An Optimal (n,n) Secret Image sharing Scheme

Bhaskar Mondal, Deep Sinha, Navin Kumar Gupta, Nishant Kumar, Pankaj Goyal
Department of Computer Science and Engineering
National Institute of Technology Jamshedpur
Jharkhand 831014, India

Abstract—In this paper, we propose a novel (n,n) secret image sharing scheme. Both the construction and revealing of shares are based on matrix addition. In this paper, we have analyzed the secret image sharing scheme proposed by Dong and Ku [8] and improved it. The method [8] was applicable only for square images. The shares generated for a complete black image were themselves completely black; they were not random which made it a (1, n) secret sharing scheme. In case of images having completely single color other than the color black, the shares were having strip patterns rather than being random. Our proposed scheme is applicable for any size of image, has no pixel expansion and can reconstruct the secret image precisely. Our scheme includes no matrix multiplication for construction of shares, rather works on simple matrix addition which reduces the computational complexity. The scheme can be directly applied for any of the binary, grayscale or color image. Experimental results show that our scheme is simple and effective.

Keywords—Optimal Secret Sharing, Image sharing, Matrix Addition, Share Construction.

I. INTRODUCTION

With the rapid development of computer technique and communication network, more and more people and organizations rely on the internet to transmit important information. However in recent years hackers have intruded many computer network systems to steal or corrupt the important information, which has caused a great loss to organizations and personal profits. Hence information security has become a very important issue in modern society. Many techniques have been developed to protect the security of information including visual cryptography, secret sharing, steganography, and other encryption techniques.

Secret sharing (SS), was first proposed by Blakley [1] and Shamir [2] independently, which encode a secret image into *n* shares. The secret image 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).

In this paper, we study secret image sharing and have modified the existing schemes to provide a better and efficient technique. The previous scheme proposed by Dong and Ku [8] makes the use of matrix multiplication property for construction of shares and addition of shares to reconstruct the secret image. We have improved the share construction technique by reducing the computational complexity by applying matrix addition instead of matrix multiplication. However image reconstruction still uses the matrix addition property. Our scheme has no pixel expansion and retains the contrast of the original secret image. Considering an image of size h×h pixels, the computational complexity of matrix multiplication is $O(h^3)$, whereas that of matrix addition is $O(h^2)$. The complexity of share generation improves in our scheme as compared to Dong and Ku [8]. Hence our proposed scheme adds to the merits of already known secret sharing schemes and optimizes it.

II. SECRET SHARING

Secret Sharing refers to a method for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own.

Now, the definition of secret sharing scheme is as follows:

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

(T_1): The secret *s* is recoverable from any *k* shares, i.e., for any set of *k* indices, $H(s|(si_1,...,si_k)) = 0$.

(T_2): Knowledge of *k*-1 or fewer shares provides absolutely no information about *s*, i.e., for any set of *k*-1 indices, $H(s|(si_1,...,si_{k-1})) = H(s)$,where $H(s)$ denotes the uncertainty of *s*, $H(a|b)$ 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. PRELIMINARIES

Proc. of the Intl. Conf. on Advances in Electronics, Electrical and Computer Science Engineering — EEC 2012
Edited by Dr. R. K. Singh.

ISBN: 978-981-07-2950-9

Here we give some denotations and facts which are necessary for the explanation of our scheme. Consider a grayscale secret image A with size $h\times w$. The darkness of each pixel can be described by its grayscale level. Usually there are 256 grayscale levels which are represented by 0,...,255. Thus image A can be represented by a matrix, $A[a_{ij}]_{hxw}$, where i=1,…,h ; j=1,…,w and a_{ij} {0,…,255}. Assume that $X = [x_{ij}]_{pxr}$ and $Y = [y_{ij}]_{pxr}$, then Z = X + Y is the sum of the matrices X and Y, where $z_{ij} = x_{ij} + y_{ij}$, '+' is named matrix addition and $z_{ij} = x_{ij} - y_{ij}$, '-' is named matrix subtraction.

A unit matrix is an integer matrix consisting of all its elements as 1. The m × n unit matrix is often denoted J_{mn}, or J_n, if m=n. Suppose that A is a matrix with size $h\times w$, J is a unit matrix with size $h\times w$ and $R_{i1},\ldots,R_{ik}$ are independently random matrices, whose each element belongs to {0,…,255}. Then we have some obvious properties as follows.

Property 1: nJ = J', where n is a scalar multiple and each element of J' matrix becomes n.
Property 2: If $R = R_{i1} + \ldots + R_{ik}$, then R is a random matrix.
Property 3: If $B = R$ + A, where A is a known matrix and R is a random matrix, then B is a random matrix.
Property 4: If $T = J' - R$, then T is random matrix.

