International Journal of Grid and Distributed Computing
Vol. 9, No. 2 (2016), pp.51-60
http://dx.doi.org/10.14257/ijgdc.2016.9.2.06

Lossless Recovery of Multiple Decryption Capability and Progressive Visual Secret Sharing

Xin Qi

Modern Educational Technology Center, Harbin University of Science and Technology, Harbin, China
qixin8000@163.com

Abstract

In order to solve the problem of non-restoration of PVSS, in this paper, we propose a method to recover the secret image without using the Boolean operation of the matrix matrix. In the lossless recovery process, each column base matrix will be "and" and "exclusive or" operation to get the original image anti-color image, and then the image can be obtained by the lossless secret image, this method can be applied to the general (k, n) threshold lossless recovery. In the absence of a computing device, it can be decrypted by superimposing, in the XOR computing device, it can realize lossless recovery. Experimental results show that the proposed algorithm can guarantee the gradual visual secret sharing, complete the restoration of the secret image, the operation is simple and efficient, and has a strong practicability.

Keywords*: PVSS; multi decryption capability; Boolean operation; lossless recovery*

1. Introduction

In 1979, Blakley [1] and Shamir[2] independently proposed a secret sharing scheme (sharing secret, SS). In the (k, n) threshold scheme, the secret information is divided into n parts (called deposit), which are held by the n participants. Any k or more participants can use the stored information to reconstruct the secret information, and less than k participants cannot get any secret information. In EUROCRYPT 1994, Naor and Shamir[3] proposed visual secret sharing (VSS) to recover the secret information by using the human visual effect, no complex password calculation. In this method, a pixel in the original dense graph is stored as a sub pixel in the sub image, and thus the loss of the pixel expansion and contrast is present.

Hou and Quan[4] proposed ($2, n$) PVSS algorithm, through the design of the two base matrix to achieve the visual secret sharing of non-pixel expansion, each shadow image randomly appeared black and white, in which the probability of black pixel point is $1/n$. With the increase of the number of shadow image superimposed, the secret image will become more and more clear. But, sharing image is still a noise image, easy for an attacker to doubt and destroy, and not able to lossless restored the original secret image.

It is very important to share technology with multi decryption in the visual secret sharing, because it cannot recover the original secret information by stacking the secret information.And,it is still a hot spot for the research of the visual contrast problem.With the development of technology, the more and more widely application of network communication and the easily obtaining of the light weight computing equipment. The quality of the image calculated by using a simple method is much higher than the effect of the visual stacking method to recover the secret information. But the secret sharing visibility, without calculating, only by the human eye recognizing the characteristics of secret information, is still irreplaceable. Therefore, studying how to ensure that the visual

ISSN: 2005-4262 IJGDC

code share, while non-destructive recovery could be carried out with a simple calculation, is an important research direction.

In the non-destructive recovery, researchers [5-7] proposed a single non-destructive recovery method by computing device, no guaranteeing visual secret sharing scheme decrypted keep stacking features. Some academics have suggested[8] multi-decryption capabilities progressive visual secret sharing scheme based on RG-VCS random grid, to achieve a non-destructive recovery. Literature[9] proposed lossless recovery only supports $(2,n),(n,n)$ threshold issue.

In this paper, we analyze the characteristics of PVSS algorithm based on literature[4]. While retaining visual secret sharing characteristics of the premise, we propose a simple Boolean operation to recover the secret information. The secret information can be recovered by using the lightweight computing device. On the basis of this, we extend the lossless recovery scheme to the general (k,n) threshold. The color's digital image expression, in the non-destructive recovery, according to the different of the array number n(odd and even) using different Boolean ("and" and "exclusive or" binding) calculation method to obtain secret anti-color image image, then turn it over to get the secret image lossless recovery. Through this algorithm, the experimental results show that the algorithm can solve the problem of PVSS's recovery, and ensuring the algorithm's visibility at the same time.

2. Related Work

PVSS scheme is designed to design two basis matrices C^0 and C^1. It is shown in table 1, 0 represents white, 1 represents black.

