An Improved Visual Cryptography Scheme Using Scrambling Pixels in Color Images

Rezvan Dastanian and Hadi Shahriar Shahhoseini

***Abstract*—Color visual cryptography scheme is useful in systems that need access control management and authentication like digital signature schemes used in banks that demand multi partner shares. In one of the basic visual cryptography schemes for color images, proposed by Hou et. al. it is claimed that an adversary cannot attain any knowledge about the secret image without the black mask. While by security analysis of this scheme we observe that having three color shares and stacking them, an adversary is able to distinguish color boundaries of the image and by considering the available colors of the image he can reach to the main image with a non negligible probability. In this paper, we utilize Arnold's cat matrix to enhance the security of this scheme by means of pixel scrambling. In the proposed scheme, we mislead the adversary who stacks three color shares of the image to reconstruct the main image. Therefore, without a meaningful loss in the speed of encryption procedure, the security of Hou scheme is increased. The simulation results justify our claim.**

***Index Terms*—Visual cryptography, halftone method, pixel scrambling**

I. Introduction

Visual cryptography scheme was first introduced in 1994 by Shamir and Noar [1]. In this scheme the secret image is divided into some shares in such a way that no information can be inferred about the secret image only by one image. But when shares are stacked, the secret image will be unfold such that the human eye can easily distinguish it. It is noteworthy that using this cryptographic method expands the secret image size by the factor of four, because in this method the secret pixel as can be seen in "Fig. 1", is substituted by a four-pixel block. As an example if a pixel in the secret image is black, we can consider one out of six black pixels in "Fig. 1". As an example if the fifth row is selected, two blocks shown in the fifth row will be selected for share #1 and share #2. So when these two blocks of two shares are overlaid, the black pixel will be resulted [2]. Visual cryptography schemes are also presented for color and grey level images. Visual cryptography for color images was first introduced by Hou in which he proposed three algorithms in which the first one of them contains three color shares and a black mask and the image resulted from decryption has a brightness of 50 percent while two other algorithms contain a brightness of 25 percent and two color shares [3-6]. In accordance with the foregoing security analysis, the security breach of the first algorithm is apparent. In which only two color shares out of the total three can provide adversary with some information about the secret image. In this regard, the boundaries of the image show up and the adversary can color the resulting image depending on the available colors of the image. In this paper in order to enhance the security of the predecessor scheme proposed by Hou, using the Arnold's cat matrix, we scramble the pixels of the image in such a way that boundaries of the image are not distinguishable by stacking shares and the adversary will be mislead by observing more objects in the image. We can create a meaningful image as well such that the adversary is not able to distinguish the main image.

This paper is organized as follows, In Section II. the Hou algorithm is reviewed. Section III describes the security analysis of the Hou algorithm, In Section IV our proposed modification is presented and its security will be analyzed. In Section V, conclusions are drawn and further studies are discussed.

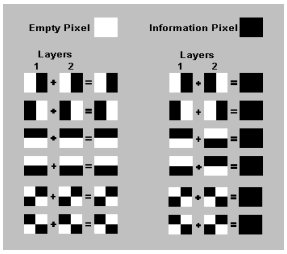


Fig. 1. Division of pixels in subpixels in visual cryptography

II. The Hou Visual Cryptography Scheme

In Hou algorithm the main image is coded in binary form using the Halftone method and then each color is encoded in accordance with the method shown in Table I. It is noteworthy that each pixel of the halftone image corresponds to one block in each color share. As can be seen in Table I, the selection criterion of the blocks in color shares in heavily dependent on the color of the main image and also the selection of the incidental block for the mask share [3]

