Multiple Secret Sharing Scheme with Gray-Level Mixing using EVCS

Aarti
Department of Computer Science and Engineering,
Dr. B. R. Ambedkar National Institute of Technology,
Jalandhar

Pushpendra K Rajput
Department of Computer Science and Engineering,
Dr. B. R. Ambedkar National Institute of Technology,
Jalandhar

ABSTRACT

Visual Secret Sharing (VSS) encrypts secret images into *n* shares and decryption is done through the human vision. But, traditional visual cryptography scheme is restricted to the number of secret images or the performance of recovered image is not good. The proposed scheme shares multiple images using gray level mixing with real size image recovery and has improved contrast of recovered images with use of inspection function. We propose a scheme that can share *m* binary secret images into *n* rectangular gray level share images. The low computation bit plane encoding scheme uses concept of Extended Visual Cryptography scheme (EVCS) to have meaningful shares that can easily managed and reduce attention of hackers over communication channel. In first phase, *m* images are broken into shares using conventional EVCS. Each image is broken into *n* individual binary shares. In the second phase, the respective shares of every image are combined with stacking the shares, since each share works as a bit plane in gray image.

Keywords— Visual Secret Sharing(VSS), Extended Visual Cryptography Scheme (EVCS), bit plane encoding, contrast

1. INTRODUCTION

With the advancement in Network Technology, large amount of digital data is transferred over communication channel via Internet, which provides instant access or distribution of digital content. So, security is a crucial problem in the transmission. Secret may be intercepted from transmission process. Traditional cryptography scheme encrypt data into cipher text which cannot be recognized by intruders. But decoding of cipher text requires large amount of computation for providing more security.

In 1979, Shamir[1] and Blakley[2] proposed secret sharing scheme which uses the concept of *(k,n)* threshold scheme, one secret message is separated into *n* shares. When at least *k(2≤k≤n)* are combined, secret image is revealed. Visual cryptography is a type of secret sharing proposed by Naor and Shamir[3], respectively, which utilizes human's own vision system to recover secret information and combines notion of cipher and secret sharing in cryptography with that of raster graphics.

A number of new schemes focus on transferring multiple images [4-10]. Most of the previous developed scheme encode one pixel at a time and have a great pixel expansion. To reduce the problem of pixel expansion many schemes have been developed that deal with a number of pixels to encode in a single runoff the method [12-14].

The shares generated by the traditional visual cryptography schemes are nearly all disorganized images. The Hacker may break the shares, although he may not know the secret. So, many researchers gave constructions of VCS for the general access structure called EVCS [15-20] which give meaningful shares instead of random shares. In 2005, Lukac and Plataniotis [12] proposed an image encryption scheme using VCS with bit plane encoding.

In this paper, we propose EVCS for multiple secret sharing. Firstly, multiple images are encoded using simple VCS technique. Using bit by bit extraction, *m* images are changes into grey scale shares from binary images. EVCS is applied on these grey-scale images to generate meaningful shares. This scheme extend previous scheme to generate innocent-looking shares using EVCS.

The rest of the paper is organized as follows. Section II briefly describes the fundamentals of visual cryptography scheme. Then, the proposed scheme is demonstrated in Section III. Section IV illustrates several experiment results. Finally, concluding remarks are given in Section V.

2. RELATED WORK

A. Extended Visual Cryptography

Naor and Shamir [3] introduce the concept of visual cryptography. The secret image is encrypted into *n* meaningless random looking shares and decryption is done by stacking shares together. OR operation is applied on the different transparencies $T = T_1, T_2, \ldots, T_n$. Detailed operation of VCS is:-

(1) $$I_1^{ij} \vee I_2^{ij} \vee \ldots\ldots \vee I_k^{ij} \vee \ldots\ldots I_n^{ij} = 0$$
$$\forall\ I_k^{ij} \in \{0\}$$

(2) $$I_1^{ij} \vee I_2^{ij} \vee \ldots\ldots \vee I_k^{ij} \vee \ldots\ldots I_n^{ij} = 1$$
$$\forall\ I_k^{ij} \in \{0,1\} \exists\ I_k^{ij} \in \{1\}$$

Where, I_k^{ij} *re*present pixel at (i,j) position of k^{th} transparency T_k, $1 \le k \le n$.

