An Extended Multi-secret Images Sharing Scheme Based on Boolean Operation

Huan Wang, Mingxing He, and Xiao Li

School of Mathematics and Computer Engineering,
Xihua University, 610039, Chengdu, China
{ideahuan18,hemingxing64}@gmail.com, lxgbxh@126.com

Abstract. An extended multi-secret images scheme based on Boolean operation is proposed, which is used to encrypt secret images with different dimensions to generate share images with the same dimension. The proposed scheme can deal with grayscale, color, and the mixed condition of grayscale and color images. Furthermore, an example is discussed and a tool is developed to verify the proposed scheme.

Keywords: Visual cryptography, Boolean operation, Image sharing, Multi-secret images.

1 Introduction

In traditional confidential communication systems, encryption methods are usually used to protect secret information. However, the main idea of the encryption methods is to protect the secret key [1]. The concept of visual cryptography is introduced by Naor and Shamir [2], which is used to protect the secret key.

Furthermore, there are a lot of works which are based on multiple-secret sharing schemes. Wang *et al.* [3] develop a probabilistic $(2, n)$ scheme for binary images and a deterministic (n, n) scheme for grayscale image. Shyu *et al.* [4] give a visual secret sharing scheme that encodes secrets into two circle shares such that none of any single share leaks the secrets. Chang *et al.* [5] report two spatial-domain image hiding schemes with the concept of secret sharing.

Moreover, many works are based on Boolean operation. Chen *et al.* [6] describe an efficient $(n+1, n+1)$ multi-secret image sharing scheme based on Boolean-based virtual secret sharing to keep the secret image confidential. Guo *et al.* [7] define multi-pixel encryption visual cryptography scheme, which encrypts a block of $t(1 \leq t)$ pixels at a time. Chen *et al.* [8] describe a secret sharing scheme to completely recover the secret image without the use of a complicated process using Boolean operation. Li et al. [9] give an improved aspect ratio invariant visual cryptography scheme without optional size expansion.

In addition, visual cryptography is used in some other fields. Wu *et al.* [10] propose a method to handle a secret image to n stego images with the $1/t$ size of the secret image. Yang *et al.* [11] design a scheme based on the trade-off between the usage of big and small blocks to address misalignment problem. Bose and

K. Mustofa et al. (Eds.): ICT-EurAsia 2013, LNCS 7804, pp. 513–518, 2013.

Pathak *et al.* [12] find the best initial condition for iterating a chaotic map to generate a symbolic sequence corresponding to the source message.

These works are interesting and efficient but sometimes weakness, such as pixel expansion problems [2] and all the secret images should have the same dimension. However, generally, the secret images may have different dimension. Therefore, we propose an extended multi-secret images sharing scheme based on Boolean operation to encrypt multi-secret images with the different dimension. Moreover, the generated share images have the same dimension, then they do not reveal any information about the secret images include their dimension.

The rest of this paper is organized as follows. Section 2 gives the basic definitions. In section 3, an extended multi-secret images sharing scheme is proposed. An experimental is presented in Section 4. Section 5 concludes this paper.

2 Preliminaries

In this section, an extended-OR operation and an extended-OR operation chain between any two different dimensions images are defined. Let $x = 30$ and $y = 203$, then $x \oplus y = 00011110 \oplus 11001011 = 11010101 = 213$. Where, "$\oplus$" is bitwise exclusive-OR operation. Furthermore, The exclusive-OR operation between any two grayscale or color images with the same dimension is defined in [6].

Definition 1. *Let $A(a_{ij})$ and $B(b_{ij})$ be two images with **different dimensions** $m \times n$ and $h \times w$, respectively, where $m \times n \neq h \times w$, $0 \leq a_{ij} \leq 255, 0 \leq b_{ij} \leq 255$. The **extended-OR operation** between A and B is defined as follows.*

1) $A_{m\times n}\overline{\oplus'}B_{h\times w} = A_{m\times n} \oplus B'_{m\times n}$. Where, B' is a temporary matrix. If $m \times n \leq h \times w$, B' orderly takes $m \times n$ pixels from the head of B. Otherwise, B' circularly and orderly takes $m \times n$ pixels from the head of B.

