MSKS for Data Hiding and Retrieval using Visual Cryptography

Mary Shanthi Rani, M.
Department of Computer Science and Applications
Gandhigram Rural Institute-Deemed University
Gandhigram-624302, Tamil Nadu, India

Germine Mary, G.
Department of Computer Science
Fatima College
Madurai – 625016, Tamil Nadu, India

ABSTRACT
Secret message in the form of image can be concealed into two or more images in Visual Cryptography (VC) schemes. The secret image can be recovered simply by stacking the shares together without any complex computation involved. The shares do not reveal any information about the secret image if they are viewed separately. In this paper, a color visual cryptography scheme using a combination of Meaningful Shares (MS) and a Key Share (KS) is proposed. These MS will not provoke the attention of hackers. The proposed scheme makes use of the XOR operation to create KS from the MS and secret image. The secret image can be decrypted by stacking the n-1 meaningful shares and key shares together by performing XOR operation. Experimental results show that the new scheme is perfectly applicable and achieves a high two level security.

General Terms
Information Security, Cryptography.

Keywords
Visual Secret Sharing, Visual Cryptography, Meaningful Share.

1. INTRODUCTION
The impacts of information technology in the current world scenario are profound. This technology has both positive and negative impacts. Information Technology has influenced our lives in many fields including education, health, entertainment, communication etc. Through these Internet technologies, more information is transmitted swiftly to all parts of the world. But it also leads to many serious problems such as hacking and malevolent usage of digital information. Some of the objects transmitted online may be vital secret images, and in such cases the senders have to take information security issues into consideration. Being a type of secret sharing scheme, visual cryptography can be used in a number of applications.

In 1994, Naor and Shamir proposed a cryptography scheme called the "(*k*, *n*)-threshold visual secret sharing scheme," and the idea they elevated is referred to as "Visual Cryptography" [1]. The major feature of their scheme is that the secret image can be decrypted simply by the human visual system without any complex computation. Naor and Shamir's scheme can hide the secret image in *n* distinct images called shares. The secret image can be revealed by simply stacking together any k shares out of n shares. Each of the shares looks meaningless like a group of random pixels. Obviously, any single share before being stacked up with the others, reveals nothing about the secret image. Hence, the security level of the secret image when transmitted via the internet can be efficiently increased. Based on Noar and Shamir VC scheme, many related methods have been developed and proposed [2-6]. However, in addition to the meaningless shares they produce, these schemes consider only binary images as secret images. The content of the secret image may text or simple black-and-white designs. Now researchers concentrate on developing new cryptography schemes that can process secret color images [7-10] that are more complex. Verheul *et al*. proposed a (*k, n*)-threshold color visual secret sharing scheme [11] based on pixel expansion for *p* color images. Each pixel is expanded to *p* sections, and each section is divided into *p* sub pixels and can produce *n* shares with *p* sections. When the *k* shares are stacked together, the *p*-color secret image is revealed. The pixel expansion is large, if *p* is large. This scheme tends to produce many blocks with large numbers of black sub pixels when revealing the secret image; in other words, the visual quality is a not good. Besides, the shares are meaningless. In order to reduce the expansion size of the secret pixel, Yang and Laih [10] proposed a *c*-color (*k*, *n*) - threshold visual secret sharing scheme. Their scheme can indeed reduce the number of black sub pixels effectively. The pixel expansion of this scheme is $c \times m$, where *c* is the number of colors in the secret image, and *m* is the pixel expansion size of each color.

The proposed scheme has no pixel expansion and hence the quality of the decrypted/stacked image is very good. In 2007, Shyu proposed an efficient *c*-color (*k*, *n*)-threshold visual secret sharing scheme [9] and has further improved the pixel expansion to maintain good visual quality of the revealed secret image. However, in spite of all the advancements both schemes have made, the shares produced by [10] and [11] are meaningless. Hou proposed another color VC scheme [7]. Based on the halftone technique and color decomposition, it decomposes the secret image into three colors *C*, *M* and *Y*. By manipulating the three color values, the color pixels in the secret image can be represented. However, similar to what happens in [8, 9, 11], the shares are meaningless. Most of the Color Visual Cryptographic techniques do not give the original image back. The quality of the generated images is not the same as the original and there is lot of loss in the picture quality.