IV. PROPOSED (*N*, *N*) SECRET IMAGE SHARING SCHEME

Novel (n, n) secret image sharing scheme for grayscale images is proposed in this section.

A. Proposed scheme for grayscale image: The proposed (n, n) secret image sharing scheme for grayscale image with 'k' grayscale levels, 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 PA of size $h \times w$

Output: Share image S_i , i {1,…,n}

Share construction:

Step1: Generate (n-1) random matrices $R_1,\ldots,R_{n-1}$, each of which has size $h \times w$ and element be {0,…,k-1} for an image with k grayscale levels.

Step2: Compute R_n = (kJ - R_1 -…- R_{n-1})mod k, where J is a unit matrix with size $h \times w$.

Step3: Compute S_i = (R_i + PA)mod k, where '+' means matrix addition and i {1,…,n-1}.

Step4: Compute S_n = (R_n + kJ - $(n$-$2)PA$)mod k, where '-' means matrix subtraction.

Image Reconstruction:

Step1: PA'= (S_1 +…+ S_n)mod k.

B. Example: An example is given here to demonstrate a (3, 3) secret image sharing scheme.

Input: grayscale image, PA = $\begin{bmatrix}221 & 135 & 237\\131 & 128 & 45\\67 & 208 & 127\end{bmatrix}$

Step1: Random Matrices, R_1=$\begin{bmatrix}45 & 56 & 135\\35 & 111 & 224\\128 & 99 & 245\end{bmatrix}$, R_2=$\begin{bmatrix}14 & 77 & 101\\37 & 79 & 112\\224 & 188 & 43\end{bmatrix}$

Step2: Random Matrix, R_3 = (256J - R_1 - R_2)mod 256

$$= (256\begin{bmatrix}1 & 1 & 1\\1 & 1 & 1\\1 & 1 & 1\end{bmatrix} - \begin{bmatrix}45 & 56 & 135\\35 & 111 & 224\\128 & 99 & 245\end{bmatrix} - \begin{bmatrix}14 & 77 & 101\\37 & 79 & 112\\224 & 188 & 43\end{bmatrix})\text{mod } 256$$

$$= \begin{bmatrix}197 & 123 & 20\\184 & 66 & 176\\160 & 225 & 224\end{bmatrix}$$

Step3: Get the three shares by computing

S_1 = (R_1 + PA)mod 256

$$= (\begin{bmatrix}45 & 56 & 135\\35 & 111 & 224\\128 & 99 & 245\end{bmatrix} + \begin{bmatrix}221 & 135 & 237\\131 & 128 & 45\\67 & 208 & 127\end{bmatrix})\text{mod } 256$$

$$= \begin{bmatrix}10 & 191 & 116\\166 & 239 & 13\\195 & 51 & 116\end{bmatrix}$$

S_2 = (R_2 + PA)mod 256

$$= (\begin{bmatrix}14 & 77 & 101\\37 & 79 & 112\\224 & 188 & 43\end{bmatrix} + \begin{bmatrix}221 & 135 & 237\\131 & 128 & 45\\67 & 208 & 127\end{bmatrix})\text{mod } 256$$

$$= \begin{bmatrix}235 & 212 & 82\\168 & 207 & 157\\35 & 140 & 170\end{bmatrix}$$

S_3 = (R_3 + $256\,J$ - PA)mod 256

$$= (\begin{bmatrix}197 & 123 & 20\\184 & 66 & 176\\160 & 225 & 224\end{bmatrix} + 256\begin{bmatrix}1 & 1 & 1\\1 & 1 & 1\\1 & 1 & 1\end{bmatrix} - \begin{bmatrix}221 & 135 & 237\\131 & 128 & 45\\67 & 208 & 127\end{bmatrix})\text{mod } 256$$

$$= \begin{bmatrix}232 & 244 & 39\\53 & 194 & 131\\93 & 17 & 97\end{bmatrix}$$

Revealing: The reconstructed secret image is

Step1: PA' = (S_1 + S_2 + S_3)mod 256

$$= (\begin{bmatrix}10 & 191 & 116\\166 & 239 & 13\\195 & 51 & 116\end{bmatrix} + \begin{bmatrix}235 & 212 & 82\\168 & 207 & 157\\35 & 140 & 170\end{bmatrix} + \begin{bmatrix}232 & 244 & 39\\53 & 194 & 131\\93 & 17 & 97\end{bmatrix})\text{mod } 256$$

$$= \begin{bmatrix}221 & 135 & 237\\131 & 128 & 45\\67 & 208 & 127\end{bmatrix} = \text{PA}$$

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.

