A NOVEL IMAGE SECRET SHARING SCHEME WITH MEANINGFUL SHARES

Hongliang Cai[1,2]*, Huajian Liu*[2]*, Qizhao, Yuan*[1]*, Martin Steinebach*[2]*, Xiaojing Wang*[1]

[1] Chengdu Institute of Computer Applications, Chinese Academy of Sciences, China
[2] Fraunhofer SIT, Darmstadt, Germany

ABSTRACT

In this paper a novel *(t, n)* threshold image secret sharing scheme is proposed. Based on the idea that there is close connection between secret sharing and coding theory, coding method on $GF(2^m)$ is applied in our scheme instead of the classical Lagrange's interpolation method in order to deal with the fidelity loss problem in the recovery. All the generated share images are meaningful and the size of each share image is the same as the secret image. The analysis proves our scheme is perfect and ideal and also has high security. The experiment results demonstrate that all the shares have high quality and the secret image can be recovered exactly.

Index Terms— image secret sharing, image encryption, multimedia security, coding theory

1. INTRODUCTION

In cryptography, a *(t, n)* secret sharing scheme is a method for distributing a secret among a group of n participants, each of which is allocated with a share of the secret. The secret can be easily restored from at least t shares, any group of less than t shares can't retrieve any information about the secret. The first secret sharing scheme is introduced by Moni Naor and Adi Shamir in 1979 [1]. The classical secret sharing scheme based on interpolation polynomial is perfect and ideal [2, 3] which are two key evaluations for secret sharing scheme. However, it is primarily concentrating on the pure digital data and don't take the content of the data into account.

In 1994, Moni Naor and Adi Shamir proposed *(t, n)* VCS (Visual Cryptography Scheme) [4] for binary image. As shown in Fig. 1, it can generate shares on transparencies and the decryption is realized by easily stacking the shares to reveal the secret image by the aid of human vision system. However, the secret only can be very simple binary image, there is also pixel expansion problem which means the size of each share is larger than the original secret image. And all the shares are meaningless, the quality of the recovered secret image is also rather low. In recent years many secret sharing schemes based on the work in [4] are developed in different directions. For example, to solve pixel expansion problem, some probabilistic VCS [5-8] are proposed, but as a tradeoff, the quality of the recovered image is lower. Some other image secret sharing schemes are developed for gray image and color image, but the recovered secret image is always so poor that it is very hard to recognize the content of the image. So most of the secret sharing schemes based on VCS don't have the property that it is ideal and perfect and also have high recovery ability because of the inherit limitation of VCS.

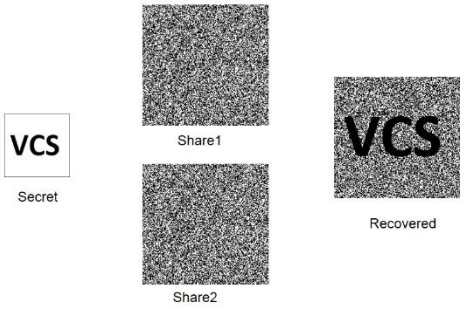

Fig. 1 An example of (2, 2) VCS

In 2002, C.C Thien and J.C. Lin proposed a novel *(t, n)* image secret sharing scheme based on Lagrange's interpolation [9]. The size of each share is reduced to 1/ t of the original secret image and all the shares are meaningless. Many other works following the basic idea in [9] have been developed in different aspects, such as, hiding the reduced shares into large host images [10,11] to improve security in transmission, reducing the size of shares by lossy or lossless compression[12]. However, these schemes still have two crucial weaknesses. First, Lagrange's interpolation method requires the computation is operated on $GF(p)$, where p is a prime number, so some pixel values of a 8-bit grey image have to be truncated to 251, which will introduce fidelity loss for the recovered secret image. Secondly, the reduction in size of share is not secure for secret sharing scheme, the size of shares should be the same as the size of the original secret. Although the shares can be hided into other images to make them the same size, yet only part information of shares have relationship to the secret, the weakness in security is not eliminated. In [13] G. Alvarez et al. constructed an ideal scheme for image sharing based on reversible cellular automata. However, this scheme is restricted to the threshold *(n, n)*. So it is still a challenge to construct an ideal and perfect secret sharing scheme with meaningful shares and high quality of recovered secret image.

