordingly
 22. **End Procedure**

The error diffusion process is illustrated in the Fig.3. The pixel $f_{ij}(m,n)$ is passed through a quantizer to obtain the corresponding pixel $g_{ij}(m,n)$. The difference between these two, $e_{ij}(m,n)$ is diffused away to the neighboring pixels by the filter $h_{ij}(k,l)$. The threshold value $t(m,n)$ determines $g(m,n)$. Here the threshold is determined using mean value of

image. This mean value varies with image. The problem with constant threshold is, when we have an image with all the pixel value below threshold value will increase error in the image during halftone process. So in this modified error diffusion method ,we have used self dependent threshold value which can be determined by taking mean value of all pixels and dividing it by 2 ($T=\text{mean}/2$). For each image this threshold is determined from their own image, which reduces the error in the halftone process. All input images should be transformed to binary form before the encryption process of share generation.

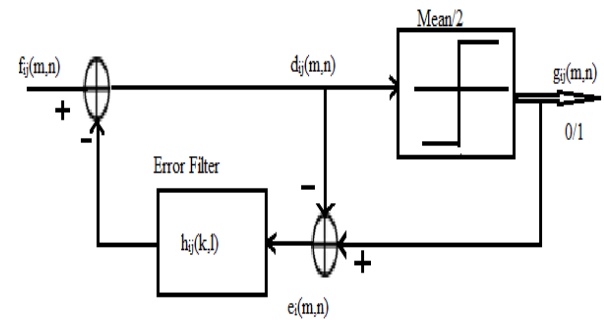


Fig.3. Error Diffusion Diagram

2.2. Meaningful Share Generation

The meaningful share generation involves through two steps[4]. In step one the matrix derivation with VIP synchronization using standard VC matrices carried out and in step two matrix distribution is carried out.

2.2.1. Construction of matrix with VIP

Our proposed encryption method focuses on VIP synchronization across color channels. VIPs are pixels that have color information of the original shares, which make the encrypted shares meaningful. In each of the m sub pixels of encrypted shares, there are q numbers of VIPs, denoted as C_i and remaining $(m-q)$ pixels deliver the information of secret message image.

Algorithm

1. For given matrices S_0 and S_1 of size $n \times m$, let $S_c[i]$ be a j^{th} bit of i^{th} row in S_c , $C(0,1)$ ($1=i=n$) and ($1=j=m$) P is the number of 1's and the given q is the number of C_i in a row of S_c
2. **procedure** MATRICES CONSTRUCTION(S_0,S_1,q)
- 3: **for** $i = 1$ **do**
- 4: **for** $l \leftarrow 1, q$ **do**
- 5: **if** $S_0[lj] = S_1[lj] = 0$ **then**
- 6: $S_0[lj] \leftarrow c_1$ and $S_1[lj] \leftarrow c_1$
- 7: **end if**
- 8: **end for**
- 9: **end for**
- 10: **for** $i = 2, n$ **do**
- 11: **for** $l \leftarrow 1, q$ **do**
- 12: **repeat**
- 13: **if** $S_0[ij] = S_1[ij] = 0$ **then**
- 14: $S_0[ij] \leftarrow c_i$ and $S_1[ij] \leftarrow c_i$
- 15: **else**
- 16: switch ($S_0[ij1], S_0[ij2]$) or
- 17: switch ($S_1[ij1], S_1[ij2]$),
- 18: where $j_1 \neq j_2$

19: end if
 20: until if there exists an α satisfying
 21: $w(S1[i]) - w(S0[i]) \geq \alpha m$
 22: end for
 23: end for
 24: end procedure

In each row of S_0, S_1 there are q number of VIPs denoted as C_i and their values are unknown during matrix construction stage.

Illustrative Example :

Consider a given basis matrices S_0 and S_1 of (2, 2)-VCS with $m = 4, p = 2$ and a given $q = 1$

$$S_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad S_0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

First we need to insert C_1 in the first row of the matrices S_0, S_1 . Compare the first element of S_0 with the corresponding element in S_1 . If we get 0 in both places, replace those 0s with C_1 then move to second row. From above S_0, S_1 matrices, the 0s at the second position in each row is replaced with C_1 as $(1C_110)$ and $(1C_110)$. For second row there are no matches found, so any two elements of any of the two matrices need to be swapped. Switching 3rd and 4th elements in second of S_0 leads to (1001) . Now replace C_2 in 3rd position results in matrices as given below

$$S_1 = \begin{bmatrix} 1 & C_1 & 1 & 0 \\ 0 & 1 & C_2 & 1 \end{bmatrix} \quad S_0 = \begin{bmatrix} 1 & C_1 & 1 & 0 \\ 1 & 0 & C_2 & 1 \end{bmatrix}$$

