Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 29 (2012) 27 – 32

Procedia Engineering

www.elsevier.com/locate/procedia

2012 International Workshop on Information and Electronics Engineering (IWIEE)

The Research of Secret Image Sharing Based on RS Erasure Code

Dan Tang[a*]

[a]*Chengdu University of Information Technology, Chengdu, 610225, China*

Abstract

Secret image sharing is an attractive research problem in information security filed. After more than ten years of development, secret image sharing has become a relatively independent area. Most current secret image sharing scheme used Lagrange interpolation of Shamir scheme as the core idea, but which way will greatly reduce the computational efficiency and system availability without a doubt because of a huge amount of data in images. According to the internal relationship between coding theory and secret sharing technology, the paper proposed a secret image scheme based on coding theory. In addition to have advantages which most secret image sharing schemes based on Lagrange interpolation own, the new method which has a more simple idea reduced computational complexity and easy to extend the field of video and audio, so has a more obvious practical value; The design and realization of the new secret image sharing scheme has indirectly proved the internal relationship between coding and secret sharing scheme.

Keywords: Secret sharing; RS Erasure Code; Digital image; Lagrange interpolation;

1. Introduction

As the development of computer technology, using digital information to communicate has gradually become the primary way of communication. Compared to many other types of digital information, the digital image was expressed as an important means of information transmitted through networks because of its vivid and intuitive characteristics. Therefore, how to effectively protect a digital image which has sensitive or confidential information has become an important issue. Encryption is a conventional method to protect secret information; we can encrypt secret or sensitive images to prevent the leakage of

* Corresponding author. Tel.: +86-18980649391.
E-mail address: tangdan@foxmail.com.

doi:10.1016/j.proeng.2011.12.662

confidential information. However, compared with text information, image information has its own unique properties, such as strong correlation, high redundancy and so on. If copying the encryption method of text data to digital images, the encryption would be difficult to get good results. Of course, we can design encryption scheme specifically for digital image. The use of secret sharing technology to protect image is another possible way. The concept of secret sharing scheme proposed for the first time by Shamir[1] and Blakley[2] in 1979, as the practicality of the technology, which has been developed rapidly [4~7]. At Cryptography Conference of Europe in 1994, Naor and Shamir expand the research of secret sharing scheme to image area [4]. Along with the widespread application of image, secret image sharing technology also has obtained an enormous development, the new secret image sharing scheme was proposed unceasingly [8~12] . However, the structure of which schemas are follows the classical idea of Shamir secret sharing scheme but different levels: Either build the entire system, or protect some important information use Lagrange interpolation to complete which design. The computational complexity of Lagrange interpolation is high and image usually contains great amount of information, and which led the Low efficiency of those schemes based on Lagrange interpolation, and most methods to improve computational efficiency would reduce security of the entire scheme. As above, we try to find a new way to break through this problem, and proposed a secret image sharing scheme based on RS Erasure Code.

2. The secret image sharing scheme based on RS erasure code

There is some intrinsic link between coding and secret sharing technology, Massey had pointed out which relation essentially in 1993 [13], and the MDS code is corresponding to the secret sharing scheme of Perfect [14]. Unfortunately, such a link was not draw attention to researchers in the field of secret image sharing for a long time. In this paper, we induct coding theory into secret image sharing technology, design a corresponding RS erasure code according to threshold structure, and realize secret image sharing through coding and decoding.

We define some symbols as follows, *S*: Secret Image; (*k,n*): Parameters of threshold structure; *L*: The number of pixels in the secret image.

The generation progress of shadows is as follows:

Step1. Identify the generator matrix *G* according to parameters *k* and *n* of threshold structure as follows:

$$G_{(k+n)\times k}=\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ d_{k+1,1} & d_{k+1,2} & d_{k+1,3} & \cdots & d_{k+1,k} \\ d_{k+2,1} & d_{k+2,2} & d_{k+2,3} & \cdots & d_{k+2,4} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ d_{k+n,1} & d_{k+n,2} & d_{k+n,3} & \cdots & d_{k+n,k} \end{pmatrix}$$

Step2. Take *k* pixels which have not been operated from the secret image *S* by some order, and the values of which k pixels can constitute a vector $\alpha_{k\times 1}=(a_1,a_2,\cdots,a_k)^{\Gamma}$.

