

A New Simple Non-Expansion Algorithm for (2, 2)-Visual Secret Sharing Scheme

Abdul-Gabbar Tarish Al-Tamimi

Computer Science Department

Faculty of Applied Sciences

University of Taiz

Taiz, Yemen

Abdullah Gaafar

Computer Science Department

Faculty of Computers and Information

University of Taiz (Torba Branch)

Taiz, Yemen

ABSTRACT

Visual cryptography (VC) is a powerful encryption technique which combines perfect secrecy and secret sharing in cryptography with respect to images. VC takes a binary image (the secret) and divides it into two or more pieces known as shares (transparencies). When the shares are superimposed, the secret can be recovered. One of the distinguishing features of VC is that it needs no computational power for decryption. All what VC needs for decryption is the human visual system (the human eye). Two main factors affect the quality of a visual cryptography scheme; the pixel expansion and the contrast. In this paper we propose a new simple non-expansion algorithm for (2,2)-visual secret sharing scheme (VSS). The shares produced by this algorithm and the reconstructed image are not expanded in size, and all have the same size as the original (secret) image. It encodes the original (secret) image a 4-pixel blockwise to 4-pixel blocks in each share.

General Terms:

Cryptography, Computer Security

Keywords:

Visual Cryptography, Pixel Non-Expansion, Visual Decryption, Secret Sharing

1. INTRODUCTION

Visual cryptography, proposed by Naor and Shamir in [8], is a paradigm for cryptographic schemes that allows the decryption process without any cryptographic computation; it is accomplished by the human visual system. The existing visual cryptography techniques are used for sharing and encrypting data, especially images, where the encryption operation does not require complex computations and the decryption operation is performed only by the human visual system [7, 1].

The visual cryptography technique divides a secret image into a set of shares (see Figure 1) and distributes those shares to participants. It is simple to implement, since it needs no complex mathematical primitives for encryption, and it needs only the logical "OR" operation for decryption which is performed automatically by human visual system (human eye) without the aid of computers. Visual cryptography is a desirable scheme as it embodies both the idea

of perfect secrecy (using a one time pad) and a very simple mechanism for decrypting/decoding the secret. The interesting feature about visual cryptography is that it is perfectly secure. There is a simple analogy from one time padding to visual cryptography. If we consider the current popular cryptographic schemes, which are usually only conditionally secure, we can see that this is the second critical advantage of visual cryptography over other cryptographic schemes [4, 2, 11].

Two main factors affect the quality of a visual cryptography scheme; the pixel expansion and the contrast. The pixel expansion refers to the number of sub-pixels in a share required to represent a single pixel in the original image, they should be as small as possible. The contrast is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image, it is preferred to be as large as possible [8].

In this paper, we propose a new simple non-expansion algorithm (NSNEA) for implementing (2,2) visual secret sharing scheme for black and white images. NSNEA maps the pixels of the secret image (SI) to transparencies as a blocks of 4 bits at a time. The resulting transparencies are of the same size as the original secret image, and hence the recovered image is of the same size as the secret image.

The rest of this paper is organized as follows, Section 2 presents related work, Section 3 presents a brief description of visual secret sharing, Section 4 introduces our proposed new simple non-expansion algorithm for (2,2)-VSS in detail, Section 5 presents the experimental results, and Section 6 is the conclusion and future work.

2. RELATED WORK

Many schemes have been proposed to overcome the problem of pixel expansion. Ito et al. [6] and Yang [12] applied probability concepts in the design of a probabilistic visual secret sharing scheme called ProbVSS for binary images. In this method, each pixel in the original secret image is represented as a black or white pixel in the shares according to a randomly selected column from a ready-made $n \times m$ matrix S_0 if the original pixel is white or randomly selected column from ready-made $n \times m$ matrix S_1 if the original pixel is black.

Chen et al. [3] proposed a size invariant scheme using block encoding method. In this scheme original image is first divided into several blocks then encode a block instead of a pixel at a time.

