Novel (*n*, *n*) secret image sharing scheme based on addition

Lin Dong, Min Ku
Department of computer science and technology
Tsinghua University
Beijing, China
donglin06@mails.tsinghua.edu.cn

***Abstract*—In this paper, we propose a novel (*n*, *n*) secret image sharing scheme. The construction of shares is based on matrix multiplication and the revealing is based on addition. The proposed scheme has no pixel expansion and can reconstruct the secret image precisely. It can be directly used to share grayscale images and can be easily extended to deal with the binary and color images. Experimental results show that the proposed scheme is efficient.**

Keywords- secret image sharing; matrix; addition;complexity; contrast

I. Introduction

Secret sharing (SS), which was first proposed by Blakley [1] and Shamir [2] independently, encode a secret into *n* shares. The secret can only be reconstructed from any *k* or more shares. Knowledge of *k*-1 or fewer shares provides absolutely no information about the secret. SS can not only guarantee the security of information, but also greatly reduce the possibility of secret inaccessible due to misfortune or betrayal, thus it has attracted many scholars' attention. A secret sharing scheme can be evaluated by its security, contrast(reconstruction precision), computational complexity, and pixel expansion (storage requirement).

With the development of multimedia technology, secret information may no longer be a simple key, but image, audio and so on [12]. In this paper, we study secret image sharing (SIS). According to different reconstruction approaches, the existing SIS schemes can be divided into three categories. The category I used the traditional SS schemes to share images by treating each pixel to be a value [3][4]. They can reconstruct the secret image precisely, however, the complexity is quite high. Computational complexity of (*n*, *n*) scheme is $O(n\log^2 n)$. The category II is visual secret sharing (VSS) schemes, proposed by Naor and Shamir[5]. Shares are stacked to recover the secret image which is equal to OR operation. This approach utilizes the human visual system to recover the secret image and requires little or no computation. In [5], two (*n*, *n*) schemes were proposed for binary images, the pixel expansion is 2^k and 2^{k-1} and contrast is $1/2^k$ and $1/2^{k-1}$ respectively. Iwamoto[6] proposed optimal (*n*, *n*) VSS scheme for grayscale images based on polynomial representation of basis matrices with minimum pixel expansion be $2^{n-1}(g-1)$, where *g* is the number of gray levels. Cimato[7] used canonical schemes to provide a constructive proof of optimality of *c*-color (*n*, *n*)-threshold VSS schemes. The lower bound expansion is $c2^{n-1}-1$ if *n* is even while $c2^{n-1}-c+1$ if *n* is odd. We can see that VSS has disadvantages of pixel expansion and low contrast. The category III utilizes XOR operation to recover the secret image, which was proposed by Tuyls[8]. Tuyls[8] proposed (*n*, *n*) scheme for binary images with no pixel expansion and precisely reconstructed image. Yi[9] presented two (*n*, *n*) schemes for color image. The schemes also have no pixel expansion; however the secret image was not precisely reconstructed with contrast 1/4. Wang[10] proposed (*n*, *n*) scheme for grayscale image. The scheme has no pixel expansion and gives an exact reconstruction. All schemes in [8-10] are constructed based on Boolean operation, which need bit-wise operation when sharing grayscale and color images.

Nowadays, although more devices or sensors have had a certain amount of computing power, the computing power is not enough to perform complex cryptography computation. Thus, how to develop secret sharing scheme with low computation complexity and high contrast is worth to study. However, to construct such (*k*, *n*) scheme is very difficult. (*n*, *n*) scheme is the special case of (*k*, *n*) scheme, and more important it helps to construct the (*k*, *n*) scheme. For example, [11] proposed a method to extend (*n*, *n*) scheme to (*k*, *n*) scheme by using shadows-assignment matrix.

Based on this, we propose a new category of SIS scheme in this paper. Its reconstruction is based on addition which has low computational complexity. The proposed (*n*, *n*) secret image sharing scheme has no pixel expansion and can recover the secret image precisely. It can not only directly deal with the grayscale images, but also can be easily extended to the binary images and the color images.