The stacking rules for two pixel values are:

Pixel Value = { ***White***, if both pixels are white ; ***Black,*** otherwise

Definition 1: A *(k, n)*-threshold EVCS can be constructed by the values $\alpha_F(m), \alpha_S(m), d$ and a family of 2^n pairs of collections $\{(B_W^{C_1 \ldots\ldots C_n})\}_{C_1 \ldots\ldots C_n} \epsilon \{b, w\}$ which satisfy the following three conditions:

1) For each $C_1 \ldots\ldots C_n \epsilon \{b, w\}$, the relative difference $\alpha_F(m)$, the threshold *d* satisfy that for each $S \epsilon B_W^{C_1 \ldots\ldots C_n}$ the OR

V of any k of the n rows meets $H(V) \leq d - \alpha_F \times m$; whereas, for any $S \epsilon B_b^{C_1 \ldots\ldots C_n}$ it results that $H(V) \geq d$

2) For each $C_1 \ldots\ldots C_n \in \{b, w\}$ and for any subsets $\{i_1 \ldots\ldots i_q\}$ of $\{1, \ldots\ldots, n\}$ with $q < k$, the two collection of $q \times m$ matrices $D_t^{C_1 \ldots\ldots C_n}$ with $t \in \{b, w\}$ obtained by restricting each n×m matrix in $B_t^{C_1 \ldots\ldots C_n}$ to rows $i_1, \ldots, i_n$ are distinguish in the sense that they contain the same matrices with the same frequencies.

3) For any $i \in \{1, \ldots, n\}$ and any $c_{1,\ldots\ldots\ldots} c_{i-1,} c_{i+1,\ldots\ldots\ldots} c_n \epsilon \{b, w\}$ it results that

$$min_{S \epsilon \mu_b} \left(H(S_i) - max_{S \epsilon \mu_w} \left(H(S_i) \right) \right) \geq \alpha_s(m).m$$

Where,

$$\mu_b = \cup_{c_1 \ldots\ldots\ldots, c_{i-1}, c_{i+1}, \ldots, c_n \in \{b,w\}} B_{W}^{C_1 \ldots\ldots\ldots C_{i-1}} b_{C_{i+1} \ldots\ldots\ldots C_n}$$

and,

$$\mu_{bw} = \cup_{c_1 \ldots\ldots\ldots, c_{i-1}, c_{i+1}, \ldots, c_n \in \{b,w\}} B_{b}^{C_1 \ldots\ldots\ldots C_{i-1}} b_{C_{i+1} \ldots\ldots\ldots C_n}$$

The first condition states that q qualified set of users, stacking their shares (or transparencies) can correctly recover the secret image. The second condition is related to the security of the scheme, it implies that by inspecting the shares one cannot gain any secret information on the shared image even though he knows the original images of all *n* shares we started with. Finally, the third condition implies that the original images are not "modified".

B. Multi-secret Sharing VCS

Definition 2: $(k_1, k_2, \ldots\ldots k_n)$ is a multi-VSS, in which n is total participants and $1 \leq k_1 < k_2 < \ldots\ldots k_h \leq n$. any k_i participants can and only can recover the secret s_i $(1 \leq i \leq h)$.

The definition above is just the basic description of multi-VSS, that is $(1 \leq i \leq h)$ persons can recover one secret image once at most. However, if $p \in (k_i, k_{i+1})$, it is unknown that whether p participants can recover s_i.

1. Hsu Method for secret sharing:

This method proposed a scheme to share multiple secrets using arbitrary angle rotation and eliminate the restriction of some specified angles $(0, 90^0, 270^0, etc.)$ defined in previous multiple secret schemes. This scheme uses angle rotation among entire 360^0 circles arbitrarily. This problem reduces the problem of limitation of secret message but arises the issue of the quality of reconstructed image. Arbitrarily angle rotation degrades the image quality of reconstructed image.

Figure 2. The results of Hsu's scheme with an angle 72^0

Our proposed scheme uses inspection function to have better contrast in reconstruction and seeks same size as original secret.

C. Xiaotian Wu and Wei Sun 's Scheme

Those random-looking shares generated by Lukac and Plataniotis's scheme attract more attention from the eavesdroppers over the communication channel. Xiaotian Wu and Wei Sun [13] proposed a scheme that removes the drawback of Lukac's scheme. Their scheme proposes a bit plane based image sharing scheme using EVCS that can share one greyscale secret image into *n* innocent-looking shadows.