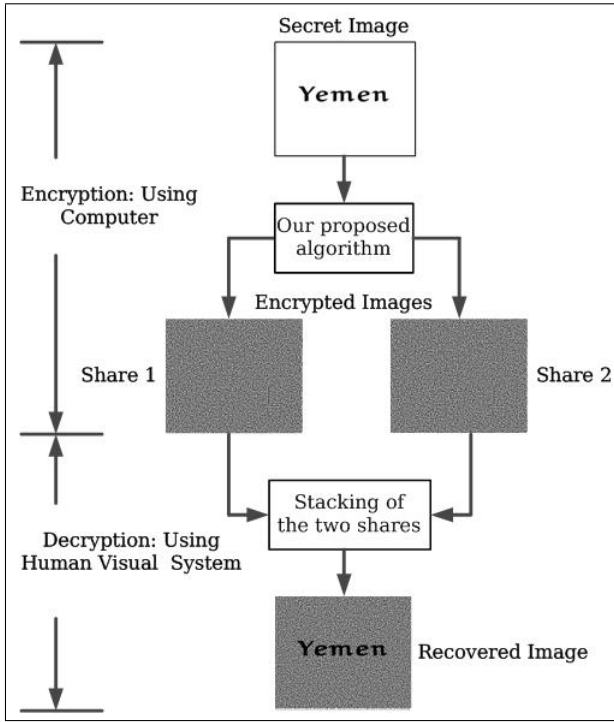


Fig. 1. An example for our proposed algorithm

Each block is encoded into k blocks on k shares and each block generate share is composed of $s/2$ white pixel and $s/2$ black pixel. The reconstructed image can be same size of original image. Pooja and Dr.Lalitha in [9] proposed a method of visual cryptography for halftone images which represent the resultant image in the same size as the original secret image. This scheme proposed the new algorithms for the (2,2) visual cryptography. The proposed scheme uses the concept of pseudo randomization and pixel reversal approach in all methods.

Ching et al. in [10] proposed two secret sharing, both of them have the characteristic that the share images they produced are with no pixel expansion.

Huang and Chang in [5] introduced a scheme that combines the non-expanded scheme with the extra ability of hiding confidential data to prevent the detection of information. In this scheme, the secret image is divided into four regions, and share blocks are subsequently generated by using the block encoding method with non-expansion ability.

3. VISUAL SECRET SHARING (VSS)

This section provides a brief description on conventional visual cryptography model as introduced by Naor and Shamir. In this model, the original secret image consists of a set of black-and-white pixels and each pixel is encrypted separately. Each pixel in the original image is represented by n blocks, which appear as n shares, one block for each share. Each block consists of a set of m black and white sub-pixels, where m is called the parameter of pixel expansion. Thus, the size of each share is m times as large as that of the secret image. A white and a black sub-pixels are represented as 0 and 1, respectively [8]. Formally, Naor and Shamir's (k, n) visual secret sharing scheme is defined in [8] as follows:

Definition 1. A solution to the (k, n) visual secret sharing scheme includes two collections C_0 and C_1 of $n \times m$ Boolean matrices obtained from permuting the columns of what so called basis matrices $S_0 = [s_{ij}]$ and $S_1 = [s_{ij}]$ where $i \in \{1, \dots, n\}$, $j \in \{1, \dots, m\}$ and $s_{ij} = 1$ iff the j^{th} sub-pixel in the i^{th} share (transparency) is black. $s_{ij} = 0$ iff the j^{th} sub-pixel in the i^{th} share (transparency) is white. To share a white pixel, one of the matrices in C_0 is randomly selected. In a similar fashion, to share a black pixel, one of the matrices in C_1 is randomly selected. The selected matrix defines the color of the m sub-pixels in each of the n transparencies. The solution is considered valid if the following two conditions are met:

1. For any $S \in C_0$, the "OR" V of any k of the n rows satisfies $H(V) \leq d - \alpha \times m$.
2. For any $S \in C_1$, the "OR" V of any k of the n rows satisfies $H(V) \geq d$.
3. For any subset $\{i_1, i_2, \dots, i_q\} \subset \{1, 2, \dots, n\}$ where $q < k$ the two collections of $q \times m$ matrices D_t for $t \in \{0, 1\}$ obtained by restricting each $n \times m$ matrix in C_t where $t \in \{0, 1\}$ to rows i_1, i_2, \dots, i_q are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The first two conditions are called contrast and the third condition is called security. C_0 is the set of all matrices obtained by permuting the columns of S_0 and C_1 is the set of all matrices obtained by permuting the columns of S_1 (see Equations 1, 2, 3, 4 as examples). n is the number of participants (the number of shares or transparencies), k is the number of qualified participants, which is the smallest number that can recover the secret image. m is the number of pixels in a share; i.e the number of pixels that are mapped to each transparency for each pixel in the original (secret) image. α is the contrast of the recovered image (the inverse of m in case of (n, n) scheme as in [8]). $H(V)$ is the Hamming weight of vector V (it is the number of 1's in V). d is a threshold value to visually interpret the reconstructed pixel as black or white ($0 \leq d \leq m$). S_0 and S_1 are called basis matrices.

For Naor and Shamir's (2, 2) visual secret sharing scheme, S_0 and S_1 may be defined as follows:

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

$$S_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad (2)$$

As such, therefore, C_0, C_1 will be as follows:

$$C_0 = \left\{ \begin{bmatrix} 1010 \\ 1010 \end{bmatrix}, \begin{bmatrix} 0101 \\ 0101 \end{bmatrix}, \begin{bmatrix} 0011 \\ 0011 \end{bmatrix}, \begin{bmatrix} 1100 \\ 1100 \end{bmatrix} \right\}, \quad (3)$$

$$\left\{ \begin{bmatrix} 0110 \\ 0110 \end{bmatrix}, \begin{bmatrix} 1001 \\ 1001 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \begin{bmatrix} 1010 \\ 0101 \end{bmatrix}, \begin{bmatrix} 0101 \\ 1010 \end{bmatrix}, \begin{bmatrix} 0011 \\ 1100 \end{bmatrix}, \begin{bmatrix} 1100 \\ 0011 \end{bmatrix} \right\}, \quad (4)$$

$$\left\{ \begin{bmatrix} 0110 \\ 1001 \end{bmatrix}, \begin{bmatrix} 1001 \\ 0110 \end{bmatrix} \right\}$$

4. THE PROPOSED NEW SIMPLE NON-EXPANSION ALGORITHM (NSNEA)

The objective of NSNEA is to produce non-expanded transparencies with each transparency has a size equals the size of the original secret image (SI), and therefore the recovered image has the same size as SI. For that purpose, NSNEA starts by checking y (the height) and x (the width) of SI if they are divisible by 2, assuming that SI is $x \times y$ image. If they are not, it begins the encoding process on the part $x' \times y'$ of SI where $x' = x - x \% 2$ and $y' = y - y \% 2$. Last column (in case of $x \% 2 \neq 0$) and last row (in case of $y \% 2 \neq 0$) are processed separately (see Figure 2).

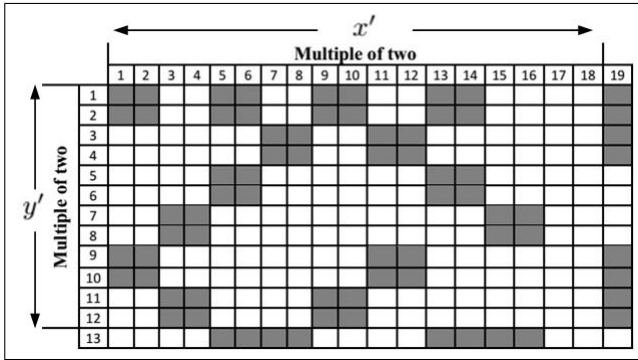


Fig. 2. Explanation for dividing SI into b blocks and how last column and last row are processed