The shares generated in these schemes [7-11] are meaningless and look like random dots. These meaningless images may make easy targets for internet invaders to peep in. The appearance of the meaningless shares is already revealing the presence of secrets to attackers. To fill in this security gap, a new method is developed and presented in this paper to use Meaningful Shares (MS) and a Key Share (KS). MS can be chosen in such a way that it has no relevance to the original image. Meaningful Shares reduce the interest of the hackers and can be managed easily. The new proposed method creates KS using MS and secret image by performing XOR operation.

This paper is organized as follows. Section 2 reviews the basics of visual cryptography and color visual cryptography, Section 3 presents the proposed scheme which includes meaningful shares and key shares created using XOR operation, Section 4 reports the experimental results and discussions. Finally, conclusion is presented in Section 5.

2. LITERATURE SURVEY

2.1 Basic Visual Cryptographic Model

Noar and Shamir proposed the first visual secret sharing scheme in 1994 [1]. Noar and Shamir's scheme uses the human visual system to decrypt the secret image and it does not involve complex computation. They proposed (k,n) threshold visual secret sharing scheme, in which n meaningless shares are generated from the given secret image and it needs at least k shares (k<n) to decode the secret image. The secret image cannot be revealed using k-1 shares. Let us consider a (2,2)-threshold visual secret sharing scheme, where the secret image be a binary image of size $N \times N$. Every pixel in the secret image is extended into a 2×2 block, and each block is composed of two black pixels and two white pixels as shown in Figure 1.

The white pixels of black-and-white images are considered transparent. This is because the output of visual cryptography is transparencies. The black-and white visual cryptography decomposes every pixel in a secret image into a 2×2 block in the two transparencies according to the rules given in Figure 1. When a pixel is white, the method chooses one of the two combinations for white pixels to form the content of the block in the two transparencies; when a pixel is black, it chooses one of the other two combinations.

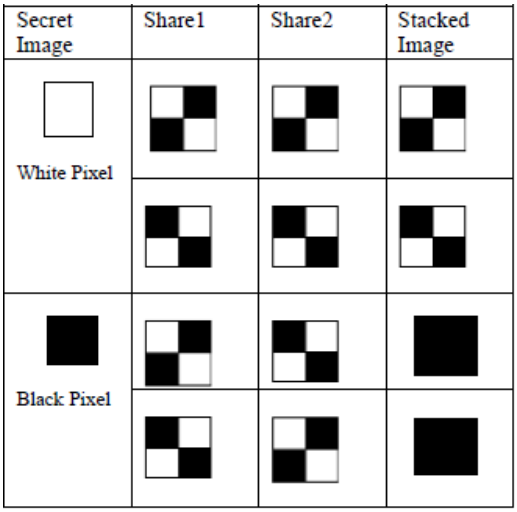

Figure 1: Sharing and stacking scheme of black and white pixels.

There are six possible patterns from which every block in a transparency can choose randomly, so the secret image cannot be identified from a single transparency. For example in Figure 2, the secret image (a) is decomposed into two visual cryptography transparencies (b) and (c). When stacking the two transparencies, the reconstructed image (d) is obtained. Though the contrast of the stacked image is degraded by 50%, human eyes can still recognize the content of the secret image. Secret image is shown only when both shares are superimposed. Stacking shares represents OR operation to human visual system. OR operation is lossy recovery. If XOR operation is applied instead of OR then we can get lossless restore of the original image. But, XOR operation requires computation. The physical stacking process can only simulate the OR operation.