II. Preliminaries

In this section, we will give some denotations and facts which are necessary in the following.

Consider a grayscale secret image *A* with size $h \times w$. The darkness of each pixel can be described by gray level. Usually there are 256 gray levels which are represented by $0,\ldots,255$. Thus image *A* can be represented by a matrix $A = [a_{ij}]_{h \times w}$, where $i = 1,\ldots,h$, $j = 1,\ldots,w$, $a_{ij} \in \{0,\ldots,255\}$. Assume that $X = [x_{ij}]_{p \times r}$ and $Y = [y_{ij}]_{r \times q}$. $Z = X * Y$ is the product of the matrices *X* and *Y*, where $z_{ij} = \sum_t x_{it} y_{tj}$ and "$*$" is named matrix multiplication.

Suppose that *A* is a matrix with size $h \times w$, *I* is a unit matrix with size $h \times h$ and $R_{i_1},\ldots,R_{i_k}$ are independently

978-0-7695-4222-5/10 $26.00 © 2010 IEEE
DOI 10.1109/IIHMSP.2010.148

random matrices, each element of which belongs to $\{0,\ldots,255\}$. Then we have some obvious properties as follows.

Property 1: $I * A = A$.

Property 2: If $R = R_{i_1} + \ldots + R_{i_k}$, then R is a random matrix.

Property 3: If $B = R * A$ and elements in each column of A are not all 0, then B is a random matrix.

Property 4: If $T = I - R$, then T is random matrix.

Next, we will give the definition of secret sharing scheme.

Definition[2]: A (k,n) secret sharing scheme divides a secret s into n shares $s_1,\ldots,s_n$, such that the following conditions are satisfied.

(C1): The secret s is recoverable from any k shares, i.e., for any set of k indices, $H(s \mid (s_{i_1},\ldots,s_{i_k})) = 0$.

(C2): Knowledge of k-1 or fewer shares provides absolutely no information about s, i.e., for any set of k-1 indices, $H(s \mid (s_{i_1},\ldots,s_{i_{k-1}})) = H(s)$.

Where $H(s)$ denotes the uncertainty of s, $H(a \mid b)$ denotes the uncertainty of a when event b happened.

The first condition is called precision and the second condition is called security. When $k = n$, it is the definition of (n,n) secret sharing scheme.

III. Proposed (*N*, *N*) Secret Image Sharing Schemes

Novel (*n*, *n*) secret image sharing schemes are proposed in this section.

A. Proposed scheme for grayscale image

The proposed (*n*, *n*) secret image sharing scheme for grayscale image, which consists of shares construction phase and revealing phase, is given as follows.

Proposed scheme: (n, n) secret image sharing scheme

Input: grayscale secret image *A* with size $h \times w$

Output: shadow image $S_i, i \in \{1,\ldots,n\}$

Share construction:

*Step**: get permutated image *PA* by using a key to generate a permutation sequence to permute the pixels of *A*.

Step1: generate *n*-1 random matrices $R_1,\ldots,R_{n-1}$, each of which has size $h \times h$ and element be $\{0,\ldots,255\}$.

Step2: compute $R_n = (I - R_1 - \cdots - R_{n-1}) \bmod 256$, where I is unit matrix with size $h \times h$.

Step3: compute $S_i = (R_i * PA) \bmod 256$, where "$*$" means matrix multiplication.

Revealing:

Step1: $PA' = (S_1 + \ldots + S_n) \bmod 256$.

*Step**: apply inverse-permutation operation to PA' to get the reconstructed image A'.

To increase the security of the secret image, "Step*" in share construction and revealing phase, which are mutually inverse and optional, are used to relocate the pixels of secret image.

An example is given here to demonstrate the proposed secret image sharing phase.

Example. A (3, 3) secret image sharing scheme.