C. Theorem

Theorem I: The proposed scheme is a (*n*, *n*) secret image sharing scheme, which generates random shares and has no pixel expansion.

Proof: Let PA be the image matrix for a grayscale image. Let 'k' be the number of gray levels of an image and J be the unit matrix of the same size as of the input image.

Let $R_1,R_2,\ldots,R_{n-1}$ are the random matrices generated by the machine and are of the same size as that of the secret image matrix. We consider a unit matrix J of the same size as that of the secret image.

Also $R_n = kJ - (R_1+R_2+\ldots+R_{n-1})$. From the Property II, IV and V, we can say that R_n is also a random matrix.

From the matrix Property III, we can say that addition of image matrix PA with the random matrices $R_1,R_2,\ldots,R_{n-1}$ will itself generate random matrices $S_1,S_2,\ldots,S_{n-1}$ which are the shares of the image.

For share S_n, from Property II, III, IV, V, we can say that $S_n = R_n + kJ - (n-2)PA$ is also a random matrix.

Hence, all the shares generated by the proposed scheme are proven to be random and do not reveal anything about the secret image.

All the shares generated by the proposed scheme are having the same size as that of the secret image matrix.

Total n shares, i.e., $S_1,S_2,S_3,\ldots,S_n$ are collected to reconstruct the secret image. Share S_1 is taken as

$S_1 = (R_1 + PA)$, $S_2 = (R_2 + PA),\ldots,S_{n-1} = (R_{n-1} + PA)$, where $R_1,R_2\ldots..,R_{n-1}$ are random matrices and,

$S_n = (R_n + kJ - (n-2)PA) \bmod k$, where R_n is also a random matrix generated by the formula,

$R_n = (kJ - (R_1 + R_2 + \ldots + R_{n-1})) \bmod k$.

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

$PA' = (S_1 + S_2 + S_3 + \ldots. + S_n) \bmod k$

$= ((R_1 + PA) + (R_2 + PA) + (R_{n-1} + PA) + (kJ - (R_1 + R_2 + \ldots + R_{n-1}) + kJ - (n-2)PA))\bmod k$

$= (2kJ+PA)\bmod k = PA$

This proves that the secret image PA is completely recoverable from n shares and has no pixel expansion i.e., $H(PA|(S_1,S_2...S_n)) = 0$ which satisfies the condition T1.

Theorem II: The proposed scheme is not a (k,n) secret sharing scheme i.e. with the help of any k shares (k<n) it would not be able to reconstruct the secret image.

Proof: Let PA be the image matrix for a grayscale image. For simplicity, let us consider the number of grayscale levels as 256 for a grayscale image.

Let $R_1,R_2,\ldots,R_{n-1}$ are the random matrices generated by the machine and are of the same size as that of the secret image matrix. We consider a unit matrix J of the same size as that of the secret image.

We take k (k<n) shares of the secret image i.e. $S_{i1},S_{i2}, S_{i3},\ldots,S_{ik}$.

We now consider two cases for the share construction phase,

Case I: n does not belong to $\{i_1,\ldots,i_k\}$. We know that, for Computing PA' according to the revealing phase for a secret image with 256 gray levels,

$PA' = [S_{i1}+S_{i2}+ S_{i3}+\ldots+S_{ik}] \bmod 256$

$= [(R_{i1}+PA) + (R_{i2}+PA) +\ldots+ (R_{ik}+PA)] \bmod 256$

$= [(R_{i1} + R_{i2} +\ldots+ R_{ik}) + k(PA)] \bmod 256$

Denote $R= R_{i1}+R_{i2}+\ldots+R_{ik}$.

Since $R_{i1},R_{i2},\ldots,R_{ik}$ are independent random matrices, according to Property II, R is also a random matrix. By Property III, PA' is also a random matrix. Hence, we can say that regenerated image is completely random.

Case II: n belongs to $\{i_1,\ldots,i_k\}$. Without loss of generality, we consider i_k=n. According to *Step 2* of the share construction phase, we consider $R_n=(256J-(R_1 + R_2 +\ldots+ R_{n-1}))$, where J is a unit matrix.