TABLE I: The Hou Visual Cryptography Scheme

Mask	Revealed color (C,M,Y)	Share1(C)	Share2(M)	Share3(Y)	Stacked image	Revealed color quantity (C,M,Y)
	(0, 0, 0)					(1/2, 1/2, 1/2)
	(1, 0, 0)					(1, 1/2, 1/2)
	(0, 1, 0)					(1/2, 1, 1/2)
	(0, 0, 1)					(1/2, 1/2, 1)
	(1, 1, 0)					(1, 1, 1/2)
	(0, 1, 1)					(1/2, 1, 1)
	(1, 0, 1)					(1, 1/2, 1)
	(1, 1, 1)					(1, 1, 1)

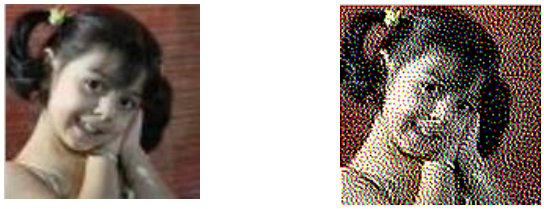
Two out of four subpixels of a block are black and the remaining subpixels are white. And also in each share two

Manuscript received May 15, 2012; revised June 12, 2012. This work was supported in part by Iran Telecommunication Research Center (ITRC).

The authors are with the Department of Electrical Engineering Of Iran University of Science and Technology, Narmak, Tehran, 16846-1311, Iran (e-mail: r_dastanian@elec.iust.ac.ir, hshsh@iust.ac.ir).

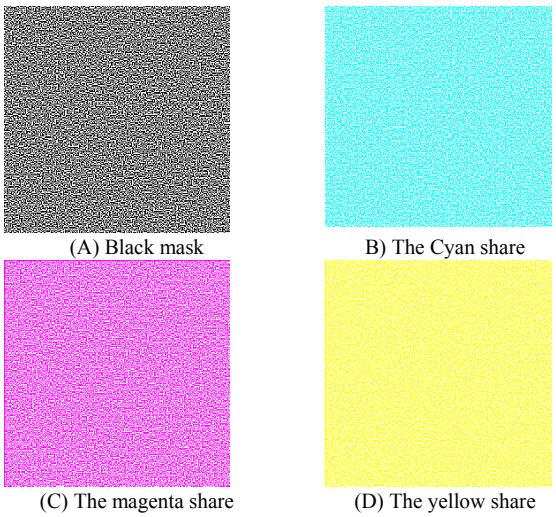
DOI: 10.7763/IJIEE.2012.V2.210

out of four blocks that correspond to one pixel in the secret image, are white and the remaining blocks are color images and as seen in the first row of Table I, the block that corresponds with the white pixel, contains two white subpixels and two black subpixels and the density of the presence of three colors of Cyan, Magenta and Yellow in a 2×2 block is $1/2$. As can be seen in the 8th row of table 1, the 4 pixels that correspond to the black pixel are all black and the density of the presence of three colors of Cyan, Magenta and Yellow is one in each 2×2 block. This procedure can be analyzed for other six colors in the same way. "Fig. 2" depicts a secret image and its corresponding halftone image. "Fig. 3" also shows four encrypted shares of "Fig. 2" and also the image resulted from stacking all shares. It is noteworthy that in the proposed visual cryptographic scheme, size of the image is enlarged with a factor of four and the results of encryption are shown with a factor of $1/4$.



(A) The main image (B) The halftone image

Fig. 2. An example image and the corresponding halftone image



(A) Black mask B) The Cyan share

(C) The magenta share (D) The yellow share

(E) The recovered image after stacking four shares

Fig. 3. (A) The black mask, (B,C,D)The color shares, (E)The image resulting from stacking the four shares.

III. Security Analysis Of Hou Scheme And Pixel Scrambling

In the Hou algorithm mentioned in Section II, the black mask is regarded as the main mask and Hou believed that no information about the secret image can be inferred without the black mask even in the presence of three other shares. In this section it is shown that the adversary is able to retrieve the main secret image with a high probability using the information of number of the colors available in the main image.