Input: grayscale image $A = \begin{bmatrix} 133 & 167 \\ 134 & 208 \end{bmatrix}$

Share construction:

*Step**: $PA = \begin{bmatrix} 134 & 133 \\ 208 & 167 \end{bmatrix}$

Step1: $R_1 = \begin{bmatrix} 171 & 251 \\ 101 & 254 \end{bmatrix}$, $R_2 = \begin{bmatrix} 172 & 136 \\ 52 & 192 \end{bmatrix}$.

Step2: $R_3 = I - R_1 - R_2$

$$= \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 171 & 251 \\ 101 & 254 \end{bmatrix} - \begin{bmatrix} 172 & 136 \\ 52 & 192 \end{bmatrix} \right) \bmod 256 = \begin{bmatrix} 170 & 125 \\ 103 & 67 \end{bmatrix}.$$

Step3: get three shares by computing

$$S_1 = (R_1 * PA) \bmod 256 = \left(\begin{bmatrix} 171 & 251 \\ 101 & 254 \end{bmatrix} * \begin{bmatrix} 134 & 133 \\ 208 & 167 \end{bmatrix} \right) \bmod 256 = \begin{bmatrix} 114 & 148 \\ 62 & 43 \end{bmatrix},$$

$$S_2 = (R_2 * PA) \bmod 256 = \left(\begin{bmatrix} 172 & 136 \\ 52 & 192 \end{bmatrix} * \begin{bmatrix} 134 & 133 \\ 208 & 167 \end{bmatrix} \right) \bmod 256 = \begin{bmatrix} 136 & 20 \\ 56 & 68 \end{bmatrix},$$

$$S_3 = (R_3 * PA) \bmod 256 = \left(\begin{bmatrix} 170 & 125 \\ 103 & 67 \end{bmatrix} * \begin{bmatrix} 134 & 133 \\ 208 & 167 \end{bmatrix} \right) \bmod 256 = \begin{bmatrix} 140 & 221 \\ 90 & 56 \end{bmatrix}.$$

Revealing: The reconstructed secret image is

Step1: $PA' = (S_1 + S_2 + S_3) \bmod 256$

$$= \left(\begin{bmatrix} 114 & 148 \\ 62 & 43 \end{bmatrix} + \begin{bmatrix} 136 & 20 \\ 56 & 68 \end{bmatrix} + \begin{bmatrix} 140 & 221 \\ 90 & 56 \end{bmatrix} \right) \bmod 256 = \begin{bmatrix} 134 & 133 \\ 208 & 167 \end{bmatrix} = PA.$$

*Step**: $A' = \begin{bmatrix} 133 & 167 \\ 134 & 208 \end{bmatrix} = A$

Note that the reconstructed secret image is exactly the same with the original secret image.

In the following, we will prove the proposed scheme is a (*n*, *n*) secret image sharing scheme.

Theorem: The proposed scheme is a (*n*, *n*) secret image sharing scheme, which has no pixel expansion and can recover the secret image precisely.

Proof: since "Step*" in share construction and revealing phase are mutually inverse, we just need to find the relationship of *PA* and PA'. As space limitation, we omit "mod 256" in the following proof. We prove the theorem by two steps as follows:

(i) *n* shadows, i.e., $S_1,\ldots,S_n$, are collected to reconstruct the secret image.

According to the share construction phase and revealing phase, by means of Property 1, we have

$$PA' = S_1 + \ldots + S_n = R_1 * PA + \ldots + R_n * PA = (R_1 + \ldots + R_n) * PA$$
$$= (R_1 + \ldots + R_{n-1} + I - R_1 - \ldots - R_{n-1}) * PA = I * PA = PA.$$

This means the secret image *A* is recoverable from *n* shares, i.e., $H(A \mid (S_1,\ldots,S_n)) = 0$. That is to say the scheme satisfies the condition (C1).

(ii) k ($k < n$) shadows, i.e. $S_{i_1},\ldots,S_{i_k}$, are collected to reconstruct the secret image.

