Multi-secret Image Sharing Scheme based on coding method

Ying Yu, Hongliang Cai, Dan Tang* and Wei Yuan
School of Software Engineering, Chengdu University of Information Technology, Chengdu, Sichuan, 610225, China
*Corresponding author’s e-mail: 910776087@qq.com

Abstract. Image Secret sharing scheme is an effective way to share a secret message by distributing the shares to different owners which has become a relatively independent research field. The classical Shamir’s scheme is based on Lagrange interpolation polynomial, and the utility of the scheme is greatly compromised by the complex polynomial operations cost. Visual cryptography is a special image sharing scheme, which uses the human visual system to recover the secret information. Multi-secret shared visual cryptography is an important research part of visual cryptography. It can share several secret images, and have important significance for perfecting the theoretical system of visual cryptography and expanding the application fields of visual cryptography. In this paper, based on the research of the internal relations between the coding theory and the secret sharing, a Multi-secret Image Sharing scheme is proposed, the generation of the shares is realized by the binary Cauchy encoding. It satisfies the general characters of the secret image sharing schemes, and the algorithm complexity is low, which is easy for implementation.

1. Introduction
As an encryption technology that can effectively protect secret information, secret sharing was initially applied to key management. For example, a safe in a bank has five keys assigned to five administrators. The rule is that only more than three of the five administrators are present to open the safe door using the keys, less than three administrators cannot open the door. With the data reliability problem caused by the rapid growth of data volume, secret sharing technology has been broadened into the field of information security. An important branch of the field is the image secret sharing technology. The concept of visual cryptography was first proposed by Naor and Shamir [1] at the 1994 European Cryptography Conference. The basic secret sharing theory was rapidly applied to the image. In 1997, they first gave a secret sharing scheme on binary images [2], the share image is printed and composed by the black and white pixels on the transparent covers. The original secret image can be restored only if the certain covers are overlapped, and cannot be recognized by any other combination. The new idea proposed by the program has received great attention, but it still has problems such as the large pixel expansion and poor visual quality. Since then, in the field of image secret sharing, the program has also been gradually improved and enriched. The method of restoring the original image using the direct overlap share image was proposed by Hou [3] et al. in 2004. It can deal with the grayscale and color images, and is fit for secret image restoration without calculation. However, the drawbacks of the method are the size of the share image is too large, and the visual quality of the restored image is low.

The concept of secret sharing were first proposed in 1979 and realized by Shamir [4] and Blakley [5]. The sensitive secret sharing image is split into n shares, only on certain conditions the original
image can be reconstructed. In secret sharing, the set of all subsets authorized is called the access structure. A \((k,n)\) threshold secret sharing scheme is a kind of secret sharing method with special access structure, where \(k \leq n\). A \((k,n)\) threshold secret sharing scheme is dividing secret information into \(n\) sub-secrets and distributing the sub-secrets to \(k\) secret holders. Only at least \(k\) secret holders are present, the sub-secrets are overlapped to recover the secret information. No information can be recovered less than \(k\) secret information. Shamir's scheme is executed the polynomial operation on the finite field, once the size of the secret image is large, the computational efficiency is very low and cost a long recovery time [6]. To solve this problem, the current solution is to encrypt the data, and then protect the keys generated by this process [7].

A coding method based on the Reed-Solomon code is proposed in this paper and applied to the secret image sharing scheme of binary images[8]. Convert the Cauchy matrix on \(GF(2^m)\) to the Cauchy matrix on \(GF(2)\), replace the elements in \(GF(2^m)\) with the matrix of size \(m \times m\) on \(GF(2)\). Then the process of sharing secret image is realized by the encoding and the recovery process is realized by the decoding method. The method not only has the excellent characteristics of constructing the Cauchy RS code in the traditional finite field without parameter limitation, but also breaks through the disadvantages that the complex operations on the traditional finite field.