The drawbacks of this scheme are:

1. It is for black and white images.

2. Need more storage capacity as shares are four times the original image.

3. It is time consuming as each pixel is encoded.

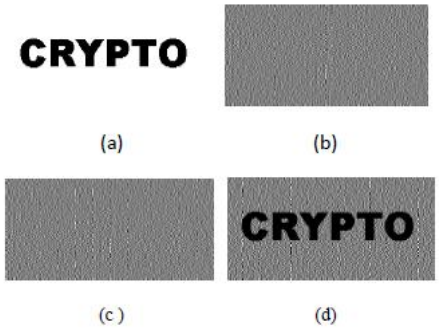

Figure 2: (a) Binary secret image (b) Encrypted share 1 (c) Encrypted share 2 (d) Decrypted secret message

2.2 Visual Cryptography Scheme for Color Images

Only black and white images were considered in Visual cryptography schemes till 1997. Verheul and Van Tilborg proposed first color visual cryptography scheme [11]. In this visual cryptography scheme one pixel is substituted by m sub pixels, and each sub pixel is divided into c color regions. In each sub pixel, precisely one color region is colored, and all the other color regions are stored black.

Liu, Wu and Lin proposed a new approach for colored visual cryptography scheme [12]. They proposed three different approaches for color image representation:

- In the first case, colors in the secret image can be printed on the shares directly. It is analogous to basic visual cryptography model. Large pixel expansion and poor quality of decoded image are the disadvantages of this approach.

- In the second case individual RGB/CMY channels are used. Red, green, blue for additive model and cyan, magenta, yellow for subtractive model. Then normal visual cryptography scheme for black and white images is applied to each of the color channels. This approach reduces the pixel expansion but quality of image gets degraded due to half toning process.

- In the third case, binary representation of color of a pixel is used and secret image is encrypted at bit-level. This approach gives good quality of image as result.

2.3 Extended Visual Cryptography Scheme

In conventional VCS, shares are formed as random patterns of pixel. These shares look like meaningless noise. Noise-like shares stimulate the attention of hackers and they might believe that some data is encrypted in these meaningless noise-like images. So it develops into susceptible security related issues. Hence it becomes difficult to manage meaningless shares, as all shares look alike. Nakajima, M. and Yamaguchi, developed Extended visual cryptography scheme (EVS) [13].

An extended visual cryptography (EVC) provide techniques to create meaningful shares instead of random shares of traditional visual cryptography and help to avoid the possible problems, which may arise by noise-like shares in conventional visual cryptography.

2.4 The Halftone Technology

Different media use different ways to represent the color level of images based on their physical characteristics. The computer screen uses the electric current to control the brightness of the pixels. The multiplicity of the lightness generates different color levels. In general, printers such as dot matrix printers, laser printers, and jet printers, can only control a single pixel to be printed (black pixel) or not to be printed (white pixel), instead of displaying the gray level or the color tone of an image directly. The way to symbolize the gray level of images is to use the density of printed dots; for example, the printed dots in the bright part of an image are thin and those in the dark part are dense (Figure 3).The method that uses the density of the net dots to replicate the gray level is called "Halftone" [14] and convert an image with gray level into a binary image before processing. As human eyes cannot identify too tiny printed dots and when viewing a dot, eyes tend to cover its nearby dots. Thus we can simulate different gray levels through the density of printed dots.

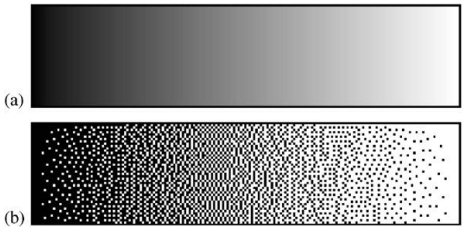

Figure 3: (a) Continuous tone (b) Halftone.

3. PROPOSED SYSTEM

3.1 Method Definition

The proposed method is a simple visual cryptography technique which combines the traditional VCS and conventional image encryption schemes. The original secret image can be retrieved by stacking n-1 color images and one key image by performing XOR operation. The number (n) of shares can be decided by the user based on the applications need. In these n shares n-1 will be Meaningful shares (MS) and one share will be a Key Share (KS). Each of n-1 MS can be any image in any format. KS can be derived by performing XOR operation on MS and Secret Image. The n-1 MS has no relevance to the original image. Meaningful Shares reduce the interest of the hackers and can be managed easily.

When the n-1 MS are combined with the KS using XOR, reveals the original secret image. The quality of the secret image revealed is the same as the original image. This algorithm has perfect reconstruction property and there is no loss of picture quality. This algorithm can also be used on gray scale image without any loss of image quality.