Compute A' according to the revealing phase as follows

$$PA' = S_{i_1} + \ldots + S_{i_k} = R_{i_1} * PA + \ldots + R_{i_k} * PA$$
$$= (R_{i_1} + \ldots + R_{i_k}) * PA$$

Denote $R = R_{i_1} + \ldots + R_{i_k}$. We consider two cases. Case 1 is for $n \notin \{i_1, \ldots, i_k\}$ and case 2 is for $n \in \{i_1, \ldots, i_k\}$.

Case 1: $n \notin \{i_1, \ldots, i_k\}$. Since $R_{i_1}, \ldots, R_{i_k}$ are independently random matrices, according to Property 2, R is random matrix too. By Property 3, $PA' = R * PA$ is random matrix with each element belonging to the set $\{0,1,\ldots,255\}$. That is to say we know nothing about the secret image A.

Case 2: $n \in \{i_1, \ldots, i_k\}$. Without loss of generality, we suppose $i_k = n$. According to *Step 2* of the share construction phase, $R_n = I - R_1 - \cdots - R_{n-1}$, where I is unit matrix, thus

$$R = R_{i_1} + \ldots + R_{i_{k-1}} + R_{i_k} = R_{i_1} + \ldots + R_{i_{k-1}} + R_n$$
$$= R_{i_1} + \ldots + R_{i_{k-1}} + I - R_1 - \cdots - R_{n-1} = I - \sum_{t<n\&t\notin\{i_1,\ldots,i_{k-1}\}} R_t$$

Since matrices $R_1, \ldots, R_{n-1}$ are independently random matrices, according to Property 2, $\sum_{t<n\&t\notin\{i_1,\ldots,i_{k-1}\}} R_t$ is random matrix too. According to Property 4, $R = I - \sum_{t<n\&t\notin\{i_1,\ldots,i_{k-1}\}} R_t$ is also random matrix. According to Property 3, $PA' = R * PA$ is random matrix with each element belonging to the set $\{0,1,\ldots,255\}$ .That is to say we know nothing about the secret image A.

From *case 1* and *case 2*, we know that knowledge of k ($k < n$) shares provides absolutely no information about secret image A, i.e., $H(A \mid (S_{i_1}, \ldots, S_{i_k})) = H(A)$. That is to say the scheme satisfies the condition (C2).

To sum up, our proposed scheme satisfies the conditions (C1) and (C2) of the above Definition, it is a (n, n) secret image sharing scheme. The scheme can reconstruct the secret image precisely. All shares and reconstructed secret image has the same size with the original secret image, thus no pixel expansion. Addition operation is used to reconstruct the secret image, which has low computational complexity. □

B. *Proposed schemes for binary and color image*

A binary image is an image that has only two possible values for each pixel. Typically the two colors used for a binary image are black and white. Each pixel is stored as a single bit 1 or 0. For binary image, in order to use the proposed scheme, a preprocessing step should be added to convert the binary image to corresponding grayscale image by combining every neighboring 8 bits to 1 byte. Then perform the proposed scheme for the grayscale image. In revealing phase, a corresponding step should be added to split 1 byte of the revealed grayscale image into 8 bits to get the recovered secret image.

For color image, any desired colors can be obtained by mixing primitive colors red (R), green (G) and blue (B). In true color system, R, G and B are respectively represented by 8 bits which can represent 0-255 variation of scale. To extend the proposed schemes for grayscale image to color image, three steps are needed. Firstly, decompose the color image into three components of R, G and B, each of which can be seen as grayscale image. Then perform the proposed scheme for grayscale image to each component R, G and B. Finally, compose R, G and B components to color shares.

IV. Experimental Result and Comparison

Experimental results and comparison of the proposed SIS schemes with previous schemes are illustrated in this section. In the following experiments, "Step*" is not include to illustrate the proposed scheme.

A. *Experimental result*

Experiment A: Construct (3, 3) secret image sharing scheme on grayscale secret image. Experimental results are showed in Fig.1: (a) is the grayscale secret image "lena.jpg", with size 200×200 ; (b)-(d) are the three shares generated by using the proposed method; (e) is the image revealed by share 1 and share 2 and (e) is random images which gives nothing about the secret image; (f) is the image revealed by all three shares and (f) is identical to (a).