A. Security Analysis

In this subsection we introduce a Boolean matrix to calculate the probability of success for an adversary to retrieve the main secret image using only two or three shares.

Assume that the 3-tuple of (C,M,Y) with the condition of $C,M,Y\in\{0,1\}$ shows the color of one pixel in the halftone secret image. $M_{(C,M,Y)}$ is a 4×4 Boolean matrix that corresponds with four blocks of four pixels belonging to the black mask share and the remaining three other shares[7]. The first row of this matrix depicts the block that corresponds with the black mask and three other rows show the blocks belonging to the Cyan, Magenta and Yellow shares respectively. Each row contains four elements that corresponds to four pixels in each block. These values from left to right belong to the left top, right top, left bottom and right bottom pixels of the image. Two out of four values shown in each row must be set to one the remaining values must be zero. One and zero indicate the presence and absence of a color respectively [7]. In this regard, the concept of similar and complementary patterns are introduced in the sequel.

1) Similar pattern. If the status of zeros and ones are alike in two rows of a Boolean matrix, then they have a similar pattern.
2) Complementary pattern. In a Boolean matrix if the status of zeros in one row is similar with the status of ones in another row, then these rows have a complementary pattern.

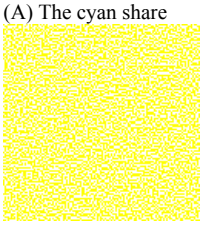
Boolean matrices have these characteristics that come in the sequel [7]. If columns of a Boolean matrix are permuted, then the pattern of the blocks corresponding with the black mask and C, M and Y shares will change. But the result of the stacking these shares will not change (after applying OR function for all the four rows) for all the Boolean matrices that are generated with the permutation of the columns of $M_{(C,M,Y)}$. Each $M_{(C,M,Y)}$ matrix contains one pair of similar columns and it can be observed that $\varepsilon_{(C,M,y)}$ contains 6 Boolean function for a 3-tuple of (C,M,Y).

It is significant to note that security of the secret image should not be dependent on the color formation or pattern. While in the Hou visual cryptography scheme, each two rows of the Boolean matrix have either similar patterns or complementary patterns and if the adversary is able to distinguish the boundaries evident in the stacking the three shares, can attack this scheme. In the sequel an example is shown to prove the insecurity of this algorithm. In "Fig. 4" the secret image consisting of four colors is demonstrated and it is assumed that the adversary has three color shares (without the mask depicted in "Fig. 5"). the adversary by stacking three shares, observes that the image consists of four general parts as a whole ("Fig. 5D"). "Fig. 6" shows the selected part in "Fig. 5d" with the enlargement factor of 800%.

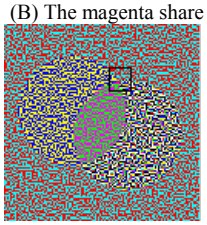
Fig. 4. The main image

(A) The cyan share

(B) The magenta share



(C) The yellow share



(D) The recovered image with stacking of three shares

Fig. 5. (A,B,C) three color shares, (D) The recovered omage with stackingof these three shares

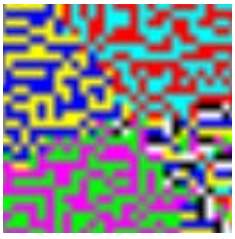


Fig. 6. The selected part of" Fig. 5D" enlarged by a factor of 8.

However, the adversary is able to recognize that the image is composed of four different colors and there will be $5\times6\times7\times8$ possible choices to color it. On the same ilk, in the magnified part of "Fig. 9" , four detached divisions are visible and in one part, yellow and blue colors are evident. Since three colors that are stacked are Cyan, Yellow and Magenta, it can be inferred that in this section, color blocks of Cyan and Magenta are in similar patterns and the Yellow block is in a complementary pattern with them. in the second part Cyan and Magenta colors are evident which show that Magenta and Yellow are in similar patterns and Yellow blocks are in complementary patterns. The same reasoning can be used to interpret other parts of the image. By and large, different parts which are evident in the image, lie in two major groups. The first group contains parts containing two colors and the second group contains parts with more than two colors. The former consists of instances in which the corresponding blocks in two shares have similar patterns and the other block possesses the complementary pattern and the latter consists of all combinations that three shares are in similar patterns. Using this method of analysis, we can divide eight matrices by four distinct groups. Furthermore without loss of generality, we assume that the black mask corresponds to the matrix $[1\ \ 0\ \ 0\ \ 1]$.