In additive model or RGB model [15] every color image is composed of pixels where each pixel is made up of 8 bit RGB values. Each 8 bit value is in the range of 0-255. i.e. Red ranges from 0-255, Green ranges from 0-255 and Blue ranges from 0-255. When all these three values for RGB are combined we get a color which defines the pixel of the image. In the proposed algorithm first get the value for n (number of shares). Depending on the value of n get n-1 images of your choice (which can be highly irrelevant to the secret image) and the original secret image (SI). The size of all the images needs to be the same. This algorithm divides the all true color images into RGB components. The RGB of the Key share is obtained by xoring every pixel of n-1 MS with every pixel of the original secret image. Every time we create a KS it gives a different value for each pixel based on the n-1 MS. The size of KS is also the same as the original image.

Algorithm MSKS

{

Read n

Read n-1 meaningful images which act as MS

Read the original secret image SI

Calculate width – w and height –h of the image

For i = 0 to w-1

For j = 0 to h-1

{

Retrieve RGB component from n-1 MS and SI

$RedKS_{(i,j)}=RMS[1]_{(i,j)} \oplus RMS[2]_{(i,j)} \oplus \ldots\ldots \oplus RMS[n-1]_{(i,j)} \oplus RSI_{(i,j)}$

$GreenKS_{(i,j)}=GMS[1]_{(i,j)} \oplus GMS[2]_{(i,j)} \oplus \ldots\ldots \oplus GMS[n-1]_{(i,j)} \oplus GSI_{(i,j)}$

$BlueKS_{(i,j)}=BMS[1]_{(i,j)} \oplus BMS[2]_{(i,j)} \oplus \ldots\ldots \oplus BMS[n-1]_{(i,j)} \oplus BSI_{(i,j)}$

Combine RGB to create $KS_{(i,j)}$

}

SI = MS[1] ⊕ ....⊕MS[n-1] ⊕ KS

} /* SI = Original Image

This technique is implemented using JAVA on Windows 7. In this proposed technique both during encryption and decryption the computation cost is low since the majority of the operations use logical XOR operations. Also in the scheme, there are no keys involved and hence there is no key management. All that is required is to transmit KS on a secret channel while MS can be transmitted on an unsecure channel as it will not provoke the attention of hackers.

4. RESULTS AND DISCUSION

In this section experimental results of the proposed scheme are discussed.

Theorem: Let A be the pixel matrix of the secret image. Let $A_1,\ldots,A_{n-1}$ be the pixel matrix of n-1 MS and A_n be the pixel matrix of KS. Then the following conditions are satisfied

i) $\bigcup_{j=1}^{n-1}(\oplus Aij) \neq A$, it means the XOR of any n-1 matrices cannot be used to obtain any information of matrix A

ii) $\bigcup_{j=1}^{n}(\oplus Aij) = A$, it indicates that only the XOR of n matrices can be used to recover information from the matrix A

Proof: Using the above method of construction we get n different matrices $A_1, \ldots, A_n$, where $A_n = A_1 \oplus A_2 \oplus \ldots \oplus A_{n-1} \oplus A$.

Here let

$A_1 = B_1$

$A_2 = B_1 \oplus B_2$ - is a random matrix

.....

$A_{n-1} = B_{n-2} \oplus B_{n-1}$ - is a random matrix

$A_n = B_{n-1} \oplus A$ - (1) - is a random matrix

No information matrix A could be obtained by the XOR operation for any n-1 matrices.

Case 1: Excluding A_n we get

$A_1 \oplus A_2 \oplus \ldots \oplus A_{n-1} = B_{n-1}$, which is a random matrix

Case 2: Including A_n

Suppose A_{im} excludes any one matrix (im ϵ {1,…,n-1})

$$A_n \oplus \sum_{ij=1}^{n-2} (\oplus A_{ij}) = B_{im-1} \oplus B_{im} \oplus A = A_k;$$

k ϵ {1,…,n-1} , where A_k is also a random matrix.