The 'OR'-ed row vectors in S_1 gives (1111), however the S_0 produces $(1C_1C_21)$. Since the 'OR'-ed vector of S_0 has C_1 and C_2 , this cannot ensure the contrast difference between S_0 and S_1 . It could be a (1111) when C_1 and C_2 are defined as 1. To avoid this, some bit positions in S_1 or S_0 to be switched to place C_i s at the same positions as well as to guarantee the contrast difference. we switch 2nd and 3rd bits of second row of S_0 . Replace the third bit with C_2 in S_0 and S_1 . we get matrices as

$$S_1 = \begin{bmatrix} 1 & C_1 & 1 & 0 \\ 0 & 1 & C_2 & 1 \end{bmatrix} \quad S_0 = \begin{bmatrix} 1 & C_1 & 1 & 0 \\ 1 & 1 & C_2 & 0 \end{bmatrix}$$

The OR-ed vectors of $S_0(1110)$ and $S_1(1111)$ and there exists contrast difference $\alpha = 1/4$. This also assures that the placement of VIP in same position in all color channels which represents accurate colors of the original image.

2.2.2. Matrix Distribution

The encryption process starts with the matrix distribution by referring secret image pixel. If the secret image pixel is 0 then the S_0 matrix will be placed in shares. Otherwise S_1 matrix rows placed in share generation. The following algorithm illustrates the steps involved in matrix distribution process explained above.

Algorithm

Procedure MATRICES DISTRIBUTION ($X, S_0^{c1,c2}, S_1^{c1,c2}$)
 1. Find the starting pixel position on secret image channel X .
 2. Conduct random column permutation $P(S_0^{c1,c2}, S_1^{c1,c2})$
 3. For color channel C of secret message X do
 4. If bit $c=1$, then
 5. Place the rows of the $S_1^{c1,c2}$ to the corresponding shares.
 6. Else if bit $c=0$ then
 7. Place the rows of the $S_0^{c1,c2}$ to the corresponding shares.
 8. End if
 9. End for.
 10. Repeat 3 to 5 for remaining shares.

The random permutation should be performed for both $S_0^{c1,c2}, S_1^{c1,c2}$ at the same time, since each row in the matrices have VIPs. This feature is essential to ensure VIP structure. Once the matrix distribution is done, we need to perform binary error diffusion [4] through which the quantization errors are diffused into neighboring pixels to produce final encrypted shares. This error diffusion is same as halftone error diffusion process as shown in the figure.4. The error diffusion performed only when the pixel is C_i . In this the threshold t_{ij} is position dependent. The pixel value is determined as 1 when $d_{ij}(m,n) > t_{ij}(m,n)$ otherwise 0.

Decryption process does not require any complex computation. To get the decrypted secret image, we simply need to stack (OR operation) the encrypted shares.

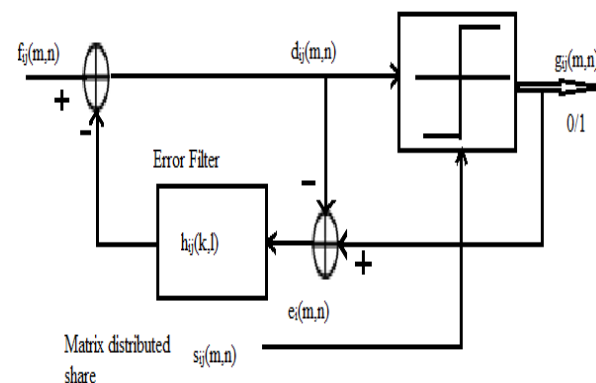


Fig.4. Binary Error diffusion

3. Experimental Results

Here the proposed scheme is demonstrated by using secret image of size 225 x 225 which shows letters U, D, R, L and Original images Lena, Baboon, Pepper and Flower of size 225 x 225 shown in Fig.5(a-d) are taken as input for halftone process. The halftone images are shown in Fig.6(a-d). The experiments are conducted for (2,2) and (3,4) Enhanced VC scheme shown in Fig.7 and Fig.8. Secret image like letters, numbers and natural scene are also taken for experiment. Tables 1 and 2. represents the computational value for Picture Quality evaluation for Encrypted shares and decrypted images. The parameters such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) are calculated between encrypted shares and original image.

Figure 5 to 8 represent the results of each step of the system. Size of images is resized to fit in the paper.