Table 1. Designed $n\times n$ Basis Matrix

Confidential information	Basis matrix	Memory matrix	Probability	Shadow image 1 2 … n	Recovery method
□(0)	$C^0=\begin{pmatrix}1&1&\cdots&1\\0&0&\cdots&0\\\vdots&\vdots&\vdots&\vdots\\0&0&\cdots&0\end{pmatrix}_{n\times n}$	$\begin{matrix}1&1&\cdots&1\\0&0&\cdots&0\\\vdots&\vdots&\vdots&\vdots\\0&0&\cdots&0\end{matrix}$	$1/n$ $1/n$ $1/n$ $1/n$	■ ■ … ■ □ □ … □ ⋮ ⋮ ⋮ ⋮ □ □ … □	OR
■(1)	$C^1=\begin{pmatrix}1&0&\cdots&0\\0&1&\cdots&0\\\vdots&\vdots&\vdots&\vdots\\0&0&\cdots&1\end{pmatrix}_{n\times n}$	$\begin{matrix}1&0&\cdots&0\\0&1&\cdots&0\\\vdots&\vdots&\vdots&\vdots\\0&0&\cdots&1\end{matrix}$	$1/n$ $1/n$ $1/n$ $1/n$	■ □ … □ □ ■ … □ ⋮ ⋮ ⋮ ⋮ □ □ … □	

The generating process of the shadow image is shown in following 1.

Input: One $M\times N$ two valued secret image S, threshold parameter n

Output: n shadow images $SC_1,SC_2,\cdots SC_n$

Step1: Generate two basic matrices as shown in table 1 C^0 and C^1

Step2: For each pixel coordinates $(i,j)\in\{(i,j)\,|\,1\le i\le M,1\le j\le N\}$, repeat steps 3-4

Step3: Random selection $L\in\{1,2,\cdots,n\}$

Step4: If $S(i,j)=0, SC_m(i,j)=C^0(L,m)$, or $SC_m(i,j)=C^1(L,m),\ m=1,2,\cdots n$

The probability that each column appears black (1) is $1/n$ in C^0 and C^1. So each shadow image cannot get any secret information, the safety and the contrast has been proved, this article will not repeat them.

3. Digital Image

The traditional VCS scheme uses 0 to represent white, 1 represent black, the digital image in the computer is 1 white, 0 black, the two can be equivalent to the logical operation.

Table 2. The Corresponding Relation between the Traditional VCS and the Boolean Operation of Digital Image

	White	Black	Recovery operation	Result
Traditional VCS	0	1	OR	1（black）
Digital image	1	0	AND	0（black）

Symbol definition: this paper OR operation uses $\otimes$ to represent, AND operation uses & to represent, XOR uses $\oplus$ to represent.

It can be shown that the conventional stacking mode uses $\otimes$ to represent, stacking of digital images is &. Digital image algorithm converts traditional VCS algorithm through simple $A\&B=\overline{A\otimes B}$.

In this paper, we use the method of digital image to express and analyze the problem, image as the two value image. So the matrix should be transformed into:

Table 3. Basis Matrix Corresponding to the Digital Image

□(1)	■(0)
$C^0=\begin{pmatrix}0&0&\cdots&0\\1&1&\cdots&1\\\vdots&\vdots&\vdots&\vdots\\1&1&\cdots&1\end{pmatrix}_{n\times n}$	$C^1=\begin{pmatrix}0&1&\cdots&1\\1&0&\cdots&1\\\vdots&\vdots&\vdots&\vdots\\1&1&\cdots&0\end{pmatrix}_{n\times n}$

4. Lossless Recovery

In order to solve the problem of non-destructive recovery based on PVSS algorithm, the following conclusions are drawn from the analysis of the basis matrix.

4.1. Theorem 1

For the problem of $(2,n)$

White: $C^0=\begin{pmatrix}0&0&\cdots&0\\1&1&\cdots&1\\\vdots&\vdots&\vdots&\vdots\\1&1&\cdots&1\end{pmatrix}_{n\times n}$, Black: $C^1=\begin{pmatrix}0&1&\cdots&1\\1&0&\cdots&1\\\vdots&\vdots&\vdots&\vdots\\1&1&\cdots&0\end{pmatrix}_{n\times n}$

1）When n($n\geq 2$) is an even number

$$C^0(:,1)\oplus C^0(:,2)\oplus\cdots\oplus C^0(:,n)=\begin{pmatrix} C^0(1,1)\oplus C^0(1,2)\oplus\cdots\oplus C^0(1,n)\\ C^0(2,1)\oplus C^0(2,2)\oplus\cdots\oplus C^0(2,n)\\ \vdots\\ C^0(n,1)\oplus C^0(n,2)\oplus\cdots\oplus C^0(n,n)\end{pmatrix}=\begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix} \quad (1)$$

$$C^1(:,1)\oplus C^1(:,2)\oplus\cdots\oplus C^1(:,n)=\begin{pmatrix}1\\1\\\vdots\\1\end{pmatrix} \quad (2)$$

Corresponding element $\oplus$ in C^0 or C^1, you can get the matrix represent the color of color, C^0 get black after the operation, C^1 get white after the operation.