Obviously from the previous step and step (1) we get

$$A_n \oplus \sum_{i=1}^{n-1} (\oplus A_i) = B_{n-1} \oplus A \oplus B_{n-1} = A$$ – the original image. The theorem is therefore proved.

From the proof of the theorem above we have:

If m x n matrices $A_1, \ldots, A_n$ satisfy the above theorem, the n distinct matrices can be used to construct a (n,n) threshold scheme, the relative contrast difference is 1, and the pixel expansion is 0.

Result of the proposed MSKS scheme for n=3 is shown in Figure 4. A 256 X 256 color secret image is used which is shown in Figure 4(a). Figure 4(b) and 4(c) shows the Meaningful Shares. Figure 4(d) represents the Key Share. Figure 4(e) shows the recovered image.

(a)

(b)

(c)

(d)

(e)

Figure 4: Result of the proposed MSKS scheme. (a) Secret Image (b) and (c) Meaningful Shares (d) Key Share (e) Recovered Image.

Table 1 and Table 2 shows brief comparison of proposed scheme with other previously developed techniques based on some important parameters like MSE, SNR and PSNR.

In statistics, the mean squared error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator (original image) and what is estimated (recovered image).

Signal-to-noise ratio (SNR) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise.

The peak signal-to-noise ratio (PSNR) in decibels, is computed between two images. This ratio is often used as a quality measurement between the original and the reconstructed image. The higher the PSNR value, better is the quality of the reconstructed image.

The MSE, SNR and PSNR calculated for the reconstructed image in comparison with the original image is given below. These values point to the superior quality of the reconstructed image and trust worthiness of the proposed scheme.

MSE: 1280.5351680151184

SNR: 16.723649614164003

PSNR: 17.056888506404437

Table 1. Comparison of MSE and PSNR values of proposed scheme with previous schemes

S.No.	Scheme	MSE	PSNR
1	Proposed Scheme	1280.53	17.0568
2	Kang [16]	5896.9	10.4245
3	Droste [5]	5846.5	10.4618

Table 2. Comparison of visual cryptography schemes On the basis of number of secret images, pixel expansion, image format and type of share generated

S. No.	Authors	No. of Secret Images	Pixel Expansion	Image Format	Type of Share generated
1.	Naor and Shamir [1]	1	4	Binary	Random
2.	Wu and Chen [17]	2	4	Binary	Random
3.	Hsu *et. al.* [18]	2	4	Binary	Random
4.	Wu and Chang [19]	2	4	Binary	Random
5.	Chin-Chen Chang *et. al.* [20]	1	4	Binary	Meaningful
6.	Liguo Fang *et. al.* [21]	1	2	Binary	Random
7.	Shyu *et. al.* [9]	n(n>=2)	2n	Binary	Random
8.	Fang [22]	2	9	Binary	Random
9.	Jen-Bang Feng *et. al.* [23]	n(n>=2)	3n	Binary	Random
10.	Mustafa Ulutas [24]	2	4	Binary	Random
11.	Tzung-Her Chen *et. al.* [25]	2	1	Binary	Random
12.	Tzung-Her Chen et al [26]	n(n>=2)	4	Binary, gray, color	Random
13.	Wen-Pinn Fang [27]	2	1	Binary	Random
14.	Zhengxin Fu[28]	4	9	Binary	Random
15.	Jonathan Weir *et. al.* [29]	n	4	Binary	Random
16.	Xiao-qing Tan [30]	1	1	Binary	Random
17.	Verheul Tilborg [11]	1	c*3	Color	Random
18.	Yang & Liah [10]	1	c*2	Color	Random
19.	Chang and Tsai [31]	1	529	Color	Meaningful
20.	Chin Chen Chang *et. al.* [32]	1	9	Gray	Meaningful
21.	Lukac and Plataniotis [33]	1	2	Color	Random
22.	Youmaran *et. al.* [34]	1	9	Color	Meaningful
23.	S.J.Shyu [35]	1	$Log_2 c*m$	Color	Random
24.	Mohsen Heidarinejad *et. al.* [36]	1	9/16	Color	Random
25.	Haibo Zhang *et. al.* [37]	1	1	Gray	Random
26.	Liu *et. al.* [12]	1	1	Color	Random
27.	Wei Qiao *et. al.* [38]	1	m	Color	Random
28.	Du-Shiau Tsai *et. al.* [39]	1	9	Color	Meaningful
29.	**Proposed**	**1**	**nil**	**Color**	**Meaningful & Random**