In this paper we propose a novel *(t, n)* image secret sharing scheme based on coding method. Since the pixel value of the image is presented by m bits in the computer, which is actually isomorphic to $GF(2^m)$, and the image can be

regarded as pixel value matrix, the image secret sharing is operating on the pixel value matrix on $GF(2^m)$. And based on the fact that there is close connection between secret sharing and coding theory, algebraic-geometry code on $GF(2^m)$ is applied into our scheme to solve the fidelity loss problem in the recovery, the recovered secret image can be exactly the same as the original secret image. Moreover, there is no pixel expansion problem and the size of each share image is equal to the size of the secret image. Furthermore, two stage coding method is applied in the encryption process to make all the shares meaningful, and all the pixels of each share have mathematical relationship with the secret image. The scheme is perfect and ideal and has high security.

The rest of this paper is organized as follows. In Section 2, the basic idea and proposed coding-based image secret sharing scheme is introduced. The analysis and experiment are given in Section 3. Section 4 is the conclusion.

2. PROPOSED SCHEME

2.1 Basic idea

There are two important evaluation properties for a good secret sharing scheme, perfect and ideal. A *(t, n)* secret sharing scheme is perfect if any authenticated subset of at least t participants can determine the original secret, while any subset of less than t participants can determine nothing about the secret. Ideal means that the data size of each share should be the same as the data size of the secret. Otherwise, if the data size of each share is smaller than the secret, the adversary can search in a small space to get some information about the secret, it is not secure for the original secret. If the share image is larger than the secret image, it is a waste of storage.

For the image secret sharing scheme, except the fundamental properties of perfect and ideal, we also hope that the image secret sharing scheme can generate the meaningful shares and the secret image should be recovered losslessly.

There is close relationship between secret sharing and coding, McEliece and Sarwate pointed out that Shamir's secret sharing scheme can be explained by the Reed-Solomon codes in [14]. In fact, *(t, n)* secret sharing scheme is isomorphic to (t, n) linear MDS code [15, 16]. A *(t, n)* linear code is the MDS (Maximum-Distance Separable) code if the minimum hamming distance of the codewords is $n - t + 1$ and any t encoded symbols can decode to get the original information. So the secret sharing in fact can be presented by coding paradigm in a more general way, the encoding and decoding process is isomorphic to the encryption and decryption in the secret sharing.

Based on this basic idea and considering the characteristic of the pixel presentation, algebraic - geometry code on $GF(2^m)$ is used in our scheme instead of the interpolation polynomial method. The systematic code form which means that the first t outputs are the same as the t original inputs is applied in the coding process so that it will be helpful in making the shares meaningful.

The generating matrix and the checking matrix play a central role in the secret sharing scheme based on coding method. In the following the construction of generating matrix in the encoding process and the checking matrix in the decoding process are shown as bellow:

Supposing $GF(q)$ is a subfield of $GF(2^m)$, $n \le q - 1 \le 2^m - 1$, and g is a primitive element of $F(q)$, $a_1 = g^1, a_2 = g^2, \ldots, a_n = g^n$ are n distinct nonzero elements of $GF(q)$. *The* $n \times (n-t)$ checking matrix H is:

$$H_{n\times(n-t)} = \begin{bmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-t-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-t-1} \\ 1 & a_3 & a_3^2 & \ldots & a_3^{n-t-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-t-1} \end{bmatrix}$$

The $n \times t$ generating matrix is:

$$D_{n\times t} = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \\ d_{t+1,1} & d_{t+1,2} & d_{t+1,3} & \ldots & d_{t+1,t} \\ d_{t+2,1} & d_{t+2,2} & d_{t+2,3} & \ldots & d_{t+2,t} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ d_{n,1} & d_{n,2} & d_{n,3} & \ldots & d_{n,t} \end{bmatrix}, d_{ij} \in GF(2^m).$$

The matrices have the property that each column of $D_{n\times t}$ is orthogonal to every column vector of $H_{n\times(n-t)}$. Notice that the checking matrix is the Vandermonde matrix, so arbitrary $n-t$ row vectors of $H_{n\times(n-t)}$ are linear independent. In fact in coding theory, the linear space of the solutions for the linear equation group $H^T_{n\times(n-t)} \cdot \beta_{n\times 1} = 0$ can construct a *(t, n)* linear MDS code , which is a special AG code [14,17], and the generating matrix of the MDS code can be transformed into the form where the upper $t \times t$ submatrix is an identity matrix. So the encoding process is $\beta_{n\times 1} = D_{n\times t} \cdot \alpha_{t\times 1}$ *over* $GF(2^m)$, and the decoding is solving $H^T_{n\times(n-t)} \cdot \beta_{n\times 1} = 0$ *to get* α.