2. Related Background

2.1. Typical Image Secret Sharing Scheme

In the image secret sharing scheme with a \((k,n)\) threshold structure the image secret information is split into \(n\) shares, and these shares are sent to \(n\) different holders and stored safely. The scheme that best reflects the \((k,n)\) threshold structure and has the perfect property of image secret sharing is the image secret sharing scheme proposed by Thien and Lin [9] in 2002. There are many solutions for this type of prototype transformation, such as in the literature [10-13] and so on. This scheme is a \((k,n)\) threshold structure and the values of \(k\) and \(n\) can be set to any positive integer of \(2 \leq k \leq n\). The share image of the scheme is smaller than the original secret image, which effectively improves the hiding ability of the share image. However, the shortcomings of the scheme are also very obvious. Since this approach requires pre-processing of the original image, so that a portion of the original image pixel information is changed. Therefore, the reconstructed image is not completely equivalent to the original image.

2.2. RS Cauchy Code

Based on the fixed connection between image secret sharing and encoding, the MDS code can be used to construct a perfect secret sharing scheme. The RS code is a MDS (maximum distance separable) \((k,n)\) code which is proposed by Reed and Solomon in 1960 without limitation on \(n\) and the number \(m\), which \(m = n - k\). RS code encoding process is achieved by a polynomial operation on the elements of the Galois field \(GF(2^m)\).

**Coding Process.** Let the k-dimensional column vector \(L = [L_1, L_2, \ldots, L_k]\), and multiply with a Cauchy matrix \(G\) of size \(n \times k\), then get an n-dimensional column vector \(M = [M_1, M_2, \ldots, M_n]\) as follows:
Decoding Process. The known coding information and the corresponding row in the generator matrix are reserved to obtain a sub-matrix, and the sub-matrix is inferred. In this way, the obtained encoded information is multiplied by the inverse matrix to obtain the final original information. The corresponding rows in the generator matrix $G$ are removed to obtain a matrix $H$, $M$ is the corresponding information, and the matrix $Z$ is the inverse matrix of $H$.

$$
\begin{bmatrix}
g_{11} & g_{12} & \cdots & g_{1k} \\
g_{21} & g_{22} & \cdots & g_{2k} \\
\vdots & \vdots & \ddots & \vdots \\
g_{nk} & g_{n2} & \cdots & g_{nk}
\end{bmatrix}
\times
\begin{bmatrix}
L_1 \\
L_2 \\
\vdots \\
L_k
\end{bmatrix}
= 
\begin{bmatrix}
M_1 \\
M_2 \\
\vdots \\
M_n
\end{bmatrix}
$$

(1)

3. Coding-based Multi-secret Image Sharing

Based on the relationship between image secret sharing and encoding, this paper constructs the multi-secret image sharing scheme according to the encoding and decoding method of binary RS Cauchy code. Take sharing and recovery of secret images $A$ and $B$ as an example, a $(k, q, n)$ threshold multi-secret sharing scheme is constructed. The scheme of this paper will be described from two parts: the generation process of the share image and the reconstruction process of the secret image. First, a Cauchy matrix $G$ of size $nk \times nk$ is constructed, and it is specified that each element in the matrix $G$ belongs to the finite field $GF(2^m)$. Second, the element is represented as a matrix of size on the $GF(2)$, where the values of $k$ and $n$ need to satisfy $2^m \geq n + k$. So the matrix $G$ is converted into a generator matrix $G$ of size $mn \times mk$.

The $mk$ pixel of a binary image is divided into a group, and a vector of the $mk$ pixels and the generator matrix are multiplied to output a vector of $mn$ bits generated from the generation matrix $G$. The $m$ data blocks are combined into one data information, and a total of $n$ pieces of data information are obtained. The $n$ pieces of data information are then distributed to participants of the sharing scheme. When the secret is restored, the obtained sub-matrix is inverted. The data information extracted from the share image is grouped into $mn$ groups. The original secret image can be obtained by the inverse matrix. The detail is described below on the present embodiment and the share image generation process and the secret image reconstruction process.