3. THE PROPOSED SCHEME

This section proposed a multi-secret sharing and recovering processes of the scheme. In order to share multiple secret images in *n* meaningful share images, scheme is proposed to hide *m* secrets and to reveal the secrets with bit by bit extraction. The proposed scheme denoted as a *(k, n)* multi-VSS is based on *k*-out-of-n extended visual secret sharing scheme for *m* secret images. It uses *n* grey level meaningful shares $S_1, S_2, \ldots S_n$ with 2^m*-1* intensity level. Each share is generated by mixing the grey level of binary shares generated by each individual image. A grey scale image having intensity level 2^m*-1* can be broken into *m* bit planes by extracting a single position bit from all pixel value and each bit plane of the image is a binary matrix that can be supposed as a binary image. If we consider this approach as a grey level decomposition of an image then the reverse of the approach can be applied by mixing the grey level to generate a single grey scale image from multiple binary images using eq (1). Further discussion of this section explain the detailed description of the scheme with an instance of *(2, 2)-EVCS* to transfer *8* binary images.

$$S(i,j) = S_{b1}(i,j)\, 2^{N-1} + S_{b2}(i,j)\, 2^{N-2} + \ldots. + S_{bn-1}(i,j)\, 2 + S_{bn}(i,j) \qquad (1)$$

D. Meaningful Grey level Share Generation

The previous random looking shares have a great interest of hackers. This problem has been resolved by many watermarking scheme applied on generated shares with VCS. With the introduction of EVCS this problem become resolved without using any other watermarking technique but shares generated by EVCS for single binary images have a large impact of noises generated either by network transmission or by attackers. The aim of proposed study is to reduce the impact of these noises on shares and transfer of multiple mages. The share generation phase can be defined as follows:

M binary secret images of size $w \times h$ each are taken to transfer. A single value of pixel $P(i, j)$ of secret image is represented in binary form, *0* to represent white and *1* to represent black.

In the first step, extended visual cryptography is used with *n* binary cover images to generate *n* binary shares of every secret image such that out of *n* at least *k* shares are required to recover the image. A simple demonstration of a single pixel decomposition using EVCS is shown in Figure 3.

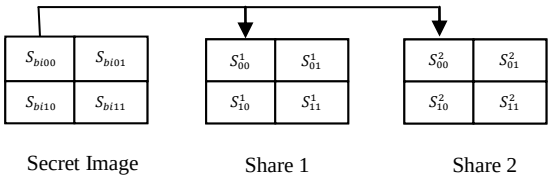


Figure 3. Pixel based Extended Visual Cryptography

In the second step, all the *n* shares of *m* secret images are stacked in the manner that each binary image combined as a single bit plane as shown in eq (1). The corresponding shares of different images are considered as single bit plane at same position in all generated grey scale shares. Eight binary images are decomposed into two shares using (2,2)-EVCS. Each share from different image is a meaningful image. The corresponding shares of every image is generated using the same binary cover images i.e. the first share is generated using the first cover image and second share of every image is generated using second cover image.

$FOR\ I\ =\ 1\ to\ 8$

$[Image_I.Share1, Image_I.Share2] =$

$EVCS\_2\_2(Image_I, cover_{image1}, cover_{image2});$

END

Then these generated binary shares are combined using a simple procedure called grey level mixing. The pseudo code for this can be written as follows:

$FOR\ I\ =\ 1{:}2*h$

$FOR\ J\ =\ 1{:}2*w$

$Share1(I,J)\ =\ 0;$

$Share2(I,J)\ =\ 0;$

$FOR\ k\ =\ 1{:}8$

$Share1(I,J) = Share1(I,J) + (pow(2,k-1) * Image_k.Share1(I,J));$

$Share2(i,j) = Share2(I,J) + (pow(2,k-1) * Image_k.Share1(I,J));$

END

END

END

E. Secret Revealing Phase

In the secret revealing stage, when any $q \geq k$ shares are collected, original image is reconstructed using following steps.

Step 1. All the collected meaningful grey scale shares are decomposed into the *m* binary bit planes using eq (1) that are corresponding to each binary share of secret image.