The encoding process on part $x' \times y'$ of SI is performed as follows: Each 4-bit block b is encoded to a 4-bit block for each share (transparency) according to the number of white pixels in b (see an example of block b in Figure 3(a) - (x, y) is the coordinate of upper left pixel in the block and $(x + 1, y + 1)$ is the coordinate of lower right pixel of the block). If number of white pixels in b equals four, then b is considered white. It is encoded by random selection of a matrix from C_0 and mapping its first row to share 1 and its second row to share 2. **If number of white pixels in b is three, the encoding of b will be half white and half black block according to the position of the black pixel.** The encoding block will be such that it has two adjacent black pixels (one black besides the original one) to ensure good representation of original pixel in the recovered image.

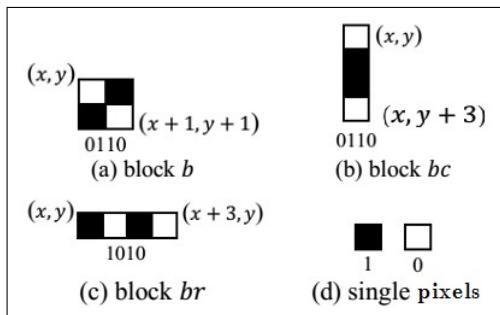


Fig. 3. Examples for different blocks forms

This encoding block is held by random selection of a matrix from C_{01} if the black pixel is the first in b (i.e. if $b = 1000$), or from C_{02} if the black pixel is the second in b and so on. $C_{01}, C_{02}, C_{03}, C_{04}$ are all subsets from C_0 (see Equations 5, 6, 7, and 8).

$$C_{01} = \{C_0(0)\} \quad (5)$$

$$C_{02} = \{C_0(3), C_0(4)\} \quad (6)$$

$$C_{03} = \{C_0(2), C_0(4)\} \quad (7)$$

$$C_{04} = \{C_0(2)\} \quad (8)$$

$$C_{05} = \{C_0(0), C_0(1), C_0(2), C_0(3)\} \quad (9)$$

If number of white pixels in block b is 2, two cases are distinguished when b is diagonal; i.e. if $b = 0110$ or $b = 1001$. Here, b is encoded by randomly selected matrix from $C_{05} \subset C_0$ to ensure that the encoding block has two adjacent black pixels. In other cases, b is encoded as a black block by randomly selected matrix from C_1 , and mapping its first row to share 1, and its second row (which is the complement of first row) to share 2.

The special cases, when the width of SI is not multiple of two or height of SI is not multiple of 2 or both of them, are processed as follows. If the width is not multiple of 2, the last column is encoded 4-bit block at a time. The last column block is like the one in Figure 3(b), it processed in the same way as block b , taking in consideration the different positions of pixels. If the height is not multiple of 2, the last row is encoded 4-bit block at a time. The last row block is like the one in Figure 3(c), it processed in the same way as block b , taking in consideration the different positions of pixels.

The last special case is that if the height (y) of SI or the width (x) of SI or both of them are not multiple of four. The $x \% 4$ pixels in last row and $y \% 4$ pixels in last column are processed pixelwise (the maximum number of them is 5 in both last column and last row). For each pixel of them, if it is white, then randomly select to encode it to white or black in both shares. If the pixel is black, randomly select to encode it to white or black in share 1 and encode it to the complement in share 2. Algorithms (1-7) present details of NSNEA.