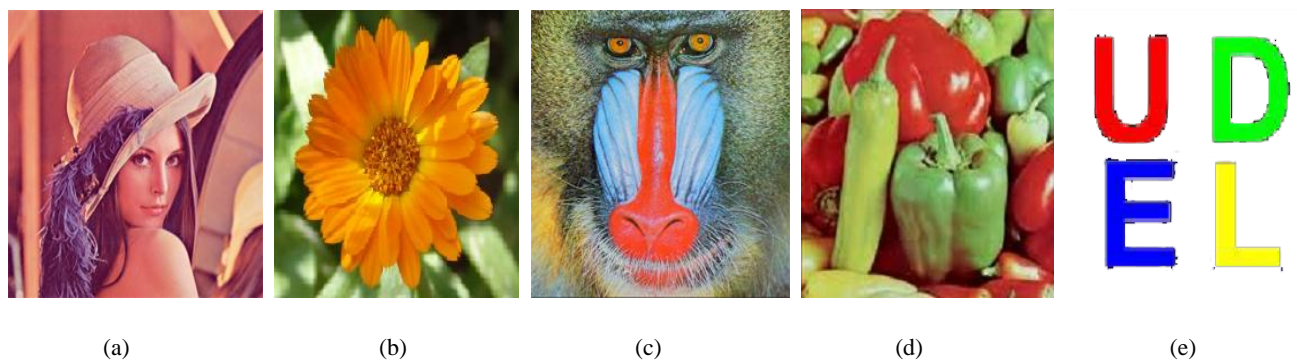


Fig.5 (a) – (d) Original Input Images of size 225x225 (e) secret input image of size 225x225

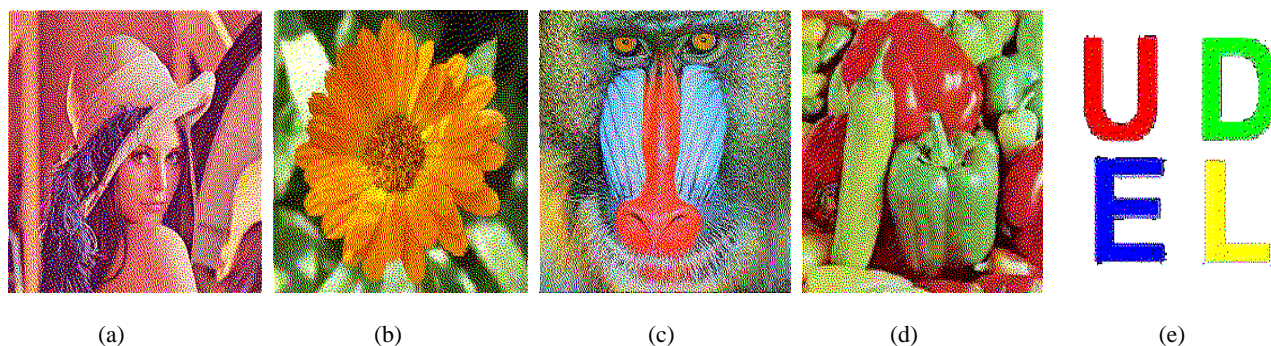


Fig.6. Halftone share images using error diffusion method

A. (2,2) VC Scheme

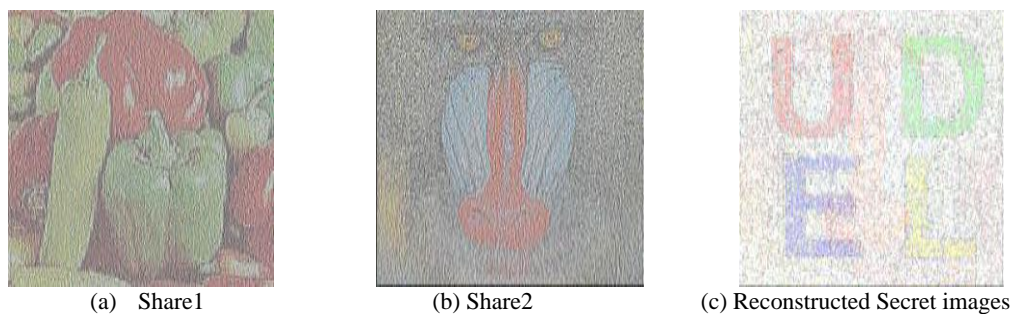


Fig.7. (a)-(b) result of encrypting images (c),(d) and (e) of figure.6.fig.7(c)Result of stacking (a) and (b) of fig.7.