Step 2. Decryption using Human Vision: To reveal the original secret by human vision, stack the corresponding binary shares to recover the original binary secret image. Staking of two shares can be considered as the OR operation performed on every bit of two binary shares as shown in eq (2).

$$S_{bi} = \begin{cases} 0,\ BSH_i^j(x,y) = 0 (1 \leq j \leq q) \\ 1,\ otherwise \end{cases} \quad (2)$$

Step 3. Decryption using inspection function: The i^{th} original secret $Image_i^*$ can be recovered by inspecting the corresponding blocks in S_b. The inspecting function is formulated in Eq.(3).

$$Image_i^* = \begin{cases} 1, HB \geq d \\ 0, otherwise \end{cases} \quad (3)$$

Where, *HB* is the hamming weight of the blocks in S_b associated to location *(x, y)* and *k* define the value of threshold that is used in EVCS. This inspecting function recovers the secret image with original size and real contrast as discussed in section IV.

F. Verification of Effectiveness for Proposed Scheme

Effectiveness of VSS can be measured through the two aspects: contrast and security over communication channel. Contrast is determined using the number of sub-pixels in secret image. Our proposed scheme uses bit plane encoding with little amount of computation at receiver side which increase the contrast of secret image. Security is attained when shares are transferred over communication channel does not reveal any information. The brief comparison of proposed scheme with different developed scheme is presented in Table 1.

Contrast

Contrast is defined as difference between black and white sub-pixels in reconstructed image. Hamming weight HB_k defined the black pixel in k^{th} block after reconstruction of the image. Contrast depends upon quality of reconstructed images. With a very little computation at receiver end for using inspecting function we can recover the image with original contrast.

Security

Security of proposed algorithm can be defined at two levels. It inherits the security feature of EVCS and the mixing of multiple images reduces the effect of multiple network attacks. Proposed scheme uses random permutation for encryption of sub-blocks of secret images SI_1 andSI_2. Each block in share consists of $2n-1$ black sub-pixels and white sub-pixels. Our scheme is robust against various attacks. To test robustness of proposed algorithm, shares images were subjected to various attacks which may affect our reconstructed image. Table 2 gives image quality parameters against different kind of blurring attacks. We evaluate the PSNR value [21-22], which is a commonly accepted criterion to evaluate the visual quality of the reconstructed image. If any intruders get information about the any one of share including size and number of blocks of shares, does not able to get the information about second share. So hit rate to reveal the information about second share and secret images are $(\frac{2n!}{n!})^{xy/n}$, where block size of each share(x,y) is $2 \times y$.

Table 1. Comparison of Proposed scheme with previous methods

Scheme	Hsu et. al.[8]		Feng et al.[9]		Proposed Scheme	
No. of secret	*Contrast*	*Pixel expansion*	*Contrast*	*Pixel expansion*	*Contrast*	*Pixel expansion*
2	1/4	4	1/6	6	1/4	4
3	-	-	1/9	9	1/4	4
4	-	-	1/12	12	1/4	4
n	-	-	1/3n	3n	1/4	4

4. EXPERIMENTAL RESULTS

In this section, experimental results of the proposed sharing scheme are demonstrated. To implement the proposed scheme eight *128 × 128* pixels binary secret images are used. A *(2, 2)*-threshold EVCS is implemented using MATLAB R2009b in this experiment that uses two binary cover images to generate two meaningful shares. Two grey scale output shares of the proposed sharing scheme are represented in Figure. 4(a) and 4(b). The histogram of generated grey scale shares illustrates the distribution of intensity level as shown in Figure 4(c) and 4(d).

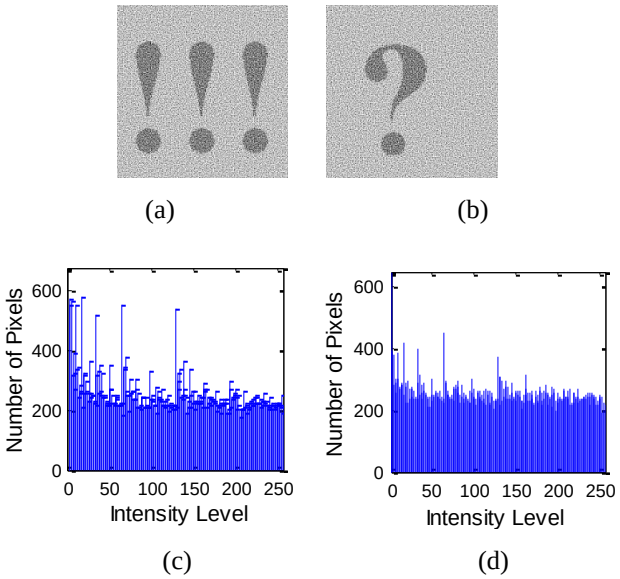
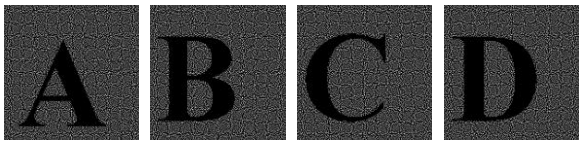


Figure 4. Grey scale share and histogram generated using proposed scheme, (a)share1, (b)share2, (c) Histogram of Share1, (d) Histogram of Share2

When the two shares are collected, the secret image can be perfectly recovered by two different decryption approach defined in section III.B. The reconstructed images using human vision are shown in Figure 5(a)-5(h).