Algorithm 1: Encoding of b to white block

```

1 encodeToWhite( $b$ ){
2   begin
3     randomly select  $M_0$  from  $C_0$ ;
4     encode  $b$  by first row of  $M_0$  to share 1;
5     encode  $b$  by second row of  $M_0$  to share 2;
6   }

```

Algorithm 2: Encoding of b using C_{0I}

```

1 encodeUsingC0I( $b, i$ ){
2   begin
3     /*  $i \in \{1, 2, 3, 4, 5\}$  */
4     randomly select  $M_{0i}$  from  $C_{0i}$ ;
5     encode  $b$  by first row of  $M_{0i}$  to share 1;
6     encode  $b$  by second row of  $M_{0i}$  to share 2;
7   }

```

Algorithm 3: Encoding of b to black block

```

1 encodeToBlack( $b$ ){
2 begin
3   randomly select  $M_1$  from  $C_1$ ;
4   encode  $b$  by first row of  $M_1$  to share 1;
5   encode  $b$  by second row of  $M_1$  to share 2;
6 }
```

Algorithm 4: Encoding of a block in last column (bc)

```

1 encodeBlockLastColumn( $bc$ ){
2 begin
3   encode  $bc$  using the same rules of encoding  $b$ , taking in
4   consideration different form of  $bc$  (see Figure 3(b));
5 }
```

Algorithm 5: Encoding of a block in last row (br)

```

1 encodeBlockLastRow( $br$ ){
2 begin
3   encode  $br$  using the same rules of encoding  $b$ , taking in
4   consideration different form of  $br$  (see Figure 3(c));
5 }
```

Algorithm 6: Pixelwise encoding

```

1 encodePixelWise(width of SI, height of SI){
2 begin
3   /* encoding of (width of SI)%4 pixels in last
4   row and (height of SI)%4 pixels in last
5   column. */
6   for each of these pixels do
7     if white then
8       randomly encode by 0 or 1 to both shares;
9     else
10      randomly encode by 0 or 1 to share 1 and by the
11      complement to share 2;
12 }
```

5. EXPERIMENTAL RESULTS

In this section, we present the experimental results of our proposed algorithm (NSNEA), which shows its correctness and efficiency. NSNEA is implemented using C# programming language on an Intel Core 2 Duo computer at 2.26 GHz and 4 GB ram. Table 1 shows a number of images with sizes 290×259 , 135×135 , 300×249 , and 225×225 besides their corresponding output reconstructed images which are of the same sizes as original images. From the output examples listed in Table 1, it is obvious that NSNEA satisfies its objective; *i.e.* non-expanded (and clear enough) reconstructed image.

6. CONCLUSION AND FUTURE WORK

Visual cryptography is a perfectly secure technique that encodes a secret image into random shares and the reconstruction of the image is by stacking (superimposing) the shares. Unfortunately, this

Algorithm 7: The New Simple Non-Expansion Algorithm

Input: The Secret Image (SI), C_0 , C_1

Output: Two shares: share1 and share2


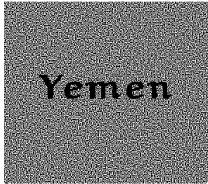






```

1 begin
2    $b$  is a block of four pixels;
3    $bc$  is a block of four pixels in last column;
4    $br$  is a block of four pixels in last row;
5    $n_0(b)$  is the number of 0's in  $b$ ;
6   width = width of SI - (width of SI)%2;
7   height = height of SI - (height of SI)%2;
8   for each  $b$  in SI (in the size width  $\times$  height) do
9     if  $n_0(b) == 4$  then
10      /*  $b$  is white */
11      encodeToWhite( $b$ );
12     else if  $n_0(b) == 3$  then
13      /*  $b$  is considered half white and half
14      black */
15      switch ( $b$ ) do
16        case 1000
17          encodeUsingC0I( $b$ , 1);
18        case 0100
19          encodeUsingC0I( $b$ , 2);
20        case 0010
21          encodeUsingC0I( $b$ , 3);
22        case 0001
23          encodeUsingC0I( $b$ , 4);
24     else if  $n_0(b) == 2$  then
25       if  $b = 1001$  or  $b = 0110$  then
26         encodeUsingC0I( $b$ , 5);
27       else
28         encodeToBlack( $b$ );
29     else
30       encodeToBlack( $b$ );
31   if (width of SI)%2 == 1 then
32     encodeBlockLastColumn( $bc$ );
33   if (height of SI)%2 == 1 then
34     encodeBlockLastRow( $br$ );
35   if (width of SI)%4  $\neq$  0 OR (height of SI)%4  $\neq$  0 then
36     encodePixelWise(width of SI, height of SI);
```

