A Matrix-Based Secret Sharing Scheme for Images

A. Martín del Rey

GICSIMAD, Department of Applied Mathematics
E.P.S. de Ávila, Universidad de Salamanca
C/ Hornos Caleros 50, 05003-Ávila, Spain
delrey@usal.es

Abstract. In this paper, we propose a novel secret sharing scheme for digital images based on the use of binary matrices. It is shown that the scheme presented is ideal and perfect. Also, it exhibits good statistical properties.

Keywords: Secret sharing. Image processing. Binay matrix.

1 Introduction and Preliminaries

The advent of personal computers and the Internet has made it possible for anyone to distribute worldwide digital information easily and economically. In this new environment, there are several security problems associated with the processing and transmission of digital images over an open network: It is necessary to assure the confidentiality, the integrity and the authenticity of the digital image transmitted. To meet these challenges, a wide variety of cryptographic protocols have appeared in the scientific literature.

Secret sharing schemes are multi-party cryptographic protocols originally related to key establishment. Specifically, they are procedures that allow one to share a secret among a set of participants such that only qualified subsets of these participants (called access structure) can recover the original secret. Moreover, no information about it can be obtained when non-qualified subsets of participants try to recover the secret. The original motivation for secret sharing was to safeguard cryptographic keys from loss. Currently, they have many applications in different areas such as access control, opening a safety deposit box, etc. The basic example of secret sharing schemes is the (m, n) -threshold scheme, where m and n are integer numbers such that $1 \leq m \leq n$. Secret sharing schemes are methods by which a third trusted party (called the dealer) computes n secret shares (or shadows) from an initial secret S and securely distributes them among the n participants. Only subsets of m or more of these participants who pool their shares may easily recover the original secret, but any group knowing only $m - 1$ or fewer shares are unable to recover the secret. Of special interest are $(2, n)$ -threshold schemes.

A secret sharing scheme is said to be perfect if the shares corresponding to each unauthorized subset of participants provide absolutely no information about the

secret S . Moreover, when the sizes of the secret and the shares are equal, the secret sharing scheme is called ideal.

These schemes were introduced independently by Shamir (see Ref. [13]) and Bakley (see Ref. [3]) in 1979 and they are based on the use of Lagrange interpolation polynomial and the intersection of affine hyperplanes, respectively. Since then several proposals have been appeared in the literature based on different mathematical primitives: matrix theory, prime numbers, etc. (see, for example [11]) Those protocols are specially designed for digital data instead of digital images. Due to the main characteristic of digital images (they have a large amount of datum and the difference between two neighboring datum is very small), it is very difficult to apply directly traditional secret sharing schemes to digital images.

The first proposal to share digital images was due to Naor and Shamir (see [10]) and it is called Visual Cryptography. It is based on visual threshold schemes k of n , i.e. the secret image is divided in n shares such that each of them is photocopied in a transparency and then, the original image is recovered by superimposing any k transparencies but no less. In the last years several construction methods based on Visual Cryptography have been proposed (see, for example, [5,6,9,14,17,22]). Besides the Visual Cryptography, another protocols to share digital images have been designed based on vector quantization ([4]), Shamir's ideas ([15,19,21]), Sharing circle ([7,12]), cellular automata ([1,2]), etc.

The main goal of this work is to propose a novel secret sharing scheme based on the use of two binary matrices which satisfy an appropriate algebraic property. Specifically, let A and B two binary matrices such that $A \oplus B = Id$, then the following result holds:

Theorem 1. $A^m \oplus B^m = Id$ if and only if $m = 2^e$, with $e \in \mathbb{Z}^+$.

Proof. A simple computation shows that (the arithmetic is over $\mathbb{Z}_2$):

$$\begin{aligned} Id = (A \oplus B)^m &= A^m \bigoplus_{j=1}^{m-1} \left(\binom{m}{j} A^j \cdot B^{m-j} \right) \oplus B^m \\ &= A^{2^e} \oplus B^{2^e} \bigoplus_{j=1}^{2^e-1} \left(\binom{2^e}{j} A^j \cdot B^{2^e-j} \right) = A^{2^e} \oplus B^{2^e} = A^m \oplus B^m. \end{aligned} \quad (1)$$

To compute the shares one has to multiply the matrices A^m and B^m by some specific binary matrices associated to the original image.