2.2 Proposed scheme

Suppose there are r secret images $S_1, S_2, \ldots, S_r$ which are the same size, each image has L pixels, and P is the coordinate position in the pixel matrix. Take the 8 bit gray image for the example, regard each secret image as a pixel matrix, the *(t, n)* image secret sharing is constructed as below, $k = n - t$. Two stage coding method is applied in our method to make all the shares meaningful.

The encryption process:

(1) Select arbitrary n meaningful images of the same size as the secret images where $\lceil 8(r+k)/t \rceil$ LSBs are set to zero in all the images and get the pixel matrices I_i *(i=1, ...,n);*

(2) The encoding is done from pixel to pixel. In the first encoding stage, take the position P for example, get all the pixels of the r secret images and n images in (1) in position P to form a vector $\alpha_{(n+r)\times 1} = (a_1, \ldots, a_r, \ldots, a_{n+r})^T$, encode with generating matrix to get vector β, $\beta = D_{(n+2r+k)\times(n+r)} \cdot \alpha_{(n+r)\times 1}$, where the multiplication between the matrix D and vector α is operating on the field $GF(2^m)$. Since the upper part of $D_{(n+2r+k)\times(n+r)}$ is an identity matrix, the first n+r elements of the vector β are the same as $\alpha_{(n+r)\times 1}$, i.e. $\beta = (a_1, \ldots, a_r, \ldots, a_{n+r}, b_1, \ldots, b_{r+k})^T$. Put all the $n+2r+k$ elements to the according position of $n+2r+k$ pixel matrices, when all L pixel positions are traversed, the former $r+n$ matrices are the same as r secret image matrices and n images in (1) , the latter $r+k$ pixel matrices $G_1, \ldots, G_{r+k}$ are in fact meaningless intermediate images;

(3) Divide $G_1, \ldots, G_{r+k}$ into t pieces $X = \{X_i, i = 1, \ldots, t\}$. In the second encoding stage, Similar as encoding for every pixel position in (2), encode X with generating matrix $D_{n\times t}$ and put the results in n matrices, so we can get n symbols $Y=\{Y_j, j=1, \ldots, n\}$;

(4) Embed Y_i into the i_{th} selected meaningful image in (1) from the lowest LSB as necessary, finally we get the n share images $I_1', \ldots, I_n'$.

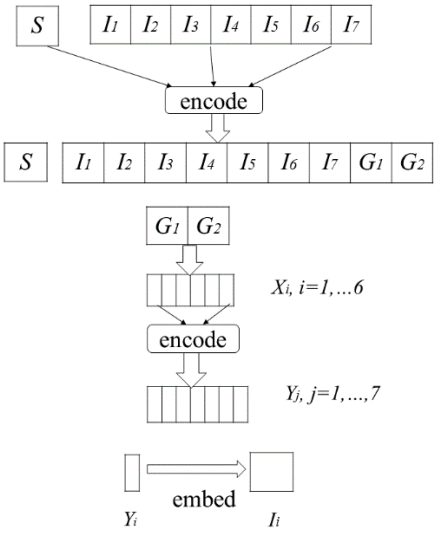

Fig. 2 Encryption of (6, 7) image secret sharing, r=1

The decryption process from arbitrary t share images is as below:

(1) Extract t embedded symbols Y' from t shares I' and padding the relevant LSB place with *0*, decode in each pixel position from Y' using the checking matrix $H_{n\times(n-t)}$ to get X;

(2) Rearrange the output t symbols of (1) into $r+k$ pixel matrices G_i, $i = 1, \ldots, r+k$;

(3) Joint G_i $(i = 1, \ldots, r+k)$ with the t pixel matrices of meaningful shares where the embedded symbols are extracted, there are $n+r$ pixel matrices, decode in the similar way from pixel to pixel to get pixel matrices of the r secret images.