2) $A_{m\times n}\overline{{}'\oplus}B_{h\times w} = A'_{h\times w} \oplus B_{h\times w}$. Where, A' is a temporary matrix. If $m \times n > h \times w$, A' orderly takes $h \times w$ pixels from the head of A. Otherwise, A' circularly and orderly takes $h \times w$ pixels from the head of A.

a_{11}	a_{12}	a_{13}
a_{21}	a_{22}	a_{23}

Image *A*

b_{11}	b_{12}	b_{13}
b_{21}	b_{22}	b_{23}
b_{31}	b_{32}	b_{33}

Image *B*

(a)

	1	2	3	4	5	6	7	8	9
A	a_{11}	a_{12}	a_{13}	a_{21}	a_{22}	a_{23}	–	–	–
B	b_{11}	b_{12}	b_{13}	b_{21}	b_{22}	b_{23}	b_{31}	b_{32}	b_{33}
B′	b_{11}	b_{12}	b_{13}	b_{21}	b_{22}	b_{23}	–	–	–
C	c_{11}	c_{12}	c_{13}	c_{21}	c_{22}	c_{23}	–	–	–

(b)

	1	2	3	4	5	6	7	8	9
A	a_{11}	a_{12}	a_{13}	a_{21}	a_{22}	a_{23}	–	–	–
B	b_{11}	b_{12}	b_{13}	b_{21}	b_{22}	b_{23}	b_{31}	b_{32}	b_{33}
A′	a_{11}	a_{12}	a_{13}	a_{21}	a_{22}	a_{23}	a_{11}	a_{12}	a_{13}
C	c_{11}	c_{12}	c_{13}	c_{21}	c_{22}	c_{23}	c_{31}	c_{32}	c_{33}

(c)

Fig. 1. An example for $\overline{\oplus'}$ and $\overline{{}'\oplus}$ operation

Example: Let $A_{2\times 3}$ and $B_{3\times 3}$ be two images, as shown in Fig.1 (a), the extended-OR operation between A and B are: $A_{2\times 3}\overline{\oplus'}B_{3\times 3} = A_{2\times 3} \oplus B'_{2\times 3}$, as shown in Fig.1 (b), and $A_{2\times 3}\overline{{}'\oplus}B_{3\times 3} = A'_{2\times 3} \oplus B_{2\times 3}$, as shown in Fig.1 (c).

Definition 2. *Let $A_1, A_2, \cdots, A_k$ be $k(k > 1)$ images with different dimensions. The* ***extended-OR operation chain*** *is defined as $\psi_{i=1}^{k} A_i = A_1 \overline{\oplus'} A_2 \overline{\oplus'} \cdots \overline{\oplus'} A_k$. Here, $A_1 \overline{\oplus'} A_2 \neq A_2 \overline{\oplus'} A_1$ unless A_1 and A_2 have the same dimension.*

3 The Sharing and Reconstruction of Multi-secret Images

In this section, n secret images with different dimensions can be encrypted to $n+1$ share images with the same dimension. $S_l, \cdots, S_m$ are denoted as $S_{[l,m]}$.

3.1 The Sharing Process

Sharing Algorithm: the sharing process is composed of following two parts.

Part1. For n secret images $G_{[0,n-1]}$, $n+1$ temporary images $S'_{[0,n]}$ with different dimensions are generated by following three steps.

(I) A random integer matrix is generated, which is the first temporary image S'_0 with the same dimension as G_1. Here, $\forall x \in S'_0$, $0 \leq x \leq 255$.

(II) According to S'_0 and the n secret images $G_{[0,n-1]}$, $n-1$ interim matrices $B_{[1,n-1]}$ are computed by $B_k = G_k \overline{\oplus'} S'_0$, $k = 1, 2, \cdots, n-1$.

(III) The other n temporary images $S'_{[1,n]}$ are computed by: a) $S'_1 = B_1$; b) $S'_k = B_k \overline{\oplus'} B_{k-1}$ if $k = 2, \cdots, n-1$; and c) $S'_n = G_0 \overline{\oplus'} B_{n-1}$.