2) When n($n\geq 3$) is odd

$$(C^0(:,1)\,\&\,C^0(:,2)\,\&\cdots\&\,C^0(:,n-1))\oplus C^0(:,n)=\begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix} \quad (3)$$

$$(C^1(:,1)\,\&\,C^1(:,2)\,\&\cdots\&\,C^1(:,n-1))\oplus C^1(:,n)=\begin{pmatrix}1\\1\\\vdots\\1\end{pmatrix} \quad (4)$$

Arbitrarily $n-1$ column corresponding element after & operation in C^0 or C^1, afer $\oplus$ operation with the last remaining column, we could get the matrix represents the color.

Prove:

When n($n\geq 2$) is an even number:

1) Every element is the same in C^0, so any two columns $C^0(i,k)\oplus C^0(i,t)=0$, $i,k,t\in\{1,2,\cdots,n\}, k\neq t$ After the first round of all the columns are finished, the number of rows is still equal, and each element is equal, circulation above process, the operation result of C^0 is $RC^0=\begin{pmatrix}0 & 0 & \cdots & 0\end{pmatrix}'$, it said the line after the operation to complete the all black 0 elements, formula (1) was a card.
2) As each row element has a different value of 0, and the rest is 1 in C^1 $C^1(i,:)=\begin{pmatrix}0 & 1 & 1 & \cdots & 1\end{pmatrix}$, $i\in\{1,2,\cdots,n\}$. $C^1(i,:)$ has $n-2$ 1, the results of these operations are the same as the formula (1), so the rest of the results $RC^1_{n-2}(i,:)=\begin{pmatrix}0 & 1 & 0\end{pmatrix}$, the result of each element $RC^1_{n-2}(i,:)$ after $\oplus$ operation is $RC^1(i,:)=1$, after all line $\oplus$ operations, the result is $RC^1=\begin{pmatrix}1 & 1 & \cdots & 1\end{pmatrix}'$, that is all lines are calculated and the results are white 1, formula (2) was a card. When n($n\geq 3$) is odd

3) Take C^0 any column $n-1$ for & operation, because of all the elements in each row are the same, after & operation, the result is the same as any one, $RC^0_{n-1} = C^0(:,i)\,.\,RC^0 = RC^0_{n-1} \oplus C^0(:,n) = C^0(:,i) \oplus C^0(:,n) = (0 \quad 0 \quad \cdots \quad 0)^{'}$, all elements of C^0 are black 0 after operation, formula (3) was a card.

4) Take C^1 any column $n-1$ for & operation, we can be learned from the law C^1, there must be an element of 1 in $n-1$, other lines must have and only one element is 0. After all 1 of the rows are removed, $C^1_{n-1}(i,j)$, $i, j \in \{1,2,\cdots,n-1\}$, matrix is C^1, the results of the operations of $C^1_{n-1}(i,j)$ columns are $RC^1_{n-1} = (0 \quad 0 \quad \cdots \quad 0)^{'}_{n-1}$, plus the last full line of 1, the result is $RC^1_{n-1} = (0 \quad 0 \quad \cdots \quad 0 \quad 1)^{'}_{n}$, last column $C^1(:,n) = (1 \quad 1 \quad \cdots \quad 1 \quad 0)^{'}_{n}$, $RC^1 = RC^1_{n-1} \oplus C^1(:,n) = (1 \quad 1 \quad \cdots \quad 1)^{'}$, all elements are white 1 after operation, formula (4) was a card.

4.2. $(2,n)$ Threshold Lossless Recovery

Aiming at $(2,n)$ threshold problem, known secret image S, generate n shadow image. According to theorem 1, with the use of lightweight computing devices with Boolean operations, it can be used for the restoration of the secret image. Recovery steps are as follows:

Input: n algorithm generated shadow image $SC_i, i \in \{1,2,\cdots,n\}$

Output: A lossless secret image S

Step1: If the number of shadow images n is even, execute step 4

Step2: If the number of shadow images n is odd, execute step 3

Step3: Arbitrary take $n-1$ shadow image of the & operation, the result of an operation $SC^{'}$ $SC^{'} = SC_1 \& SC_2 \& \cdots \& SC_{n-1}, i \in (1,2,\cdots,n-1)$