Accordingly, the four possible matrices are as shown below.

1) Matrices in which Yellow and Magenta show up with similar patterns and Cyan comes in complementary pattern. The Boolean matrices of Red and Cyan colors are depicted below.

$$Cyan = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \qquad \text{Red} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \tag{1}$$

2) Matrices in which Cyan and Magenta show up with similar patterns and Yellow comes in complementary pattern with them. The Boolean matrices of Yellow and Blue colors are depicted below.

$$Blue = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \qquad Yellow = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \tag{2}$$

3) Matrices in which Yellow and Cyan are in similar patterns while Magenta is in complementary pattern.The Boolean matrices of Magenta and Green are as shown below.

$$Green = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad Magenta = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \tag{3}$$

4) Matrices in which all three colors of Cyan, Magenta and Yellow are in similar patterns. The Boolean matrices of Black and White colors are shown below.

$$Black = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad White = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \tag{4}$$

Based on what stated above, as an example, for the first and second zone of "Fig. 7", the adversary has two options for coloring the zone, etc. Therefore, the probability of the adversary to guess the main image is

$$P_S = \binom{4}{4} \times \frac{2^4}{\binom{8}{4}} = \frac{8}{35} \tag{5}$$

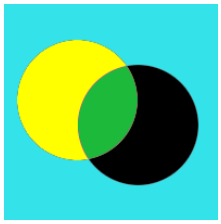


Fig. 7. The colored image for security analysis done by an adversary

If this approach is repeated for other images with different colors and different shares, the results shown in Table II depicts the probability at which the adversary can conceive the secret image.

TABLE II: THE PROBABILITY OF RECOVERING THE MAIN SECRET IMAGE FOR DIFFERENT NUMBER OF SHARES FROM THE IMAGE

Number of colors of the secret image	Number of available shares of an adversary	Probability of recovering the image
2	2	4/7=57%
2	3	6/7=86%
3	3	4/7=57%
4	3	8/35=23%

According to the aforementioned statements, we can bring the same reasoning for images containing more colors. In "Fig. 7" we can see that the adversary can recolor the image that is formed by stacking three color shares.

IV. Enhancing Security Using The Proposed Method

In Section III, it was mentioned that the adversary is able to recognize the boundaries of the main image with the knowledge of three color shares and he can achieve to the main image with a large probability. In this Section it is shown that if the main image is pixel scrambled before it is encrypted, the security of this scheme will be enhanced, because the adversary using the information of the parts he has, cannot attain correct information about boundaries of the image. Pixel scrambling can be achieved using a variety of methods such as the Baker's map, chaos, etc. [8] but in this paper it has been achieved using the Arnold's cat algorithm [9]. Map of the Arnold's cat algorithm can be derived using equations (6) and (7).

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A.\begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{6}$$

$$A = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \tag{7}$$

In these methods tuple of (x_{n+1}, y_{n+1}) shows the location of the pixel in the $n+1^{th}$ round, (x_n, y_n) depicts location of the pixel in the n^{th} round and a and b are natural numbers.