Step3. Encode the vector identified in step 2 with the generator matrix G constructed in step 1: $\beta_{(k+n)\times 1}=G_{(k+n)\times k}\cdot\alpha_{k\times 1}$, and the final result is $(k+n)\times 1$ .dimension vector, and denote it as $(b_1,b_2,\cdots,b_{k+1},b_{k+2},\cdots,b_{k+n})$.

Step4. Seen by the structure of the generator matrix G: $a_i = b_i, 1 \le i \le k$, so conserve the last n elements of the vector β temporarily.

Step5. Repeat step 2 to step 4, until all of pixels in the secret image have been calculated. If the remnant number of the secret image is less than k when the last calculation, and then make up with 0.

Step6. After all calculations finished, we get $\lceil L/k \rceil$ set of data which have the same structure, $(b_{k+1}, b_{k+2}, \cdots, b_{k+n})$.

Step7. Arrange the $\lceil L/k \rceil$ set of data above, we can get a matrix, and denote it as V.

$$V = \begin{pmatrix} b_{1,k+1} & b_{1,k+2} & \cdots & b_{1,k+n} \\ b_{2,k+1} & b_{2,k+2} & \cdots & b_{2,k+n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{\lceil L/k \rceil,k+1} & b_{\lceil L/k \rceil,k+2} & \cdots & b_{\lceil L/k \rceil,k+n} \end{pmatrix}$$

Step8. Each row and its number of matrix V is the primitive share, and then we get n primitive shares.

Step9. We get n final shares (shadow images) through embed n primitive shares into n images which selected at will, and denote them as $v_1, v_2, \cdots, v_n$.

When the steps above are completed, the original secret image S can be destroyed and n shadow images would be distributed to n different participants at the same time. And when any k participants contribute their shadows, the original secret image can be reconstituted.

The rebuild process of secret image is as follows:

Step1. Construct an empty set, and denote it as S.

Step2. Take primitive share data from k shadow images, these data form k sets: $v'_1, v'_2, \cdots, v'_k$,and the number of which sets are $d'_1, d'_2, \cdots, d'_k$.

Step3. Sort the sets $v'_1, v'_2, \cdots, v'_k$, by set number from small to large, After that, all share data denoted as $v_1, v_2, \cdots, v_k$, while set numbers denoted as $d_1, d_2, \cdots, d_k$.

Step4. Construct a matrix $D'_{k\times k}$. Assign the dith row of generator matrix G to ith row of $D'_{k\times k}$, $1 \le i \le n$; Resolve the inversion of matrix $D'_{k\times k}$,and denoted it as $D_{k\times k}$.

Step5. Take one element from each set $v_1, v_2, \cdots, v_k$, and then sort all of these elements by order and construct a vector $\beta_{k\times 1} = (b_1, b_2, \cdots, b_k)$.

Step6. Matrix $D_{k\times k}$ multiplies by vector β , $\alpha = D \cdot \beta$, the result vector α can be denoted as $\alpha = (a_1, a_2, \cdots, a_k)$.

Step7. Put k elements $(a_1, a_2, \cdots, a_k)$ in vector α in set by order.

Step8. Repeat step 5 to step 7, and until all data have be calculated.

Now the reconstruction process completed, the pixel value of any point (*x,y*) in secret image is equal to $S(x, y)$.

3.Experiments and analysis

In this section, some classic experiments would be illustrated. All images in figure 1 are the original images we used below.