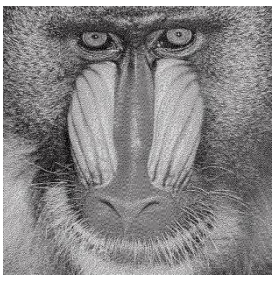
Step4: All shadow images $\oplus$:

$SC = SC_1 \oplus SC_2 \oplus \cdots \oplus SC_n$, if there is $SC^{'}$, then $SC = SC^{'} \oplus SC_n$

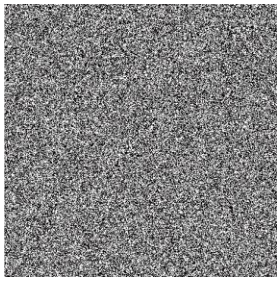
Step5: Take SC back the results of the operation, get the lossless secret image S

4.3. Simulation Results

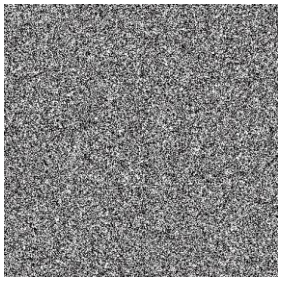
The experimental results of the lossless recovery are shown in Figure 1, Figure 2.



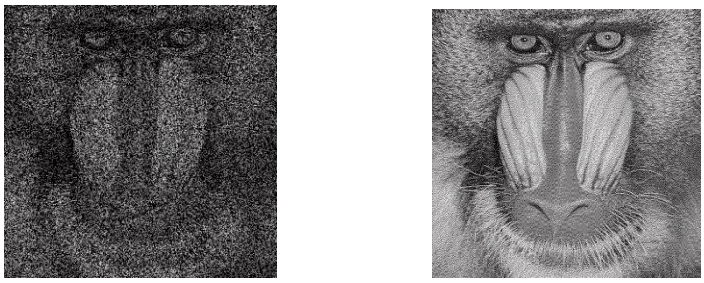
(a) Secret image S



(b) Shadow image SC_1

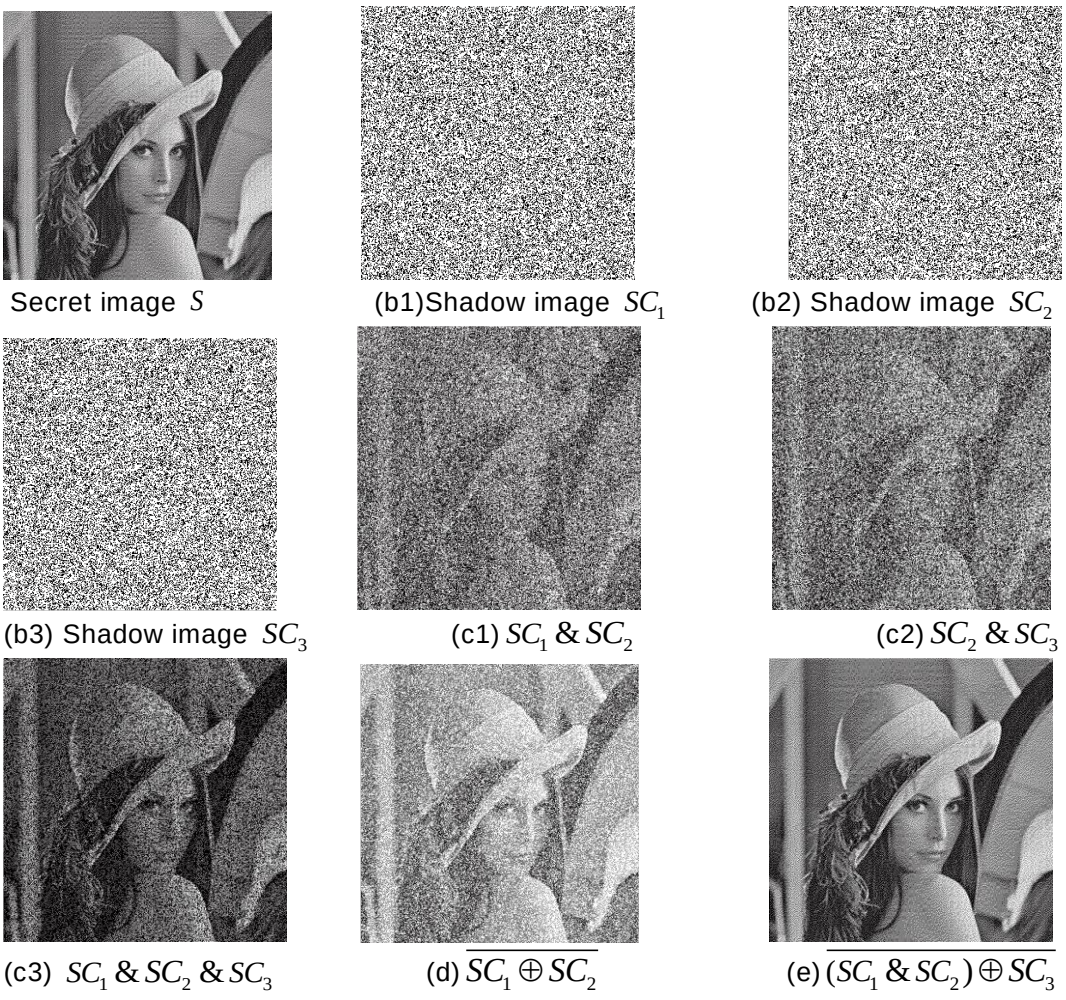


(c) Shadow image SC_2



(d) $SC_1 \& SC_2$ (e) $\overline{SC_1 \oplus SC_2}$

Figure 1. (2, 2) PVSS Lossless Recovery



(a) Secret image S (b1)Shadow image SC_1 (b2) Shadow image SC_2

(b3) Shadow image SC_3 (c1) $SC_1 \& SC_2$ (c2) $SC_2 \& SC_3$

(c3) $SC_1 \& SC_2 \& SC_3$ (d) $\overline{SC_1 \oplus SC_2}$ (e) $\overline{(SC_1 \& SC_2) \oplus SC_3}$

Figure 2. (2, 3) PVSS Lossless Recovery

From Figure 1, we can see that the n is an even number of shadow images, according to theorem 1, take (b) (c) a simple operation $\oplus$ and negated color, lossless restoration of the original secret image S, it is shown in (e), (e) and (a) in full agreement, to achieve lossless recovery, the algorithm is simple and efficient.

From Figure 2, we can see that when $n = 3$ is odd, according to theorem 1, adopt the first 2 shadow image (b1) and (b2) to carry out & operation, the results and the third shadow image (b3) to calculate $\oplus$ operation and negated color, lossless

restoration secret image S, it is shown in (e), (e) and (a) in full agreement, to achieve lossless recovery.