3.1. Generating Share Image

In the $(k, q, n)$ threshold secret image sharing scheme, the secret image $A$ generates $n$ shares by threshold secret sharing. Where $k$ or more than $k$ shares are overlapped, the original secret image $A$ can be recovered, and less than $k$ share images cannot acquire any information. The pixels of the secret image $A$ and the secret image $B$ are subjected to XOR operation to obtain an intermediate image $C$. 

$$
\begin{bmatrix}
z_{11} & z_{12} & \cdots & z_{1k} \\
\vdots & \vdots & \ddots & \vdots \\
z_{q1} & z_{q2} & \cdots & z_{qk}
\end{bmatrix}
\times
\begin{bmatrix}
g_{11} & g_{12} & \cdots & g_{1k} \\
g_{21} & g_{22} & \cdots & g_{2k} \\
\vdots & \vdots & \ddots & \vdots \\
g_{nk} & g_{n2} & \cdots & g_{nk}
\end{bmatrix}
\times
\begin{bmatrix}
L_1 \\
L_2 \\
\vdots \\
L_k
\end{bmatrix}
= 
\begin{bmatrix}
z_{11} & z_{12} & \cdots & z_{1n} \\
\vdots & \vdots & \ddots & \vdots \\
z_{q1} & z_{q2} & \cdots & z_{qn}
\end{bmatrix}
\times
\begin{bmatrix}
M_1 \\
M_2 \\
\vdots \\
M_k
\end{bmatrix}
$$

(2)
The intermediate image $C$ generates $n$ shares by secret sharing of thresholds. The $q$ and $q$ or more share images overlap to recover the intermediate image $C$, and less than $q$ share images cannot acquire any information. The encoding process consists of Figure 1 and Figure 2:

**Figure 1. Generate matrix structure diagram.**

![Generate matrix structure diagram](image1)

**Figure 2. Coding structure diagram.**

![Coding structure diagram](image2)

Step 1: Set the set $s_1, s_2, \ldots, s_n$ of number $n$, and number the $n$ sets by $n_i = i$.

Step 2: Extract $mk$ pixels that have not been shared from the secret image $A$ according to a fixed order. The value corresponding to the $mk$ pixels is denoted as $p_1, p_2, \ldots, p_{mk}$, and the transposition operation of $p_1, p_2, \ldots, p_{mk}$ is recorded as $\alpha$.

Step 3: According to the above generation matrix $G$, encode $\alpha$ to obtain $\beta$, $\beta = G \cdot \alpha$.

$$
G \cdot \alpha = \begin{bmatrix}
g_{11} & g_{12} & \cdots & g_{1,kw} 
g_{21} & g_{22} & \cdots & g_{2,kw} 
g_{31} & g_{32} & \cdots & g_{3,kw} 
\vdots & \vdots & \ddots & \vdots 
g_{m1} & g_{m2} & \cdots & g_{m,kw}
\end{bmatrix}
\times
\begin{bmatrix}
p_1 
p_2 
\vdots 
p_{mk}
\end{bmatrix}
= \begin{bmatrix}
0 
1 
\vdots 
0
\end{bmatrix}
$$

(3)

Step 4: Place the $n$ elements in $\beta$ generated in step 3 into the set in step 1 respectively.

Step 5: Repeat steps 2-4 until all pixels of the secret image $A$ are processed.

Step 6: The $n$ sets after the above steps are the initial share information of the secret image $A$.

Step 7: The pixel of the secret image $A$ is scrambled using the permutation function. The pixels of the secret image $A$ and the secret image $B$ are XOR to obtain an intermediate image $C$.

Step 8: Set the set $s_1, s_2, \ldots, s_n$ of number $n$ and number the $n$ sets by $n_i = i$.

Step 9: Extract $qm$ pixels that have not been shared from the intermediate image $C$ according to a fixed order. The value corresponding to the $qk$ pixels is denoted as $p_1, p_2, \ldots, p_{qm}$, and $p_1, p_2, \ldots, p_{qm}$ records the transpose operation as $\alpha'$.