scheme leads to the degradation in the quality of the recovered images and in image size expansion. In this paper, we have introduced a non-expansion algorithm for (2, 2)-VSS scheme which solves the problem of pixel expansion. The principle of this scheme is to encode the secret image in 4-pixel blocks with each block is assigned to a 4-pixel block in each of the two shares according to the number of white pixels in the block. The shares (transparencies) produced by this algorithm and the reconstructed image are not expanded in size, and all have the same size as the original (secret) image. The introduced algorithm (NSNEA) is tested and it is found that it gives the result which is intended for.

Our future work will concentrate on enhancing the contrast of the reconstructed image.

Table 1. Some Recovered Images Using Our Algorithm

No.	Original Image	Recovered Image
1	 <p>Yemen</p> <p>290×259</p>	 <p>Yemen</p> <p>290×259</p>
2	 <p>135×135</p>	 <p>135×135</p>
3	 <p>300×249</p>	 <p>300×249</p>
4	 <p>225×225</p>	 <p>225×225</p>

7. REFERENCES

- [1] Thekra Abbas and Zou Bei. A novel non-expansion visual secret sharing scheme for binary image. *International Journal of Digital Content Technology and its Applications (JDCTA)*, 4(6):106–114, 2010.
- [2] Shyamal Kumar Mondal Biswapati Jana, Gargi Hait. Survey on size invariant visual cryptography. *International Journal of Computer Science and Information Technologies(IJCSIT)*, 5(3):3985–3990, 2014.
- [3] Y. F. Chen, Y. K. Chan, C. C. Huang, M. H. Tsai, and Y. P. Chu. A multiple-level visual secret-sharing scheme without image size expansion. *Information Sciences*, 177(21):4696–4710, November 2007.
- [4] Young-Chang Hou. Visual cryptography for color images. *Pattern Recognition*, 36, 2003.
- [5] Yi-Jing Huang and Jun-Dong Chang. Non-expanded visual cryptography scheme with authentication. *IEEE 2nd International Symposium on Next-Generation Electronics (ISNE)*, February 25–26 2013.
- [6] Ryo Ito, Hidenori Kuwakado, and Hatsukazu Tanaka. Image size invariant visual cryptograph. *IEICE Trans. Fundam. Elect. Commun. Comput. Sci.*, E82-A(10):2172–2177, 1999.
- [7] Abdullah Jaafar and Azman Samsudin. A survey of black-and-white visual cryptography models. *International Journal of Digital Content Technology and its Applications(JDCTA)*, 6(15):237–249, August 2012.
- [8] M. Naor and A. Shamir. Visual cryptography. In *Proceeding of Advances in Cryptology EUROCRYPT'94, Lecture Notes in Computer Science*, volume 950, pages 1–12. Springer-Verlag, 1995.
- [9] Pooja and Dr.Lalitha Y. S. Non expanded visual cryptography for color images using pseudo-randomized authentication. *International Journal of Engineering Research and Development*, 10(6):01–08, June 2014.
- [10] Ching-Lin Wang, Ching-Te Wang, and Meng-Lin Chiang. The image multiple sharing schemes without pixel expansion. In *International Conference on Machine Learning and Cybernetics*, volume 4, Guilin, 10–13 July 2011.
- [11] Jonathan Weir and WeiQi Yan. A comprehensive study of visual cryptography. *Transactions on DHMS V, LNCS*, 6010, 2010.
- [12] C. N. Yang. New visual secret sharing schemes using probabilistic method. *Pattern Recognition Letter*, 25(4):481–494, 2004.