Part2. $n+1$ share images $S_{[0,n]}$ with the same dimension can be generated by the $n+1$ temporary images $S'_{[0,n]}$ by the following steps.

(I) Extract the widths ($w_{[0,n-1]}$) and heights ($h_{[0,n-1]}$) of the n secret images $G_{[0,n-1]}$. Let $G^{wh}_{[0,n-1]}$ be n matrices with the same dimension 2×3, which are used to save the $w_{[0,n-1]}$ and $h_{[0,n-1]}$, respectively. We have:

$$G_i^{wh} = \begin{pmatrix} w_i^1 & w_i^2 & w_i^3 \\ h_i^1 & h_i^2 & h_i^3 \end{pmatrix}, where \begin{cases} w_i = w_i^1 \times w_i^2 \times w_i^3 & ,1 \leq w_i^k \leq 255 \\ h_i = h_i^1 \times h_i^2 \times h_i^3 & ,1 \leq h_i^k \leq 255 \end{cases}$$

Therefore, $G^{wh}_{[0,n-1]}$ can be considered as the new n secret images. Then, the new $n+1$ temporary images S_i^{wh} are generated from G_i^{wh} using Part1.

(II) According to $S'_{[0,n]}$ and S_i^{wh}, the $n+1$ share images $S_{[0,n]}$ can be computed as following steps.

(1) Let $M_w = max\{w_i\}$ and $M_h = max\{h_i\} + 1$.

(2) Generate $n+1$ empty images $S_{[0,n]}$ with dimension $M_w \times M_h$ and copy all the elements of $S'_{[0,n]}$ to $S_{[0,n]}$, respectively. The last lines of $S_{[0,n]}$ are empty.

(3) Copy all the elements of $S^{wh}_{[0,n]}$ to the last line of $S_{[0,n]}$, respectively.

(4) Fill in the rest of the $n+1$ images $S_{[0,n]}$ with the random numbers which are belong to 0 and 255.

Finally, the $n+1$ share images are generated with the same dimension $M_w \times M_h$. The proposed sharing scheme is shown in Fig.2.

Theorem 1. *Assume that n secret images $G_{[0,n-1]}$ with different dimensions are encrypted to $n+1$ share images $S_{[0,n]}$. All the share images cannot reveal any information independently.*

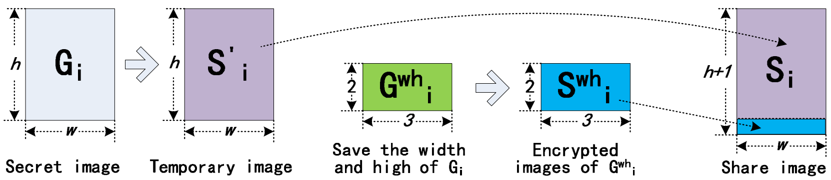


Fig. 2. Sharing process and the structure of share image

Proof: Since S_0 is a random matrix, then, obviously, $B_k = G_k\overline{'\oplus}S_0$ are still random matrixes. Furthermore, all S_k which are computed from B_k are also random matrices. Where, $k = 1, 2, \cdots, n-1$. Therefore, all the share images have the randomness, then they cannot leak any information independently.

3.2 The Reconstruction Process

Part1. The width and height of each secret image can be obtained from $S_{[0,n]}$.

(I) For the $n+1$ share images $S_{[0,n]}$, extract the $n+1$ temporary images $S^{wh}_{[0,n]}$ with the dimension 2×3 from the head of the last lines of $S_{[0,n]}$, respectively.

(II) The $n+1$ temporary images $S^{wh}_{[0,n]}$ can be decrypted using the following Part2 to obtain other $n+1$ temporary image $G^{wh}_{[0,n]}$ with the dimension 2×3.

(III) Let w_i^1, w_i^2, w_i^3 (h_i^1, h_i^2, h_i^3) be the first (second) line of G_i^{wh}, then $w_i = w_i^1 \times w_i^2 \times w_i^3$ $(h_i = h_i^1 \times h_i^2 \times h_i^3)$ is the width (high) of secret image G_i.