(3,4) VC Scheme

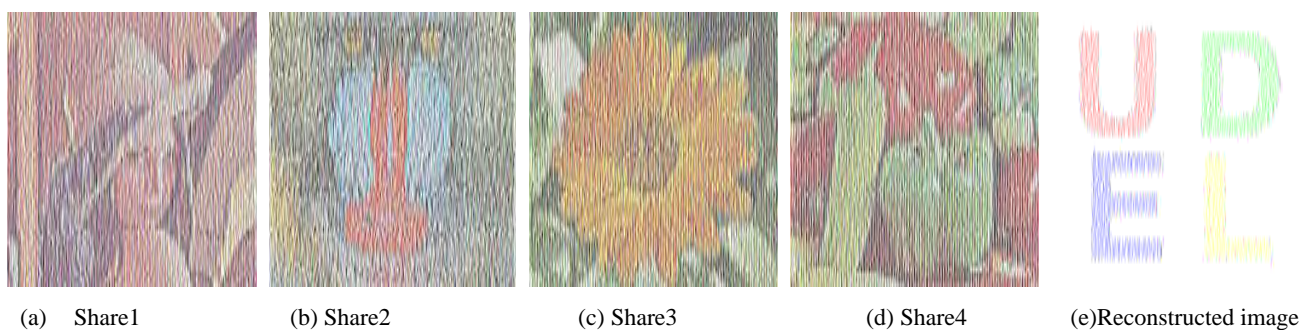


Fig.8. (a)-(d) Result of encrypting images (a),(b) ,(c),(d) and (e) of figure 6.fig.8 (e) Result of stacking (a),(b) ,(c)and (d)of figure 8

4. Discussion

Four different meaningful shares have been tested for quality improvement using proposed modified error diffusion method. The results bring out the following points.

1. For meaningful shares such as Lena ,Baboon ,pepper, Flower image, the PSNR values are increased by 1.04 db, 1.07 db ,0.12 db and 0.016 db respectively than constant threshold error diffusion method .

2. For decrypted secret images like letters ,Numbers and Natural images the difference in PSNR values is 0.042 db,0.05db,0.02 db respectively ,which is slightly higher than existing method

Summary of the result is shown in tables 1&2 ,which clearly indicates that the proposed dependent threshold error diffusion method can certainly improve the quality of encrypted shares and decrypted secret images than the existing method.

Table.1 PSNR value comparison for different encrypted shares

Images	Constant Threshold (Existing method)		Dependent threshold (Proposed method)	
	MSE	PSNR	MSE	PSNR
Lena	4613.17	10.84	4255.90	11.88
Baboon	4649.30	10.83	4247.98	11.90
Pepper	4770.48	11.30	4706	11.42
Flower	5142.55	11.05	5128.06	11.066

Table.2. PSNR value comparison for different secret images

Images	Constant Threshold (Existing method)		Dependent threshold (proposed method)	
	MSE	PSNR	MSE	PSNR
Letter	1850	15.02	1845	15.044
Number	1567.08	16.20	1560.80	16.225
Natural image	6084.44	10.30	6078.63	10.32

5. Applications

The growth in the information technology, Internet, Mobile communication, and Digital Multimedia applications has opened new opportunities in scientific and commercial applications. But this progress has also led to many serious security problems such as hacking, duplications and malevolent usage of digital information. 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 transmission of secret messages.

6. Conclusion

This paper introduces a new encryption method to construct color EVC scheme with VIP synchronization and modified threshold error diffusion for visual quality improvement. VIPs synchronize the positions of pixels that carry visual information of original images across the color channels to retain the original pixel values before and after encryption. Modified threshold Error diffusion is used to construct the shares such that the noise introduced by the preset pixels is diffused away to neighbors when encrypted shares are generated and optimizes the halftone process to improve the quality of encrypted shares and decrypted secret image. In addition, the use of edge sharpening filter further enhances the image quality.

Appendix A

Edge enhancement is an image processing filter that enhances the contrast of edges of an image. The filter works by identifying sharp edge boundaries in the image, such as the edge between a subject and a background of a contrasting color, and increasing the image contrast in the area immediately around the edge. This has the effect of creating subtle bright and dark highlights on either side of any edges in the image

7. 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] 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.
- [6] Hsien-Chu Wu1, Hao-Cheng Wang, and Rui-Wen Yu "Color Visual Cryptography Scheme Using Meaningful Shares" IEEE Computer Society.
- [7] S. J. Shyu, "Efficient visual secret sharing scheme for color images,"Pattern Recognit., vol. 39, no. 5, pp. 866–880, May 2006.
- [8] 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.
- [9] "Digital Image Processing" Third Edition, by William K. Pratt. John Wiley & Sons Publication 2003.