If the number of shadow images n is unknown, it is not good to use theorem 1, because the theorem needs to know n is odd or even, so in this case the use of lightweight computing devices will all be operational shadow image obtained and negated color, we still can get a good contrast to the secret image, it can be identified very high.

Contrast calculation formula is shown as follows:

$$\alpha = \frac{P_0 - P_1}{1 + P_1} = \frac{P(S'[AS0] = 0) - P(S'[AS1] = 0)}{1 + P(S'[AS1] = 0)} \tag{5}$$

Table 4 n is Unknown Directly after the XOR Shadow Image Contrast

	t=2	t=3	t=4	t=5
(5,5)	0.3995	0.3336	0.7995	0.6674
(4,4)	0.4974	0.4006	1	
(3,3)	0.6679	0.4988		
(2,2)	1			

Table 5 n is Unknown after Stack Shadow Image Contrast

	t=2	t=3	t=4	t=5
(5,5)	0.1667	0.3336	0.5002	0.6674
(4,4)	0.1986	0.4006	0.6009	
(3,3)	0.2500	0.4988		
(2,2)	0.3342			

The quantitative data from table 4 can be seen, even though the arithmetic can get good contrast even when there is no complete shadow image, as can be seen from table 4, the contrast is significantly higher than that in table 5 by a simple stack to get the contrast, when t is odd, at least to the simple stack of contrast.

5. (k,n) Lossless Recovery of Threshold

5.1. General Threshold Expansion Method

$$\begin{aligned} S &= (SC_1, SC_2) \\ &= (SC_1, (SC_{21}, SC_{22})) \\ &= (SC_1, (SC_{21}, (SC_{221}, SC_{222}))) \\ &= (SC_1, (SC_{21}, (SC_{221}, (SC_{2221}, (\cdots))))) \end{aligned} \tag{6}$$

The first $k-2$ image is used (2,2) threshold, repeatedly to generate the memory of the sub image (2,2) sub deposit. The memory image is calculated by using the repeated use (2,2), make up $k-2$ save image, finally, the remaining 2 threshold images are obtained by $(2, n-k+2)$ threshold.