Computing PA' according to the revealing phase for a secret image with 256 gray levels,

$PA'= [S_{i1} + S_{i2} + S_{i3} +\ldots + S_{ik}] \bmod 256$

$= [S_{i1} + S_{i2} + S_{i3} +\ldots+ S_{ik-1} + S_n] \bmod 256$

$= [(R_{i1}+PA) + (R_{i2}+PA) +\ldots+ (R_{ik-1}+PA) + (256J - (R_1 + R_2 + \ldots + R_{n-1}) + 256J - (n-2)PA)] \bmod 256$

$-$

$-$

$-$

As because k<n, the above equation will generate a random matrix using Properties I-V and will not reveal the original secret image. If k=n, the above equation becomes $PA'=(512J + PA)\bmod 256 = PA$. Hence the original image can only be regenerated by taking all the n shares.

From *Case 1* and *Case 2*, we know that the knowledge of *k* (*k<n*) shares provides absolutely no information about the secret image *PA* i.e., $H(PA|(S_{i1},S_{i2}\ldots S_{ik})) = H(PA)$ which satisfies the condition T2.

To sum up, our proposed scheme satisfies the conditions (T1) and (T2) 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.

D. 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, the grayscale level (k) should be taken as 2. The rest of the procedure is same for construction of shares and revealing phase to recover the 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 generate shares. In the revealing phase, again take the decomposed RGB components of the shares and perform the proposed scheme separately. Finally merge the generated RGB components to recover the secret image.

V. EXPERIMENTAL RESULTS

Experimental results of the proposed SIS schemes are illustrated in this section.

Experiment A:

Construct a (3, 3) secret image sharing scheme on binary secret image. Experimental results are showed in Figure.1: (a) is the binary secret image “lena.bmp”, with size 512×450; (b)-(d) are the three shares generated using the proposed method; (e) is the image revealed by the combination of any two shares like share 1 and share 2 and is a completely random image which gives nothing about the secret image; (f) is the image revealed by the combination of all three shares and (f) is identical to (a).

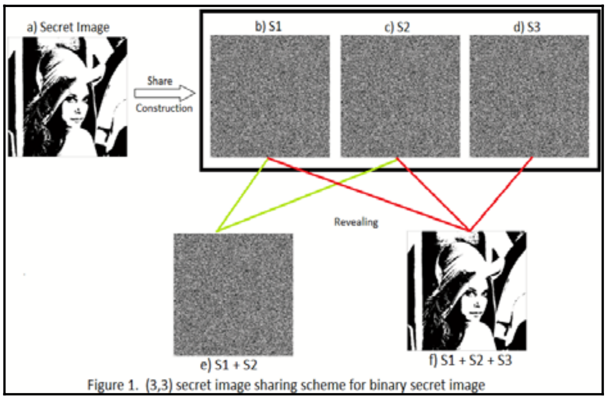

Figure 1. (3,3) secret image sharing scheme for binary secret image

Experiment B:

Construct a (4, 4) secret image sharing scheme on grayscale secret image. Experimental results are showed in Figure.2: (a) is the grayscale secret image “lena_gray.jpg”, with size 512×450 ; (b)-(e) are the four shares generated using the proposed method; (f) is the image revealed by the combination of any two shares like share 1 and share 2 and is a completely random image which gives nothing about the secret image; (g) is the image revealed by the combination of any three shares like share 2, share 3 and share 4 and is a completely random image which again gives nothing about the secret image; (h) is the image revealed by the combination of all four shares and (h) is identical to (a).

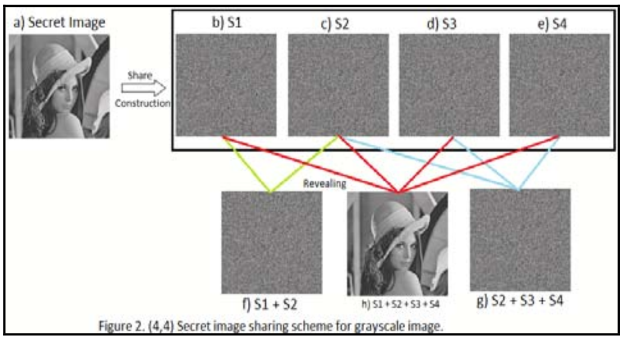

Figure 2. (4,4) Secret image sharing scheme for grayscale image.

Experiment C:

Construct a (3, 3) secret image sharing scheme on secret color image. Experimental results are showed in Fig.3: (a) is the secret color image “lena_color.jpg”, with size 512×450; (b)-(d) are the three shares generated using the proposed method; (e) is the image revealed by the combination of any two shares like share 1 and share 2 and is a completely random image which gives nothing about the secret image; (f) is the image revealed by the combination of all three shares and (f) is identical to (a).