Step 10: Encode $\alpha'$ according to the above mentioned generation matrix $G'$ to obtain $\beta'$, $\beta' = G' \cdot \alpha'$.
\[
\begin{bmatrix}
1 & 0 & 1 & \cdots & 1 & 0 \\
1 & 1 & 0 & \cdots & 0 & 1 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 1 & 0 & \cdots & 1 & 0 \\
\end{bmatrix}
\times
\begin{bmatrix}
0 \\
1 \\
\vdots \\
0 \\
\end{bmatrix}
= 
\begin{bmatrix}
0 \\
1 \\
\vdots \\
0 \\
\end{bmatrix}
\quad (4)
\]

Step 11: Until all the pixels in the intermediate image \( C \) are processed, the \( n \) sets are the initial share information of the intermediate image \( C \).

Step 12: Select several images with the same size as the secret image as the host images.

The initial share information of the secret image \( A \) obtained in step 6 and the intermediate image \( C \) are embedded in the host image according to the data of the \((q,n)\) threshold. So we can get \( n \) shares of the secret sharing scheme.

### 3.2. Reconstructing Secret Images

The secret image \( A \) generates \( n \) shares by secret sharing of \((k,n)\) thresholds, wherein \( k \) and \( k \) or more share images are overlapped to recover the original secret image \( A \). The intermediate image \( C \) is generated by \((q,n)\) threshold secret sharing. The share, in which the \( q \) and \( q \) or more share images are overlapped, can restore the intermediate image \( C \). The secret image \( B \) requires the intermediate image \( C \) and the secret image \( A \) to perform an exclusive OR operation.

Step 1: Set a set \( S \) corresponding to the original image \( A \).

Step 2: Extract the share data information related to the image \( A \) from the \( k \) share image, and divide it into group of size \( nm \) data, and set it as \( \beta \).

Step 3: Construct another matrix \( Z \), assign the value of the generator matrix \( G \) to the matrix \( Z \) from the first row, and then invert the matrix \( Z \), denoted as \( Z \).

Step 4: Multiply the matrix \( Z \) and \( \beta \), and the result is \( \alpha \), \( \alpha = Z \cdot \beta \).

Step 5: Put the \( km \) elements in the results of the above steps into \( S \) in a fixed order.

Step 6: Repeat steps 1-5 according to the pixel points until all calculations are completed to obtain the original image \( A \).

Step 7: Set a set \( S \) corresponding to the intermediate image \( C \).

Step 8: Extract the share data information related to the intermediate image \( C \) from the \( q \) share image. The data is divided into groups according to \( nm \) data, and is recorded as \( \beta^\prime \).

Step 9: Construct another matrix \( X \), assign the value of the generator matrix \( G \) to the matrix \( X \) from the first row, and invert the matrix \( X \), denoted as \( X \).

Step 10: Multiply the matrix \( X \) and \( \beta^\prime \), and the result is \( \alpha^\prime \), \( \alpha^\prime = X \cdot \beta^\prime \).

Step 11: Put the \( qm \) elements in the results of the above steps into \( S \) in a fixed order.

Step 12: Repeat steps 7-11 until all calculations are completed to obtain the intermediate image \( C \).

Step 13: XOR the intermediate image \( C \) and the secret image \( A \) to obtain a secret image \( B \).

The multi-secret image sharing scheme used in this paper can use of the available space of the host image more effectively and improve the information storage capacity of images. In terms of image secret sharing, secret images \( A \) and \( B \) having different visual meanings can be continuously recovered. Moreover, when the scheme is applied to the transmission of the real secret information, the secret image \( B \) can be set as true secret information, and the secret image \( A \) is confusing information. At this time, even if the enemy intercepts the \( k \) share images for direct recovery, the secret image seen is the confusing image information \( A \). This scheme also provides more protection for the real secret image \( B \).
4. Typical Experiment
Take the \((4, 5, 7)\) multi-threshold image secret sharing as an example to test the algorithm scheme in this paper. The original secret image is divided into 7 share images. 4 of the 7 share images can recover the secret image \(A\), and 5 of the 7 share images can recover the secret image \(B\).