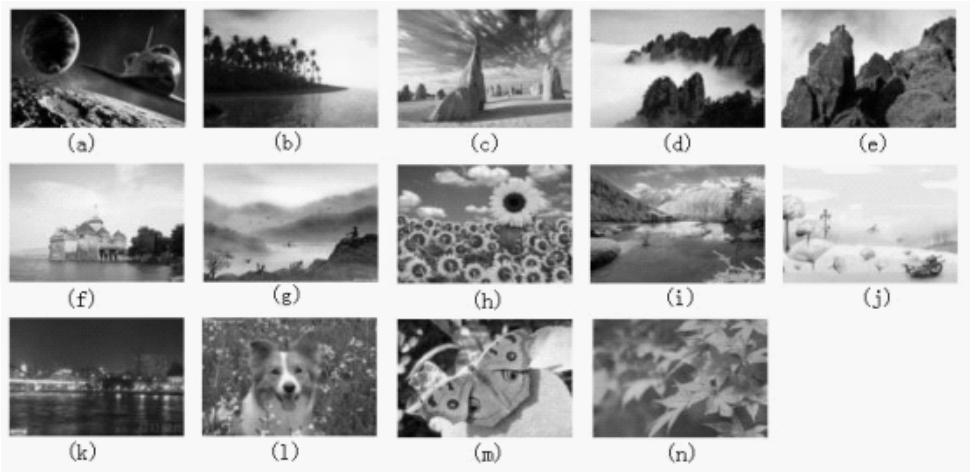

Fig. 1. Original images

Experiment 1, Example of (3, 5) threshold

Suppose image (a) in Figure 1 as the secret image, and use image (b) to image (f) as cover images to hide primitive share data. The effect of calculate results is shown in Figure 2. Image (b) to Image (f) are the final shadow images, and image (a) is the secret image reconstructed by calculation of any three shadow images. We can prove it, image (a) in Figure 2 is the same as image (a) in Figure 1 exactly.

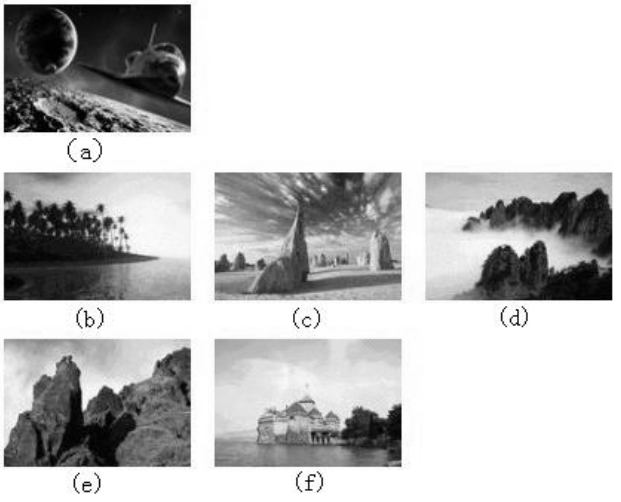

Fig. 2. Secret image sharing of (3, 5) threshold

Experiment 2, Example of (6,8) threshold

Suppose image (a) in Figure 1 as the secret image yet, and use image (h) to image (n) as cover images to hide primitive share data. The effect of calculate results is shown in Figure 3. Image （b） to Image (i) are the final shadow images, and image (a) is the secret image reconstructed by calculation of any three shadow images. We can prove it; image (a) in Figure 3 is the same as image (a) in Figure 1 exactly.