5. CONCLUSION

Visual Cryptographic technique is being used by many countries for transferring secret messages in the form of hand written documents, text images etc. This study developed a method for constructing n share MSKS scheme. The construction and reconstruction of the Key Share and secret image adopt only the XOR operation and the quality and size of the recovered image is equal to that of the original image. Compared with the results from other visual cryptography schemes, the advantages of this MSKS Scheme are as follows. There is no pixel expansion. The picture quality of the reconstructed image is good. The algorithm complexity of MSKS scheme is lower than that of the previously proposed secret image sharing schemes. Furthermore this scheme also provides perfect security. Other than its size, the intruder will not be able to gain any information from the MSKS image. By passing Meaningful Share and Key Share through different channels, a two level security can be achieved. By choosing a meaning share which is entirely different from the original secret image one can divert the attention of the hackers.

This work can be extended to hide multiple secrets by creating multiple key shares, whereas the meaningful shares for all the secret images can be the same. These key shares will act as a master key to recover all secret information in the form of images.

6. REFERENCES

[1] Naor, M and Shamir, A., 1995. "Visual Cryptography", Advances in Cryptology- EUROCRYPT'94, pp. 1-12.

[2] Ateniese, G., Blundo, C., De Santis, A and Stinson, D.R., 1996. "Visual Cryptography for general Access structures", Information and Computation, Vol. 129, pp. 86-106.

[3] Ateniese,G., Blundo, C., De Santis,A and Stinson, D. R., 1996. "Contructions and bounds for visual cryptography", Proceedings of the 23rd International Colloquium on Automata Languages and Programming, pp. 416-428.

[4] Blundo, C and De Santis,A., 1998. "Visual cryptography Schemes with perfect reconstruction of black pixels", Computer & Graphics, Vol. 22, No. 4, pp. 449-455.

[5] Droste,S., 1996. "New results on visual cryptography", Advances in cryptography: CRYPT'96, Lecture Notes in Computer Science, No. 1109, Springer-Verlag, pp. 401-415.

[6] Naor, M and Shamir,A., 1996. "Visual cryptography : improving the contrast via the cover base", presented at Security in Communication Networks.

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

[8] Rijmen.V and Preneel, B., 1996. "Efficient color visual encryption for shared colors of benetton", Eurocrypto' 96, Rump Session, Berlin.

[9] Shyu, S.J., Huanga, S.Y., Lee, Y.K., Wang, R.Z. and Chen, K., 2007. "Sharing multiple secrets in Visual Cryptography", Pattern Recognition, Vol. 40, Issue 12, pp. 3633 – 3651.

[10] Yang, C. N. and Laih, C. S., 2000. "New colored visual secret sharing schemes", Designs, Codes and cryptography, Vol. 20, No. 3, pp. 325-335.

[11] Verheul, E and Tilborg, H.V., 1997. "Constructions and Properties of K out of N Visual Secret Sharing Schemes". Designs, Codes and Cryptography, 11(2) , pp.179–196.

[12] Liu, F., Wu C.K., Lin, X.J., 2008. "Colour Visual Cryptography Schemes", IET Information Security, vol. 2, No. 4, pp.151-165.

[13] Nakajima, M., and Yamaguchi, Y., 2002. "Extended visual cryptography for natural images", Journal of WSCG. v10 i2. pp. 303-310.

[14] Poynton, C.A., Frequently asked questions about color, http://www.inforamp.net/poynton.

[15] Siddharth Malik, Anjali Sardana, Jaya, 2012. "A Keyless Approach to Image Encryption", 2012 International Conference on Communication Systems and Network Technologies.

[16] Kang,I., Gonzalo R. Arce and Heung-Kyu Lee. 2011. "Color Extended Visual Cryptography using Error Diffusion", IEEE Trans. Image Process., vol. 20, no.1.