Figure 3 is the secret image \(A\) of the experiment. Figure 4 is a secret image \(B\). Seven different share images are generated according to the above algorithm in this paper, as shown in Figures 5(a)-(g). Overlapping four share images can restore Figure 6, and overlapping five share images can be restored to Figure 7.

![Figure 3. Secret image A.](image1)
![Figure 4. Secret image B.](image2)
![Figure 5(a). Share image 1.](image3)

![Figure 5(b). Secret image 2.](image4)
![Figure 5(c). Secret image 3.](image5)
![Figure 5(d). Secret image 4.](image6)

![Figure 5(e). Secret image 5.](image7)
![Figure 5(f). Secret image 6.](image8)
![Figure 5(g). Secret image 7.](image9)

![Figure 6. Reconstructed secret image A.](image10)
![Figure 7. Reconstructed secret image B.](image11)

The four image shares of (a) to (g) in Fig.5 can be used to recover the secret \(A\) in Fig.6, and the five share images can be used to recover the secret \(B\) in Fig.7. It obviously shows that Fig.6 is same to the secret image \(A\), and Fig.7 is same to the secret image \(B\). The scheme of this paper can realize the exact image secret reconstruction.

5. Conclusion
The multiple secrets sharing scheme based on coding method proposed in this paper uses the encoding model of RS Cauchy code to realize multiple secret images sharing and recovery. The operation is XOR on the binary domain, which has a prominent operation performance. And the scheme can exploit the available space of the host image, which can improve the information storage capacity of images and provides better protection for the real secret image. Moreover, the image shares are equal to the secret image, so the scheme is more secure. At last, the scheme and has strong practicability and low algorithm complexity.

Acknowledgments
This work was financially supported by the project of Sichuan Science and Technology Department (2019YFG0103) and the project of Sichuan Educational Commission (18ZB0127).

References
[1] Naor, M., Shamir, A. (1994) Visual cryptography. Lecture Notes in Computer Science. Commun.,950(9), 1-12.
[2] Naor, M., Shamir, A. (1996) Visual cryptography II: Improving the contrast via the cover base. In: Lomas M. (eds) Security Protocols. Security Protocols 1996. Lecture Notes in Computer Science. Commun., 1189: 197-202.

[3] Hou, Y., Du, S. (2004) Visual Cryptography techniques for Color Images without Pixel Expansion. Journal of Information. Technology and Society. Commun., 109(1): 87-95.

[4] Shamir, A. (1979) How to share a secret. Communications of the ACM. Commun., 22: 612-613.

[5] Blakley, G. (1979) Safeguarding cryptographic keys. In: AFIPS 1979 National Computer. New York, pp. 313-317.

[6] Kurihara, J. (2008) A New (k,n)-Threshold Secret Sharing Scheme and Its Extension. In: Information Security. ISC 2008. Berlin, pp. 455-470.

[7] Yang C., Lai J. (2013) Protecting data privacy and security for cloud computing based on secret sharing. In: 2013 International Symposium on Biometrics and Security Technologies. Chengdu, pp. 163-185.

[8] Shyu, S., Chen K. (2011) Visual multiple secret sharing based upon turning and flipping. Information Sciences. Commun., 181(15): 3246-3266.

[9] Thien, C., Lin, J. (2002) Secret image sharing. Computers & Graphics. Commun., 26(5): 765-770.

[10] Chang, C., Lin, C. (2008) A novel secret image sharing scheme in color images using small shadow images. Information Sciences. Commun., 178(11): 2433-2447.

[11] Tsai, D., Horng G. (2009) A novel secret image sharing scheme for true-color images with size constraint. Information Sciences. Commun., 179(19): 3247-3254.

[12] Zhou, Z., Yang, C. (2018) Secret Image Sharing based on Encrypted Pixels. In: IEEE Access, pp. 1-1.

[13] Li, P., Yang, C. (2016) A novel two-in-one image secret sharing scheme based on perfect black visual cryptography. Journal of Real-Time Image Processing. Commun., 14(1): 41-45.