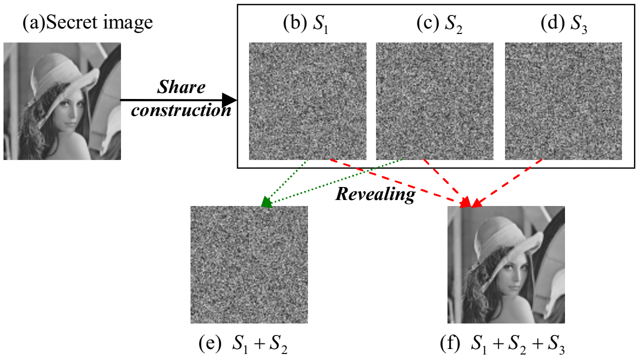

Figure 1. (3, 3) secret image sharing scheme for grayscale secret image.

Experiment B: Construct (3, 3) secret image sharing scheme on binary secret image. Experimental results are showed in Fig.2: (a) is the binary secret image "TH.bmp", with size 120×80 ; (b) is the corresponding grayscale image by combining every neighboring 8 bits to 1 byte; (c)-(e) are the three shares; (f) is the grayscale image revealed by share 1 and share 2 and (g) is the corresponding binary image which gives nothing about the secret image; (h) is the grayscale image revealed by all three shares and (i) is the corresponding binary image which is identical to (a).

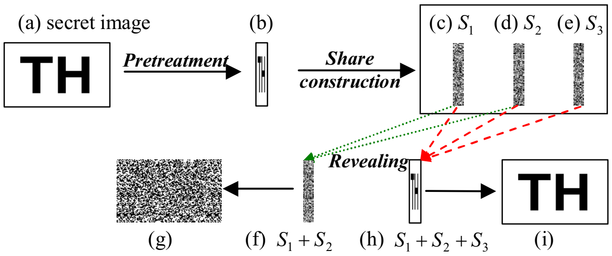

Figure 2. (3, 3) secret image sharing scheme for binary secret image.

Experiment C: Construct (4, 4) secret image sharing scheme on color secret image. Experimental results are showed in Fig.3: (a) is the color secret image "lena.jpg", with size 200×200 ; (b)-(e) are the four shares; (f) is the image revealed by share 1 and share 2, which gives nothing about the secret image; (g) is the image revealed by share 2, share 3 and share 4, which gives nothing about the secret image; (h) is the image revealed by all four shares which is identical to (a).

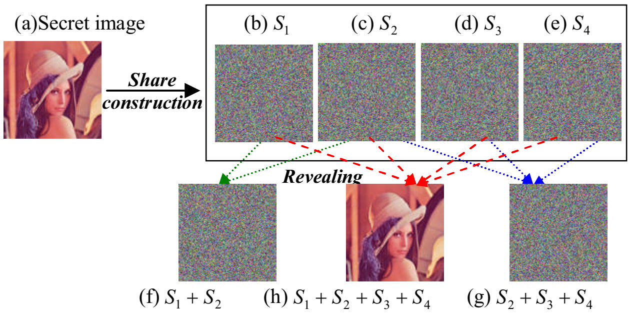

Figure 3. (4, 4) secret image sharing scheme for color secret image.

From the experimental results, we can see that secret image is precisely recovered. For grayscale and color image, each shadow and reconstructed secret image have the same size as the original image. For binary image, each shadow is 8 times smaller than that of the original image.

B. Comparison

To further demonstrate the features of our proposed new category of secret sharing scheme, we will compare our (n, n) scheme with the other three categories in terms of four criteria: security, contrast, computational complexity and pixel expansion.

1) Security: All schemes must satisfy the security condition and we have proved our new scheme satisfies the security condition.

2) Contrast: Category I can reconstruct the secret image precisely. Category II has low contrast. Category III can reconstruct the secret image better than category II and some schemes in category III can reconstruct the secret image precisely. Our proposed scheme can reconstruct the secret image precisely.