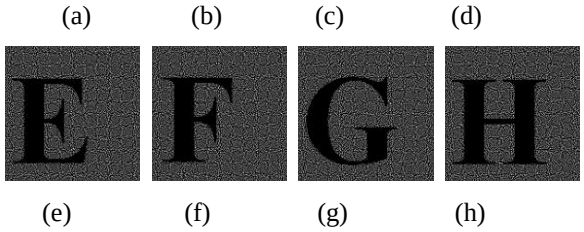


Figure 5. Reconstructed Images using Human Vision, (a) Image1, (b) Image2, (c) Image3, (d) Image4, (e) Image5, (f) Image6.

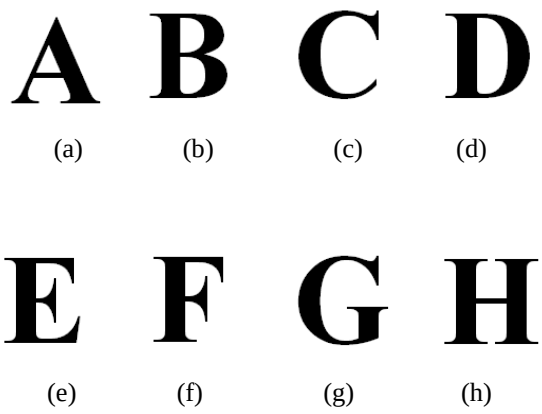


Figure 7. Reconstructed Images using Inspection, (a) Image1, (b) Image2, (c) Image3, (d) Image4, (e) Image5, (f) Image6.

The contrast of recovered images can be improved using inspection function. It also recovered the images with real size as the secret images have. The results of inspecting function are shown in Figure 6(a)- 6(h).

Table 2 shows the impact of various attacks on shares during transmission. The two most widely criteria Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) for image quality are used to define the impact of various attacks. The descriptive values shown in Table 2 are an average of test performed on all share images. A diagrammatic representation of MSE and PSNR is shown in Figure 7.

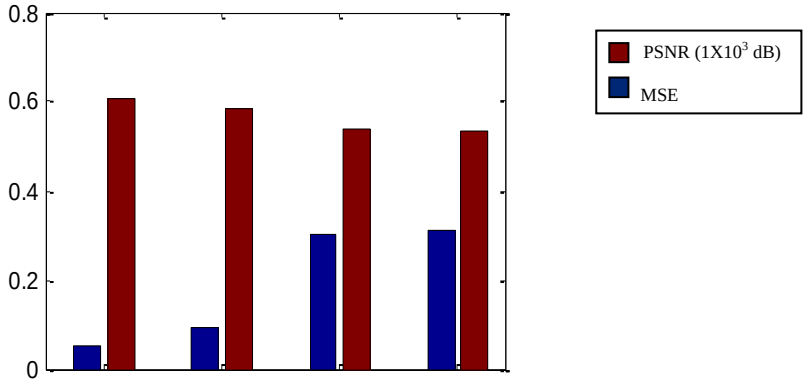


Figure 7. MSE and PSNR values on different attacks

Table 2 Impact of Different Blurring effects on Shares and recovered Images

Noise Type	MSE	PSNR	NK	AD	Effect of noise on reconstruction
Salt and Pepper	0.0529875	60.892375	0.952313	0.0274125	
Salt and Pepper(v=0.09)	0.09155	58.5158875	0.918938	0.0452625	
Poison	0.30005	53.7318875	0.73495	0.1496	
Speckle	0.312945	53.2453575	0.71601	0.1658025	

5. CONCLUSIONS

This paper proposed a multiple secret sharing scheme based on EVCS and grey level mixing. The share generated using proposed scheme have an intensity of $2^m - 1$ for sharing m binary images. The shares generated are some meaningful images that have less influence of various network attacks. This scheme can be used to share multiple images without the need of designing new codebook. It uses the previous codebook defined for extended visual cryptography.