Non destructive recovery steps are as follows:

Input: Using the algorithm to generate the memory map $SC_i, i \in (1,2,\cdots,n)$

Output: Lossless secret image S

Step1: If $n-k+2$ is even numbers, execute step 4

Step2: If $n-k+2$ is odd numbers, unify the group $n-k+2$

Step3: Obtain SC_a

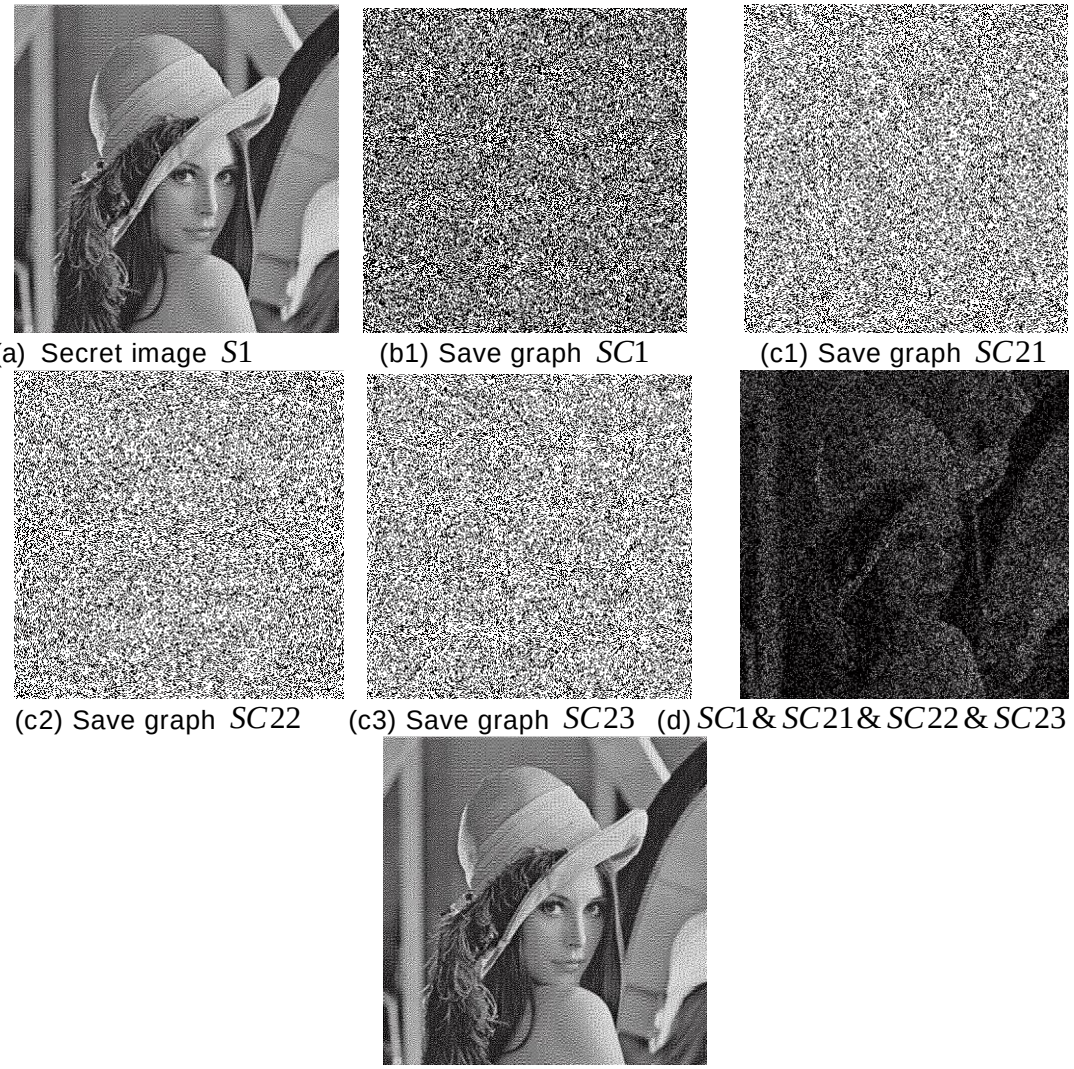
Step4: Obtain lossless secret image S

5.2. (k,n) Simulation Results

Simulating the non-destructive recovery of progressive secret sharing.