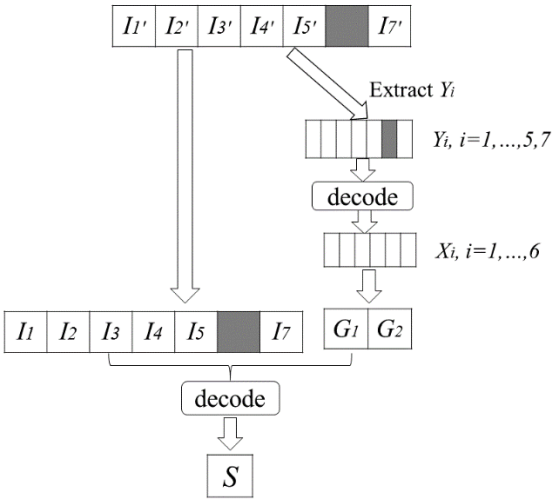

Fig. 3 Decryption of (6, 7) image secret sharing, r=1

3. ANALYSIS AND EXPERIMENT

First we simply analyze the feasibility of the decryption process. In the first encoding stage of encryption, jointed with the r secret images and the n selected meaningful images, the $n + r$ images take part into the encoding as the input using generating matrix $D_{(n+2r+k)\times(r+n)}$ and generate $n + 2r + k$ output, it is in fact a $(n+r, n+2r+k)$ threshold. In the second encoding stage, the latter r+k meaningless intermediate images in the first stage are rearranged into t pieces and participate into encoding using the matrix $D_{n\times t}$, it is a (t, n) threshold. When there are t participated share images in the decryption, in the first decoding stage, the t extracted symbols can decode to get $r+k$ meaningless intermediate images G_i, and in the second decoding stage, jointed with the t meaningful shares images, the $n+r$ images are enough to reconstruct r secret images.

The performance analysis is given out in two evaluations for secret sharing, security and the image quality. And comparison with some research before is included.

There are two important evaluations for secret sharing schemes: perfect and ideal. Firstly, the success of decryption shows that arbitrary t shares can recover the secret image, when the participated shares are less than t, it is impossible to decode to get any information about the secret, because in fact this is equal to solve the set of equations where the number of equations is less than the number of unknown quantity. So this scheme is perfect. Secondly, the size of each share is the same as the secret image, it shows the scheme is also ideal. While in the scheme in [9-11], if we do not consider the information hiding process, the pixel number of each share which is generated under the threshold (t, n) is in fact $1/t$ of the secret image, it is not ideal.

In the security aspect, in the first encoding stage all the meaningful images and the secret images take part in encoding, then the pieces of the output meaningless images

in the first stage are coded again and embedded into LSB of the selected n meaningful images, so in fact all the data of the final n share images have mathematic relationship with the secret images. In contrast, there is no relationship between the selected meaningful host images and the secret images in [10,11], so it will introduce the security problem that the adversary maybe retrieve the secret when getting only small part of hidden information in the shares.

In the image quality aspect, the recovered secret image is exactly the same as the original secret image, because we use coding method on $GF(2^m)$ which is suitable for the characteristic of pixel presentation and the pixel matrices are decoded perfectly. While in the schemes [9-11] based on the field $GF(p)$, some pixel value of the secret image which is larger than 251 have to be truncated, so there is fidelity loss in the recovery. And in Visual Cryptography scheme, the quality of the recover image is always very low and the content can be only recognized roughly by human's eyes.

The quality of the share images is also taken into account in our scheme because after two stage encoding all the final shares are meaningful. Supposed R LSBs of the selected meaningful images are preserved for the embedding space, we can easily know $R = 8(r + k) / t$. From the perspective of information hiding capacity in spatial domain, the expected quality of the embedded images are higher than 37 dB when $8(r + k) / t \leqslant 3$, it is almost imperceptible by human eyes. However, it is impossible for VCS schemes and many other image secret sharing schemes.

In addition, as a novel scheme based on coding method different with the classical interpolation polynomial method, the computation complexity is also lower, and the computation can further speed up by dividing the m bit plain into two parts m_1 and m_2 and parallelly execute on small field $GF(2^{m1})$ and $GF(2^{m2})$, and if we continue to divide it into smaller parts, the computation will be faster.

Table 1 shows the comparison between our scheme and different kinds of secret sharing schemes.