(IV) The $n+1$ temporary images $S'_{[0,n]}$ can be obtained from the $n+1$ share images $S_{[0,n]}$ according to the widths and highs in step III.

Part2. The n secret images $S_{[0,n]}$ can be obtained according to $S'_{[0,n]}$.

(I) The first secret image $G_0 = S_n\overline{\oplus'}B_{n-1} = S_n\overline{\oplus'}(S_{n-1}\overline{\oplus'}B_{n-2} = S_n\overline{\oplus'}(S_{n-1}$ $\overline{\oplus'}(S_{n-2}\overline{\oplus'}B_{n-3})) = S_n(\overline{\oplus'}(S_{n-1}\overline{\oplus'}(S_{n-2}(\overline{\oplus'}, \cdots, (S_2\overline{\oplus'}S_1))\cdots)$.

(II) $n-1$ interim matrices B_k are generated by: $B_1 = S'_1$ and $B_k = S'_k\overline{\oplus'}B_{k-1}$, $k = 2, \cdots, n-1$.

(III) The other secret images are computed by $G_k = B_k\overline{\oplus'}S_0$, $1 \le k \le n-1$.

Theorem 2. *Assume that n secret images $G_{[0,n-1]}$ with different dimensions are encrypted to $n+1$ share images $S_{[0,n]}$, then the secret images $G_{[0,n-1]}$ can be correctly reconstructed using the $n+1$ share images $S_{[0,n]}$.*

Proof: If $k = 0$: We have $\Psi^n_{i=1}S_i = S_1\overline{\oplus'}S_2\overline{\oplus'}\cdots\overline{\oplus'}S_n = B_1\overline{\oplus'}(B_2\overline{\oplus'}B_1)\overline{\oplus'}\cdots\overline{\oplus'}$ $(B_{n=1}\overline{\oplus'}B_{n-2})\overline{\oplus'}(G_0\overline{\oplus'}B_{n-1}) = G_0$. If $k \ge 1$: We have $\Psi^k_{i=0}S_i = S_0\overline{\oplus'}S_1\overline{\oplus'}\cdots\overline{\oplus'}S_k = S_0\overline{\oplus'}B_1\overline{\oplus'}(B_2\overline{\oplus'}B_1)\overline{\oplus'}\cdots\overline{\oplus'}(B_k\overline{\oplus'}B_{k-1}) = S_0\overline{\oplus'}B_k = G_k$.

3.3 Color Images and the Mixed Condition of Grayscale/Color Images

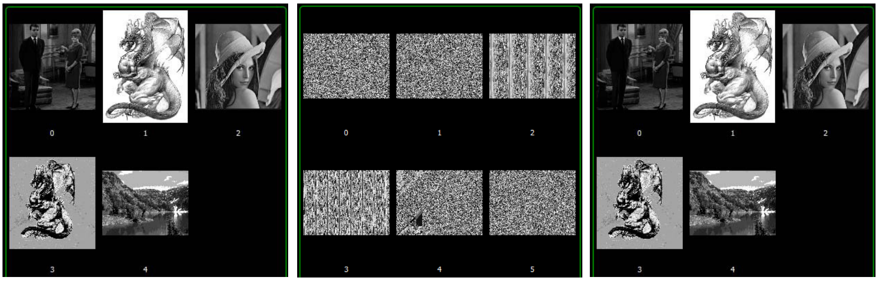
The difference between handling color and grayscale images is that each pixel of 24-bit color images can be divided into three pigments, i.e., red (r), green (g), and blue (b). We have $A\overline{\oplus'}B = [a_{i,j,k}\overline{\oplus'}b_{i,j,k}]$, where $k = r, g, b$.

For the mixed condition, each color image is divided into three (red, green, and blue) identical grayscale images. Let A be grayscale image and B be color image, we have $A\overline{\oplus'}B = [a_{i,j}\overline{\oplus'}b_{i,j,k}]$, where $k = r$ (red), g (green), b (blue).

4 Verification and Discussion

To verify the correctness of the proposed extended scheme, a tool is developed.