6. REFERENCES

[1] G.R. Blakley, Safeguarding cryptographic keys, in: Proceedings of the National Computer Conference, vol. 48, NJ, USA, 1979, pp. 313–317.

[2] A. Shamir, How to share a secret, Commun. ACM 2 2 (1) (1979) 612 – 613.

[3] M. Naor, A. Shamir," Visual cryptography", in: A. De Santis (Ed.), Advances in Cryptology: Eurpocrypt'94, Lecture Notes in Computer Science, vol. 950, 1995, pp. 1–12.

[4] D. Wang, P. Luo, L. Yang, D. Qi, and Y. Dai, "Shift visual cryptography scheme of two secret images," Progress in Natural Science, Vol. 13, No. 6, pp. 457 - 463, 2003.

[5] R. Z. Wang, Y. K. Lee, S. Y. Huang, and T. L. Chia, "Multilevel visual secret sharing," Proceedings of the Second International Conference on Innovative Computing, Information and Control, Kumamoto, Japan, pp. 283 - 283, 2007.

[6] Y.-C. Hou, "Visual cryptography for color images,"Pattern Recognition, vol. 36, pp. 1619 – 1629, 2003.

[7] T.-S. Chen, J.-H. Shiesh, H .-W. Chen, Using circular shadow image and fixed angle segmentation for visual cryptography system, in: Pan-Yellow-Sea International Workshop on Information Technologies for the Network Era, Saga, Japan, March 2002, pp. 214–220.

[8] H.-C. Hsu, T.-S. Chen, Y.-H. Lin, The ring shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing, in: Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, March 2004, pp. 996–1001

[9] J. B. Feng, H. C. Wub, C. S. Tsaic, et al.. Visual secret sharing for multiple secrets. Pattern Recognition, 2008, 41(12): 3572-3581.

[10] C. Wu, C. C. Chang, Sharing visual multi-secrets using circle shares, Computer Standards & Interfaces, 28: 123–135, 2005.

[11] S. Shyong, S. Y. Huang, Y. K. Lee and R. Z. Wang. Sharing multiple secrets in visual cryptography, Pattern Recognition. 2007.

[12] Hou, Y. C. and Tu, S. F. : 'A visual cryptographic technique for chromatic images using multi-pixel encoding method',

Journal of Research and Practice in Information Technology, Vol.37, No.2, 2005, pp.179-191.

[13] Tu, S. F. and Hou, Y. C. : 'Design of visual cryptographic methods with smooth-looking decoded images of invariant size for grey-level images',The imaging Science Journal, Vol.55, No.2, 2007, pp.90-101.

[14] Zhang, H. et al., ' Visual cryptography for general access structure using pixel-block aware encoding', Journal of Computers,Vol.3,No.12,2008,pp.68-75.

[15] D. S. G. Ateniese, C. Blundo and D. R. Stinson, "Constructions and bounds for visual cryptography," in 23rd International Colloquium on Automata, Languages and Programming, ser. Lecture Notes in Computer Science, F. M. auf der Heide and B. Monien, Eds., vol. 1099. Berlin: Springer-Verlag, 1996, pp. 416-428.

[16] Z. Zhou, G. R. Arce, and G. D. Crescenzo, Halftone visual cryptography, IEEE Transaction on Image Processing , vol. 15, no. 8, pp. 2441–2453, 2006.

[17] InKoo Kang, Gonzalo R. Arce, Heung-Kyu Lee, Color extended visual cryptography using error diffusion, icassp, 2009, pp.1473-1476.

[18] H.C. Wu, H.C. Wang, and R.W. Yu, Color Visual Cryptography Scheme Using Meaningful Images, IEEE Computer Society, vol. 03, pp.173-178,2008.

[19] D. Wang, F. Yi, and X. Li. , "On general construction for extended visual cryptography schemes," Pattern Recogn, vol. 42, pp. 3071 -3082, Nov. 20 09.

[20] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC2008, IEICE, 2008.

[21] C.C. Lin, W.H. Tsai, Secret image sharing with steganography and authentication, Journal of Systems and Software 73 (2004) 405–414

[22] C.C. Chang, Y.P. Hsieh, C.H. Lin, Sharing secrets in stego images with authentication, Pattern Recognition 41 (2008) 3130–3137.