If the image shown in "Fig. 4" is scrambled, (the image resulting from stacking three color images is depicted in "Fig. 8") then the adversary will no longer distinguish the correct boundaries of the image with stacking the parts he already possesses. The periodicity of scrambling of the image is shown in equations (8) and (9).

$$r_m = A^m r_0 \bmod N \tag{8}$$

$$r_T = A^T r_0 \bmod N = r_0 \tag{9}$$

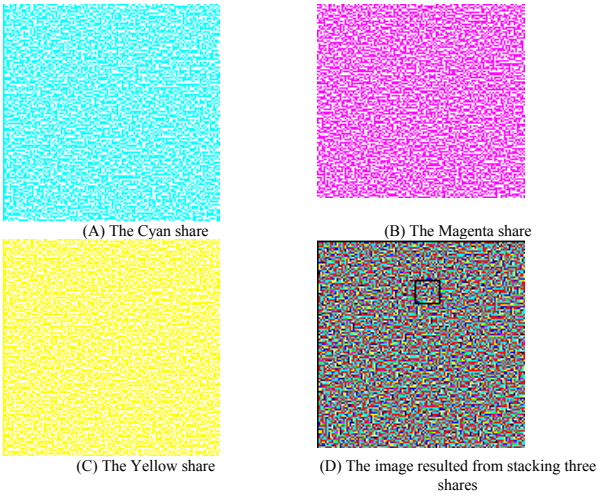


Fig. 8. (A, B, C) The resulting color shares after 13 rounds of scrambling with the Arnold's cat. (D)Image resulted from stacking three color shares.

In Eq.9, T depicts the period i.e. after T times of scrambling using the Arnold's cat, each pixel goes back to its first place. As can be seen in "Fig. 15", since the size of our main image is 64×64 pixels according to [9], our period is 64 and hence pixel scrambling does not exist.

In "Fig .9" the selected part of "Fig. 8d" is magnified 8 times and it illustrates that this time we cannot distinguish the boundaries for this image.

In order to scramble the pixels in each step, we can send the number of pixel scrambling to the receiver using a key exchange algorithm (e.g. Diffie-Hellman key exchange) and in order to further misleading the adversary, we can choose different number of pixel scrambling rounds using the Arnold's cat matrix for each color share and the adversary is intrigued because he thinks that the image contains multi objects.

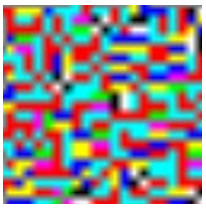


Fig. 9. The selected part of "Fig. 8D" enlarged with the factor of 8.

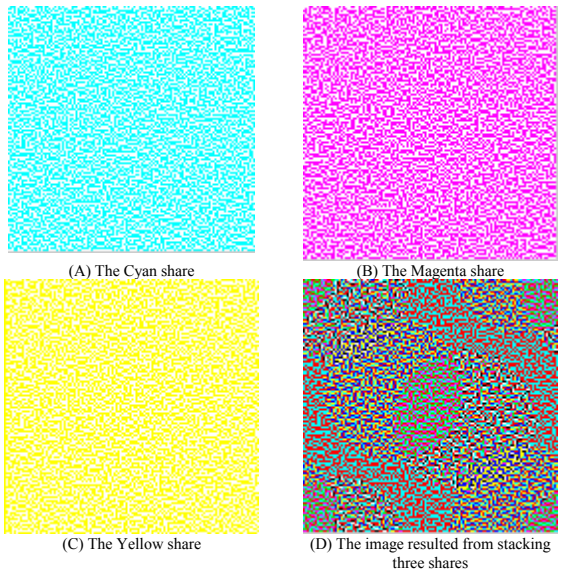


Fig. 10. (A, B, C) The resulting color shares after 16 rounds of scrambling with the Arnold's cat. (D)Image resulted from stacking three color shares.

As "Fig. 10" depicts, it is evident that if the image has a regular structure, for rounds equal to exponents of 2, the image resulted from stacking three shares can result in a meaningful image and will not be suspicious because of having a regular structure. However, if the image lacks an ordered structure, then it will be highly scrambled so that recognition of the boundaries of the image will be so difficult for an adversary and he cannot distinguish the boundaries and hence cannot attack this scheme in this way and he will guess the image as having many objects.