Table 1 Comparison with other secret sharing schemes

	Perfect	Ideal	Meaningful shares	Recovery
Our scheme	Yes	Yes	Yes,high quality	Exact
The scheme in [9]	Yes	No	No	Not Exact
The scheme in [10,11,12]	Yes	No	Yes	Not Exact
VCS [4]	Yes	No	No	Low quality

The following is an example of (6, 8) secret sharing scheme. As we all known, the RGB color image can be converted into 3 greyscale images. So our scheme is also available for the color image. Fig. 4 is the experiment result on color image.

(a) The secret image

(b) The 8 share images

(c) The recovered secret image

Fig. 4 An example of (6 , 8) scheme

4. CONCLUSION

This paper proposed a novel secret sharing scheme with meaningful shares. Coding method is applied in the scheme because it is a more general model than the interpolation polynomial method. The algebraic-geometry code over $GF(2^m)$ is used instead of $GF(p)$ in many previous work because the presentation of image pixel value on the computer is actually isomorphic to $GF(2^m)$, so it will bring the benefit that the recovered secret image is exactly the same as the original one. In addition, in order to make all the share images meaningful, two coding stage are applied in the encryption process and the information hiding technology is used. And the payload is low so that the quality of the share images is high. The analysis proves that our scheme is perfect and ideal, and has better security and performance than many other existing schemes.

5. AKNOWLEDGMENTS

This work is supported by CASED (Center for Advanced Security Research Darmstadt).

6. REFERENCE

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[2] E. Dawson, and Diane Donovan, "The breadth of Shamir's secret-sharing scheme," *Computer and Security*, no. 13, pp. 69–78, 1994.

[3] M. Van Dijk, "On the information rate of perfect secret sharing schemes," *Designs, Codes and Cryptography*, vol. 6, no. 2, pp. 143–169, 1995.

[4] M. Naor, and A. Shamir, "Visual cryptography," *Advances in Cryptology: Eurocrypt'94, Berlin: Springer-Verlag*, pp. 1–12, 1995.

[5] R. Ito, H. Kuwakado and H. Tanaka, "Image size invariant visual cryptography*," IEICE TRANS. FUNDAMENTALS*, vol. E82-A, no. 10, pp. 2172–2177, 1999.

[6] Yi, F., Wang, D., Li, S., & Dai, Y, "Probabilistic visual cryptography scheme with reversing," *JOURNAL-TSINGHUA UNIVERSITY*, *48*(1), 121, 2008.

[7] S. Cimato, R. De Prisco and A. De Santis, "Probabilistic visual cryptography schemes," *The Computer Journal*, vol. 49, no. 1, pp. 97–107, 2006.

[8] Ching-Nung Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognition Letters*, vol. 25, no. 4, pp. 481–494, 2004.

[9] C. C. Thien, and J. C. Lin, "Secret image sharing," *Comput. Graph*, vol. 26, no. 5, pp. 765–770, 2002.

[10] Thien Lin, "An image-sharing method with user-friendly shadow images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 12, pp. 1161–1169, 2003.

[11] Yu-Shan Wu, Chih-Ching Thien and J. -C. Ja-Chen Lin, "Sharing and hiding secret images with size constraint," *Pattern Recognition*, vol. 37, no. 7, pp. 1377–1385, 2004.

[12] Chin-Chen Chang, Chia-Chen Lin, Chia-Hsuan Lin and Yi-Hui Chen, "A novel secret image sharing scheme in color images using small shadow images," *Information Sciences: an International Journal*, vol. 178, no. 11, pp. 2433–2447, 2008.

[13] G. Alvarez, Ascensión Hernández Encinas, Luis Hernández Encinas and Ángel Martín del Rey, "A secure scheme to share secret color images," *Computer Physics Communications*, vol. 173, no. 1-2, pp. 9–16, 2005.

[14] R. J. McEliece, and D. V. Sarwate, "On sharing secrets and Reed-Solomon codes," *Comm. ACM*, vol. 24, no. 9, pp. 583–584, 1981.

[15] James L. Massey, "Minimal codewords and secret sharing," *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, pp. 276–279, 1993.

[16] G. R. Blakley, and G. A. Kabatianski, "Ideal perfect threshold schemes and MDS codes," *IEEE Conference Proc., International Symposium on Information Theory*, ISIT'95, pp. 488, 1995.

[17] F. J. MacWilliams, and N. J. A. Sloane, "The theory of error-correcting code," *New York: North-Holland Publishing Company*, 1977.