Example: There are five secret grayscale images G_0, G_1, G_2, G_3, G_4 with the dimensions 256×256, 360×477, 256×256, 196×210, 640×480, as shown in Fig.3(a). Here, $M_w = 640$ and $M_h = 480 + 1 = 481$. Then, the five secret images are encrypted and extended to six share images with the same dimension 640×481 using our tool, as shown in Fig.3(b). The reconstructed images are also decrypted using this tool, as shown in Fig.3(c). However, it is unsatisfactory that using these schemes developed in [3–12] to encrypt the five secret images since for any two secret images, some pixels in the bigger (dimension) secret image is out of the operation range for the smaller one and these pixels certainly cannot be encrypted. The comparison of these schemes is shown in Table 1.



(a) Five secret images (b) Six share images (c) Five reconstructed images

Fig. 3. An example with five secret images

Table 1. Comparison of these schemes

Schemes	Pixel expansion	Image distortion	Dimension restriction
In [3, 12]	No	Yes	Yes
In [4, 5]	Yes	Yes	Yes
In [6, 8]	No	No	Yes
In [7, 9]	Yes	No	Yes
In [10, 11]	No	Yes	Yes
This paper	No	No	No

5 Conclusions

An extended multi-secret image sharing scheme based on Boolean operation is proposed, which can share multi-secret images with different dimension. The grayscale and color images are appropriated in our scheme. Furthermore, this scheme can handle the mixed condition of grayscale and color images and the share images do not suffering pixel expansion. Moreover, the reconstructed secret images are the same dimension. In addition, all share images cannot leak any information about the secret images include the dimensions.

Acknowledgments. This work is supported by the National Nature Science Foundation of China (No. 60773035), the International Cooperation Project in Sichuan Province (No. 2009HH0009) and the fund of Key Disciplinary of Sichuan Province (No. SZD0802-09-1).

References

1. Shamir, A.: How to Share a Secret. Communications Assocating Computer 22(11), 612–613 (1979)
2. Naor, M., Shamir, A.: Visual Cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995)
3. Daoshun, W., Zhang, L., Ning, M., Xiaobo, L.: Two Secret Sharing Schemes Based on Boolean Operations. Pattern Recognition 40(10), 2776–2785 (2007)
4. Shyu, S.J.: Sharing Multiple Secrets in Visual Cryptography. Pattern Recognition 40(12), 3633–3651 (2007)
5. Chinchen, C., Junchou, C., Peiyu, L.: Sharing a Secret Two-tone Image in Two Gray-level Images. In: 11th International Conference on Parallel and Distributed Systems, pp. 300–304. IEEE Press, Tainan (2005)
6. Tzung, H.C., Chang, S.W.: Efficient Multi-secret Image Sharing Based on Boolean Operations. Signal Processing 6(12), 90–97 (2011)
7. Guo, T., Liu, F., Wu, C.: Multi-pixel Encryption Visual Cryptography. In: Wu, C.-K., Yung, M., Lin, D. (eds.) Inscrypt 2011. LNCS, vol. 7537, pp. 86–92. Springer, Heidelberg (2012)
8. Yihui, C., Peiyu, L.: Authentication Mechanism for Secret Sharing Using Boolean Operation. Electronic Science and Technology 10(3), 195–198 (2012)
9. Peng, L., Peijun, M., Dong, L.: Aspect Ratio Invariant Visual Cryptography Scheme with Optional Size Expansion. In: Eighth Intelligent Information Hiding and Multimedia Signal Processing, pp. 219–222. IEEE Press, Piraeus (2012)
10. Yus, W., Chihching, T., Jachen, L.: Sharing and Hiding Secret Images with Size Constraint. Pattern Recognition 37(7), 1377–1385 (2004)
11. Chingnung, Y., Anguo, P., Tseshih, C.: Misalignment Tolerant Visual Secret Sharing on Resolving Alignment Difficulty. Signal Processing 89(8), 1602–1624 (2009)
12. Bose, R., Pathak, S.: A Novel Compression and Encryption Scheme Using Variable Model Arithmetic Coding and Coupled Chaotic System. IEEE Transactions on Circuits and Systems-I: Regular Papers 53(4), 848–856 (2006)