V. Conclusion

The first proposed algorithm for visual cryptography proposed by Hou featured the brightness of 50 percent which seemed fair comparing to the other algorithms while by

analyzing the security of this scheme, we found out that the adversary can disclose the boundaries of the main image without share of the black mask and he can then color the image depending on the number of colors of the main image and achieve to the main image with a non-negligible probability. Using the Arnold's cat matrix, we scramble the pixels of the image in such a way that boundaries of the secret image cannot be distinguished by stacking shares and the adversary will be intrigued by observing more objects in the stacked image. The results of simulation depict that we can create meaningful images using different number of rounds for selected images (in other terms extended visual cryptography scheme can be utilized).in order to further intriguing the adversary, we can first create shares of Visual cryptography and then scramble each share in various rounds using the Arnold's cat matrix and then we should exchange the scrambling schemes for each share using key exchange methods such as Diffie-Hellman key exchange method.

ACKNOWLEDGMENT

The authors are thankful of the financial support provided by Iran Telecommunication Research Center (ITRC). Also, The authors also thank Mr Arash Karimi for his helps in reviewing the early draft of the paper.

REFERENCES

[1] M. Naor and A. Shamir, "Visual Cryptography," Department of Applied Math and Camputer Science, Weizmann Institude , Rehovot, 1998.

[2] E. Verheul and H. V. Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," *Designs, Codes and Cryptography*, pp.179–196, 1997.

[3] Y. C. Hou. "Visual cryptography for color images," Pattern Recognition Society. Published by Elsevier Science Ltd, pp. 1619-1629, 2003.

[4] S. J. Shyu, "Efficient visual secret sharing scheme for color images," In *Proc. of Pattern Recognition Society39, Published by Elsevier Ltd*, pp. 866–880, 2006.

[5] Z. Zhor ,G. R. Arce, and G. D. Crescenzo, "Halftone Visual Cryptography," *IEEE Trans. on Image Processing*, vol. 15, no. 8, pp. 2441-2453, 2006.

[6] F. Liu, C. K. Wu, and X. J. Lin, "Colour visual cryptography schemes," in *Proc. of Information Security*, vol. 2 , pp. 151-165, 2008.

[7] B. Leung, F. Ng, and D. S. Wong, "On the security of a visual cryptography scheme for color images," *Pattern Recognition Society42*, Published by Elsevier Ltd , pp. 929-940, 2008.

[8] X. Y .Yu, J. Zhang, H. E. Ren, G. S. Xu, and X. Y. Luo. "Chaotic Image Scrambling Algorithm Based on S DES," *The proceeding of Journal of Physics:Conference Series48*, pp. 349-353, 2008.

[9] F. Forati and H. S. Shahhoseini, ""Bi-level Scrambling For Image Secresy," *The Proceeding of 4th Society Of Cryptology Conference* (ISCC07), Tehran, Iran, pp. 16-18, 2007.

Rezvan Dastanian was born in Iran, Ahvaz, in 1987. She received the B.Sc. and M.Sc. degrees in electrical engineering from Iran University of Science and Technology, Iran, Tehran in 2008 and 2011 respectively and is currently working toward the Ph.D. degree in electrical engineering at Shiraz University of Technology. Her research interests include cryptography, Biochemical computing, current mode and data converter.

Hadi Shahriar Shahhoseini received B.S. degree in electrical engineering from University of Tehran, in 1990, M.S. degree in electrical engineering from Azad University of Tehran in 1994, and Ph.D. degree in electrical engineering from Iran University of Science and Technology, in 1999. He is an assistant professor of the electrical engineering department in Iran University of Science and Technology. His areas of research include networking, supercomputing and reconfigurable computing. More than 130 papers have been published from his research works in scientific journals and conference proceedings. He is an executive committee member of IEEE TCSC and serves IEEE TCSC as regional coordinator in middle-East Countries.