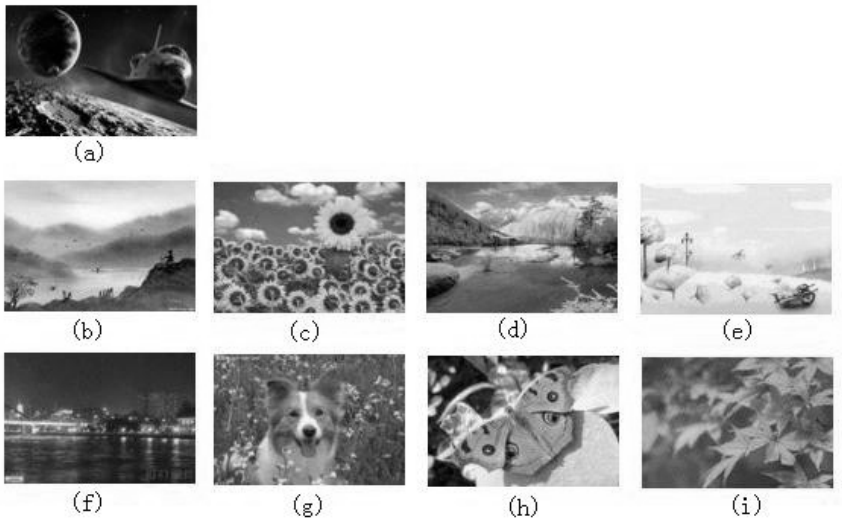

Fig. 3. Secret image sharing of (6, 8) threshold

These are the actual effect of the new scheme. Compared with those schemes based on Lagrange interpolation, the new scheme has all advantages of such schemes [8~12]: arbitrary (*k,n*) threshold setting, $(2 \le k \le n)$; adapt to a variety of common types of image; restore the secret image accurately; Perfect scheme; shadow images are much smaller than the original secret image, it's a good feature to hide share data. The new scheme is more concise, easy to implement; and the most important point is, the complexity of the algorithm reduced greatly: the algorithm complexity of new scheme is about $O(k^2 \cdot L / k) = O(k \cdot L)$, and algorithm complexity of those scheme based on Lagrange interpolation is about $O(k^3 \cdot L / k) = O(k^2 \cdot L)$.

4. Conclusion

The paper proposed a secret image sharing scheme based on RS erasure code. Besides have all advantages of which schemes based on Lagrange interpolation, and the computational complexity of the new scheme is much lower. This is a more practical solution.

Acknowledgements

This paper is supported by Youth Fund of Sichuan Provincial Education Department, No. 10ZB094. The author also wants to extend his thanks and appreciation to Professor WANG Xiao-Jing for his support.

References

[1] Shamir A. How to share a secret[J].Commu.ACM22, 1979, pp:612-613.

[2] Blakley G. Safeguarding cryptographic keys[J].In:Proc.AFIPS1979 National conf., New York, 1979,pp.313-317.

[3] M Naor,A Shamir. Visual cryptography[c].Advances in Cryptology Eurocrypt'94,1994:1-12.

[4] Asmuth C.,Bloom J.. A Modular approach to key safeguarding. IEEE Transactions on Information Theory,1983,29(2):208-210.

[5] Karnin E.D.,Green J.W.,Hellman M.E.. On sharing secret systems.IEEE Transactions on Information Theory,1983,29(1):35-41.

[6] Ito M.,Saito A.,Matsumoto T..Secret sharing scheme realizing general access structure. Proceedings IEEE Grobecom'87,1987:99-102

[7] Benaloh J.,Leichter J..Generalized secret sharing and monotone functions. Advances in Cryptology-CRYPTO'88,1990:27-35.

[8] CC Thien,JC Lin. Secret image sharing[J].Computer&Graphic,2002,26(5):765-770.

[9] Chang-Chou Lin, Wen-Hsiang Tsai. Seeret image sharing with steganography and authentication[J]. The Journal of system and software, 2004(73):405-414.

[10] Li Bai.A Reliable (k,n) Image Secret Sharing Seheme. Dependable, Autonomic and Secure Computing[C]. 2nd IEEE International Symposium on Sept, 2006:31-36.

[11] Thien, Lin. An image-sharing method with user-friendly shadow images. IEEE Transactions on Circuits and Systems for Video Technology, 2003. 1161-1169.

[12] Yu-Shan Wu, Chih-Ching Thien and J.-C.Ja-Chen Lin. Sharing and hiding secret images with size constraint. Pattern Recognition, 2004, 37(7):1377-1385.

[13] Massey, James L. Minimal codewords and secret sharing. Proceedings of the 6th Joint Swedish-Russian InternationalWorkshop on Information Theory,1993.276-279.

[14] Blakley G R, Kabatianski G A. Ideal perfect threshold schemes and MDS codes. Proceedings. 1995 IEEE International Symposium on Information Theory, 1995.488.