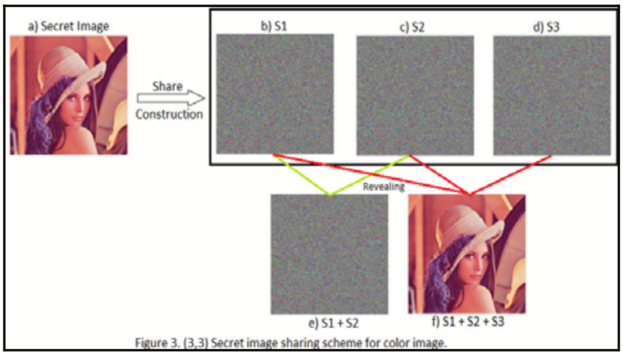

Figure 3. (3,3) Secret image sharing scheme for color image.

From the experimental results, we can see that secret image is precisely recovered. For binary, grayscale and color image, each shadow and reconstructed secret image have the same size as the original image. Also there is no restriction of having a square sized image.

VI. 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 four categories in terms of four criteria:

security, pixel expansion, contrast, share generation operation & its computational complexity, reconstruction operation & its computational complexity,

*1) **Security**:* All schemes must satisfy the security condition and we have proved our new scheme satisfies the security condition in the theorem and experimental results. Since an image usually consists of many pixels, the possibility of finding the secret would be $(k)^{h\times w}$, where $h\times w$ is the number of pixels in the shares of the image or the image share size and k is the number of gray levels of the image. For example, for a grayscale image's share with resolution 512×450, one would need $256^{512\times 450}$ brute force attempts to find the secret, which is computationally infeasible.

*2) **Contrast**: S*ome schemes in category I can reconstruct the secret image precisely whereas others lack the precision. Category II reconstructs the secret image precisely. Our proposed scheme can also reconstruct the secret image precisely.

*3) **Pixel expansion**:* Shares of category I and II for grayscale image have the same size with the original image. Our proposed scheme generates the shares of the same size.

4) ***Share generation complexity***: Considering an image of size h×w pixels, Category I uses the Boolean operations (XOR) to generate the shares with the complexity of O(h×w). The computational complexity of category II is O(h^3) and it works only for square images. Whereas, that of our proposed scheme is O(h×w). Hence the complexity of share generation improves drastically in our scheme.

*5) **Share Reconstruction complexity**:* Category I reconstructs the secret image by Boolean operation and the computation complexity is *O*(*n*). Category II reconstructs the secret image by addition operation and the computation complexity is *O*(*n*). Our scheme reconstructs the secret image by addition operation and the computation complexity is *O*(*n*).

TABLE I: COMPARISON BETWEEN VARIOUS SCHEMES

Scheme Category	**Contrast**	**Pixel Expansion**	**Share Generation Operation**	**Complexity for each share generation**	**Reconstruction Operation and Complexity**
I [6, 7]	<=1	1	XOR	O(h×w)	XOR O(n)
II [8]	1	1(for grayscale and color) 1/8 (for binary)	Matrix Multiplication	O(h^3)	Matrix Addition O(n)
Our proposed	1	1	Addition	O(h×w)	Matrix Addition O(n)

Note:

n is the total number of shares to be generated.

h, w are the height and width of the image in terms of pixels respectively.

VII. CONCLUSION

In this paper, we proposed a new (n,n) secret image sharing scheme which uses addition for the construction and reconstruction operation. Compared with the other sharing schemes, the proposed (*n*, *n*) scheme for grayscale image can construct random shares and reconstruct the secret image precisely with low computational complexity. Common software tools, such as Matlab can be used to implement the matrix operations and reconstruct the secret images. It can be easily extended to binary and color image. Moreover, the proposed schemes provide perfect security. The obvious advantages of our schemes in terms of low computation complexity, no pixel expansion and high reconstruction contrast/accuracy are encouraging. Secret sharing schemes have a vast scope of improvement. Researchers are looking for new fields of applications. We are currently investigating the approaches of extending this scheme to a more general *(k, n)* scheme and other schemes like multi-image sharing and video streaming.

VIII. ACKNOWLEDGMENT

The authors would like to thank the reviewers for their valuable comments. This work is supported by Department of Computer Science and Engineering, N.I.T. Jamshedpur, India.

IX. 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] M. Naor, A. Shamir, "Visual cryptography," Advances in Cryptology-EUROCRYPTO'94, Springer-Verlag, vol.950, 1995, pp.1-12.

[5] 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.

[6] 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.

[7] 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.

[8] Lin Dong, Min Ku, "Novel (n,n) secret image sharing scheme based on addition," Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (2010), iih-msp, pp.583-586.