3) Computational complexity: Category I reconstruct the secret image by polynomial interpolation and the computation complexity is $O(n\log^2 n)$. Category II and category III reconstruct the secret image by Boolean operation and the computation complexity is $O(n)$. Our scheme reconstructs the secret image by addition operation and the computation complexity is $O(n)$.

4) Pixel expansion: Shares of category I have the same or smaller size than the original image. Shares of category II is much bigger than the original image, since one pixel are expanded to m subpixels. Shares of category III and our proposed scheme for grayscale image have the same size with the original image. Our proposed scheme for binary image has smaller shares.

For clarity, the detail of the above comparison is listed in Table 1.

TABLE I. COMPARISON OF DIFFERENT (N, N) SIS SCHEMES

Category	*Contrast*	*Pixel expansion*	*Reconstruct operation*	*Complexity*
I [3,4]	1	<=1	Polynomial interpolation	$O(n\log^2 n)$
II [5,6,7]	<<1	>>1	OR(stacking)	$O(n)$
III [8,9,10]	<=1	1	XOR	$O(n)$
Our proposed	1	1 (for grayscale and color) 1/8 (for binary)	Addition	$O(n)$

V. CONCLUSION

In this paper, we propose a new category of secret image sharing scheme which uses addition as the reconstruct operation. Compared with the other sharing schemes, the proposed (n, n) scheme for grayscale image can reconstruct the secret image precisely with low computational complexity. It can be easily extended to binary and color image. We are currently investigating to extend this scheme to more general (k, n) scheme.

ACKNOWLEDGMENT

The authors would like to thank the reviewers for their valuable comments. This work is supported by Post-Doctor Foundation of China under Grant 20090460316.

REFERENCES

[1] G. R. Blakley, “Safeguarding cryptographic keys,” Proc. AFIPS NCC, vol.48, 1979, pp.313-317.

[2] A.Shamir, “How to share a secret,” Commun. ACM, vol.22 (11) , 1979, pp.612-613.

[3] C. C. Thien, J. C. Lin, “Secret image sharing, ” Computers and Graphics, vol.26(5) , 2002, pp.765-770.

[4] R. Z. Wang, C. H. Su, “Secret image sharing with smaller shadow images,” Pattern Recognition, vol.27,2006, pp.551-555.

[5] M. Naor, A. Shamir, “Visual cryptography,” Advances in Cryptology-EUROCRYPTO’94, Springer-Verlag, vol.950, 1995, pp.1-12.

[6] M. Iwamoto, H. Yamamoto, “The optimal n-out of-n visual secret sharing scheme for gray-scale images,” IEICE Trans. Fundam. E85-A (10) , 2002, pp.2238–2247.

[7] S. Cimato, R. De Prisco, A. De Santis, “Optimal colored threshold visual cryptography schemes,” Designs Codes and Cryptography, vol.35(3), 2005, pp. 311–335.

[8] P. Tuyls, H.D.L. Hollmann, J.H.van Lint, L. Tolhuizen, “Xor-based visual cryptography Schemes,” Designs Codes and Cryptography, vol.37, 2005, pp.169–186.

[9] F. Yi, D.S. Wang, P. Luo, Y.q. Dai, “Two new color (n, n)-secret sharing schemes,” Journal on Communications (Chinese), vol.28(5), 2007,pp.30-35.

[10] D.S.Wang, L. Zhang, N. Ma, X.B. Li, “Two secret sharing schemes based on Boolean operations,” Pattern Recognition, vol.40, 2007, pp.2776-2785.

[11] K.Y. Chao, J.C. Lin, “Secret image sharing: a Boolean-operations-based approach combining benefits of polynomial-based and fast approaches,” International Journal of Pattern Regnition and Artificial Intelligence, vol.23(2),2009, pp. 263-285.

[12] Ryouichi Nishimura, Shun-ichiro Abe, Norihiro Fujita and Yoiti Suzuki, “Reinforcement of VoIP Security with Multipath Routing and Secret Sharing Scheme,” Journal of Information Hiding and Multimedia Signal Processing, vol. 1(3), 2010, pp. 204-219.