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

[18] Hsu, H.C., Chen, T.-S., Lin, Y.-H., 2004. "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, pp. 996–1001.

[19] Wu, H.-C., Chang, C.-C., 2005. "Sharing Visual Multi-Secrets Using Circle Shares", Comput. Stand. Interfaces 134(28), pp. 123–135.

[20] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin, 2005. "Sharing A Secret Two-Tone Image In Two Gray-Level Images", Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05).

[21] Liguo Fang, BinYu, "Research On Pixel Expansion Of (2,n) Visual Threshold Scheme", 1st International Symposium on Pervasive Computing and Applications, pp. 856-860, IEEE.

[22] Wen-Pinn Fang, 2007. "Visual Cryptography In Reversible Style", IEEE Proceeding on the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2007), Kaohsiung, Taiwan, R.O.C.

[23] Jen-Bang Feng, Hsien-Chu Wu, Chwei-Shyong Tsai, Ya-Fen Chang, Yen-Ping Chu, 2008. "Visual Secret Sharing for Multiple Secrets", Pattern Recognition 41, pp. 3572 – 3581.

[24] Mustafa Ulutas, Rıfat Yazıcı, Vasif V. Nabiyev, Güzin Ulutas, 2008. (2,2)- "Secret Sharing Scheme With Improved Share Randomness", 978-1-4244-2881-6/08, IEEE.

[25] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, 2008. "Multiple-Image Encryption By Rotating Random Grids", Eighth International Conference on intelligent Systems Design and Applications, pp. 252-256.

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

[27] Wen-Pinn Fang, 2009. "Non-Expansion Visual Secret Sharing In Reversible Style", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2.

[28] Zhengxin Fu, Bin Yu, 2009. "Research On Rotation Visual Cryptography Scheme", International Symposium on Information Engineering and Electronic Commerce,pp 533-536.

[29] Jonathan Weir, WeiQi Yan, 2009. "Sharing Multiple Secrets Using Visual Cryptography", 978-1-4244-3828-0/09, IEEE, pp 509-512.

[30] Xiao-qing Tan, 2009. "Two Kinds Of Ideal Contrast Visual Cryptography Schemes", International Conference on Signal Processing Systems, pp. 450-453.

[31] Chang, C., Tsai, C and Chen, T., 2000. "A New Scheme For Sharing Secret Color Images In Computer Network", Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27.

[32] Chin-Chen Chang , Tai-Xing Yu , 2002. "Sharing A Secret Gray Image In Multiple Images", Proceedings of the First International Symposium on Cyber Worlds (CW.02).

[33] Lukac, R., Plataniotis, K.N., 2005 . "Bit-Level Based Secret Sharing For Image Encryption", Pattern Recognition 38 (5), pp. 767–772.

[34] Youmaran, R., Adler, A., Miri, A., 2006. "An Improved Visual Cryptography Scheme For Secret Hiding", 23rd Biennial Symposium on Communications, pp. 340-343.

[35] Shyu, S.J., 2006. "Efficient Visual Secret Sharing Scheme For Color Images", Pattern Recognition 39 (5) pp. 866– 880.

[36] Mohsen Heidarinejad, Amirhossein Alamdar Yazdi and Konstantinos N Plataniotis., 2008. "Algebraic Visual Cryptography Scheme For Color Images", ICASSP, pp. 1761-1764.

[37] Haibo Zhang, Xiaofei Wang, Wanhua Cao, Youpeng Huang, 2008. "Visual Cryptography For General Access Structure By Multi-Pixel Encoding With Variable Block Size", International Symposium on Knowledge Acquisition and Modeling, pp. 340-344.

[38] Wei Qiao, Hongdong Yin, Huaqing Liang, 2009. "A Kind Of Visual Cryptography Scheme For Color Images Based On Halftone Technique", International Conference on Measuring Technology and Mechatronics Automation 978-0-7695-3583-8/09, pp. 393-395.

[39] Du-Shiau Tsai, Gwoboa Horng, Tzung-Her Chen, Yao-Te Huang, 2009." A Novel Secret Image Sharing Scheme for True-Color Images with Size Constraint", Information Sciences179 3247-3254, Elsevier.