As shown in Figure 3, aiming at (3,4) threshold, first according to the algorithm split into two shadow images $SC1$, $SC2$, and then use the (k,n) threshold expansion method, take $SC2$ divide into shadow images (c1)(c2)(c3). Using theorem 1 to (c1)(c2)(c3), then using theorem 1 to $SC1$, $SC2$, we can get lossless restoration secret image $S1$.

As shown in Figure 4, aiming at (3,5) threshold, first according to the algorithm split into two shadow images $SC1$, $SC2$, and then use the (k,n) threshold expansion method, take $SC2$ divide into shadow images (c1)(c2)(c3) (c4).

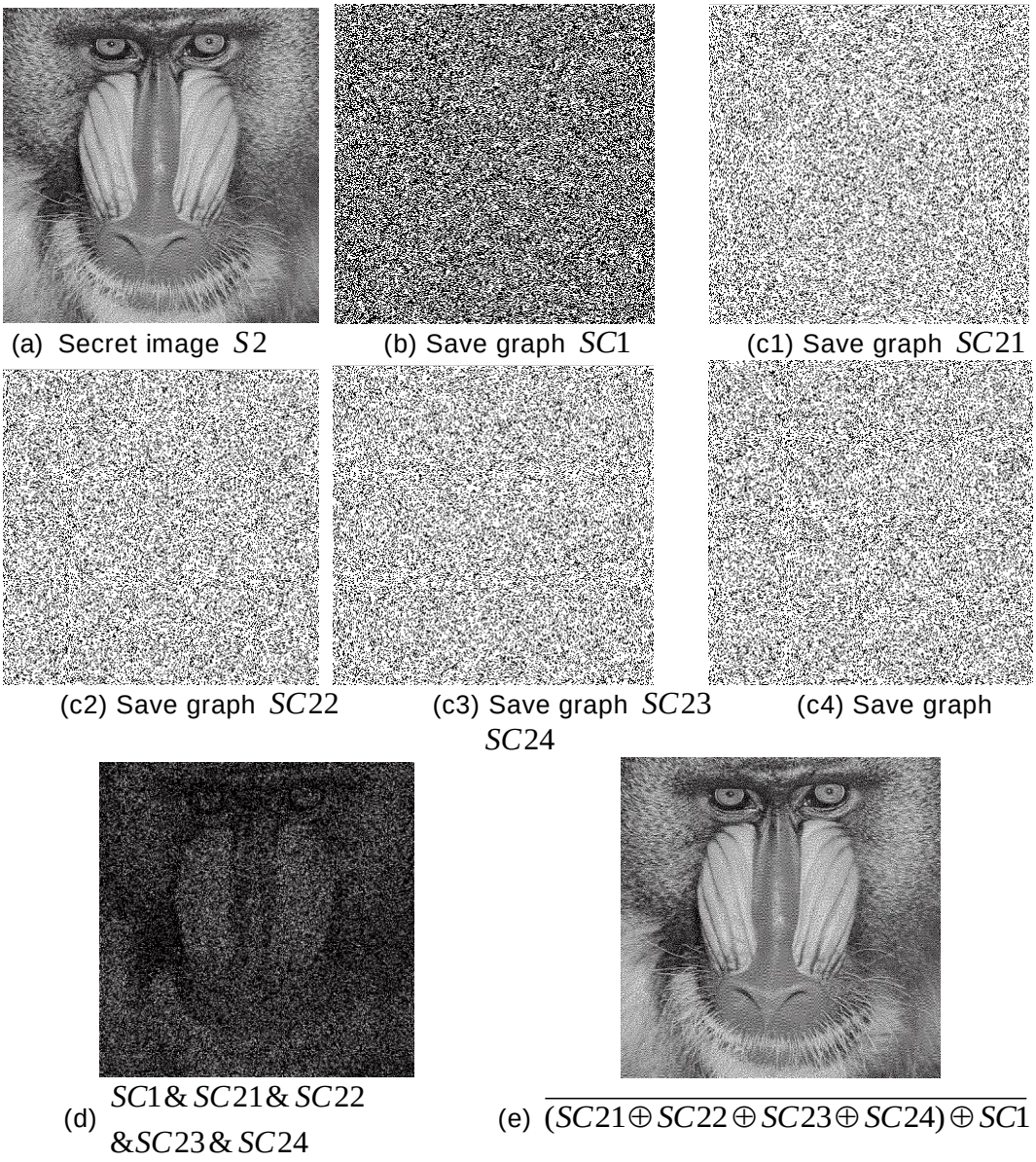


(a) Secret image $S1$ (b1) Save graph $SC1$ (c1) Save graph $SC21$

(c2) Save graph $SC22$ (c3) Save graph $SC23$ (d) $SC1 \& SC21 \& SC22 \& SC23$

(e) $\overline{((SC21 \& SC22) \oplus SC23) \oplus SC1}$

Figure 3. (3,4) Threshold Progressive Visual Secret Sharing



(a) Secret image $S2$ (b) Save graph $SC1$ (c1) Save graph $SC21$

(c2) Save graph $SC22$ (c3) Save graph $SC23$ (c4) Save graph $SC24$

(d) $SC1 \& SC21 \& SC22 \& SC23 \& SC24$ (e) $\overline{(SC21 \oplus SC22 \oplus SC23 \oplus SC24) \oplus SC1}$

Figure 4. (3, 5) Threshold Progressive Visual Secret Sharing

6. Conclusion

Based on the PVSS, the use of lightweight equipment, the shadow image achieves the secret information lossless recovery through a simple and computing, with a simple operation, visual features.

Based on the algorithm of literature [4], adopting the expression of digital image, the conclusion is as follows:

1) The lossless recovery method of the $(2, n)$ problem:

1. When n is even, the secret information can be recovered though XOR of all shadow image and negating color.

2. When n is odd, through the n-1 shadow image and operation and the result with the last shadow image XOR and negating color, the secret information can be lossless recover.

2) For the problems of (k, n), combined with the algorithm of literature [7]:

1. If it is an even number, directly $\oplus$ to all of the direct memory, the lossless secret image could be obtained.

2. If it is an odd number, we use the theorem 1 to pre process the lase generating stored separately graphics. The obtained results compared with the rest of the remaining points, the lossless secret image could be obtained.

In summary, at the premise of retaining the characteristics of original progressive visibility secret sharing, this paper achieve the decryption recovery shared secret in more destructive capabilities, algorithm supporting non-destructive recovery of general (k, n) threshold.

References

[1] G R. Blakley, "Safeguarding cryptographic keys", //Proceedings of the National Computer Conference. New York, USA:IEEE,**(1979)**, pp. 313-317.
[2] A. Shamir, "How to share a secret [J]", Communications of the ACM, vol. 22, no. 11, **(1979)**, pp. 612-613.
[3] M. Naor, A. Shamir, "Visual cryptography[C]", //Advances in Cryptology-EUROCRYPT'94 Lecture Notes in Computer Science, Workshop on the Theory and Application of Cryptographic Techniques, May 9-12.Perugia,Italy:Springer,**(1995)**, pp. 1-12.
[4] Y C Hou, Z Y Quan, "Progressive visual cryptography with unexpanded share", IEEE Trans. on Circ. and Sys. for Video Tech , vol. 21, no. 11, **(2011)**, pp. 1760-1764.
[5] T. Bhattacharjee, J. Prakash Singh , A. Nag, "A Lossless Secret Image Sharing Scheme based on Pixel Partitioning", International Journal of Electronics Communication and Computer Technology,vol. 2, Issue 1, **(2012)**, pp. 51-56.
[6] P-Y Lin,C-S Chan, "Invertible secret image sharing with steganography", Pattern Recognition Letters 31 **(2010)**, pp. 1887–1893.
[7] H. Luo, F. Yu, J-S Pan,Z-M Lu, "Robust and Progressive Color Image Visual Secret Sharing Cooperated with Data Hiding", Eighth International Conference on Intelligent Systems Design and Applications.IEEE,**(2008)**, pp. 431-436.
[8] X. Yan, S. Wang, AAhmed A.Abd El-Latif. And Xiamu Niu. "Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery". Multimidia Tools and Applications,24 December **(2013)**, pp. 1-22.
[9] W. D, Z. L,Ma N,et al, "Two secret sharing schemese base on Boolean operations". Pattern Recognit, vol. 40, no. 10, **(2007)**, pp. 2776-2785.
[10] S J Shyu, "Image encryption by random grids", Pattern Recognition, vol. 40, no. 3, **(2007)**, pp. 1014-1031.
[11] T H Chen, K H Tsao, "Threshold visual secret sharing by random grids", Journal of Systems and Software,vol. 84, no. 7, **(2011)**, pp. 1197-1208.
[12] X. Yan, S. Wang, and X. Niu, "Threshold construction from specific cases in visual cryptography without the pixel expansion", Signal Processing, Volume 105,December **(2014)**, pp. 389-398.