The scheme proposed in this work is a $(2, n)$ secret sharing scheme whose main advantages are the following: There is no data expansion; There is no loss of resolution in the recovered image; It is secure against the most important cryptanalytic attacks; The computational complexity is low since the algorithm involves only bit operations.

The rest of the paper is organized as follows: In section 2 the secret sharing scheme is presented; in section 3, the security analysis of the protocol is shown;

the generalization of the protocol to obtain a different access structure is presented in section 4 and finally, the conclusions and further work are shown in section 5.

2 The Protocol to Share Digital Images

In this section we will describe the $(2, n)$ -threshold scheme to share a secret digital image I among a set of n participant, where n is even: $P_1^1, P_1^2, \dots, P_{n/2}^1, P_{n/2}^2$. Specifically it consists of three phases: The setup and sharing phases, which are carried out by the dealer, and the recovery phase which is carried out by two qualified participants.

The setup phase. Let I be a gray-level digital image defined by $n \times n$ pixels such that p_{ij} stands for the numeric value of the color of the (i, j) -th pixel. Let $J = (p_{ij})$ be the matrix defining the digital image, that is, $J = (p_{ij})$ is the $n \times n$ matrix where $p_{ij} = (q_{ij}^1, q_{ij}^2, \dots, q_{ij}^8) \in \mathbb{Z}_2^8$, with $1 \leq i, j \leq n$. As a consequence eight binary matrices with coefficients in $\mathbb{Z}_2$ are extracted from $J = (q_{ij}^k)$, where $1 \leq i, j \leq N$ and $1 \leq k \leq 8$.

Note that for the sake of simplicity we write $J = J_1 || J_2 || \dots || J_8$. Each of these matrices stands for a B&W image. For example, in Figure 2 are shown the eight binary subimages corresponding to Lena image given in Figure 1

Fig. 1. Lena gray-level image defined by 128×128 pixels

The sharing phase. The dealer chooses two binary matrices which are singular modulo 2, A and B , satisfying the Theorem 1.

The dealer randomly computes the following sequence of integer numbers: $e_1 \leq e_2 \leq \dots \leq e_{n/2}$, such that $m_i = 2^{e_i}$ $1 \leq i \leq n/2$.

The dealer computes $n/2$ shares S_i^1, S_i^2 , with $1 \leq i \leq n/2$, as follows:

$$\begin{aligned} S_i^1 &= A^{m_i} * J = A^{m_i} \cdot J_1 || A^{m_i} \cdot J_2 || \dots || A^{m_i} \cdot J_8, \\ S_i^2 &= B^{m_i} * J = B^{m_i} \cdot J_1 || B^{m_i} \cdot J_2 || \dots || B^{m_i} \cdot J_8. \end{aligned} \quad (2)$$

where the product of matrices is given modulo 2.

The recovery phase. To recover the original image the users P_i^1 and P_i^2 pool their shares, S_i^1, S_i^2 , and computes the following: $C_j = (A^{m_i} \cdot J_j) \oplus (B^{m_i} \cdot J_j)$, $1 \leq j \leq 8$. Then, the original image is: $J = C_1 || C_2 || \dots || C_8$.

Fig. 2. (a) Subimage J_1 ; (b) Subimage J_2 ; (c) Subimage J_3 ; (d) Subimage J_4 ; (e) Subimage J_5 ; (f) Subimage J_6 ; (g) Subimage J_7 ; (h) Subimage J_8

3 The Security Analysis

3.1 Main Properties of the Protocol

The secret sharing scheme proposed in this work is perfect since it involves singular matrices. Consequently, from one share of the form S_i^1 or S_i^2 , it is impossible to determine the initial image J . Moreover, this scheme can be also considered as ideal the size of the shares is exactly the same than the size of the secret to be shared. Moreover, since the images are considered as matrices of the same dimensions, no loss of resolution is presented in the recovered image.

3.2 Statistical Analysis

We have performed a statistical analysis in order to prove the confusion and diffusion properties of the proposed protocol, which allows it to strongly resist statistical attacks. Specifically the histograms of original image and the shares are checked and the correlation coefficients are computed.

Let us consider the 256 gray-scale image of size 128×128 given in Figure 3-(a). Its histogram is shown in Figure 3-(b).

The shared images computed with the parameters: $e_1 = 1, e_2 = 2, e_3 = 3$ are shown in Figure 4, whereas their corresponding histograms are shown in Figure 5.

Fig. 3. (a) Peppers picture defined by 128×128 pixels and 256 gray-levels; (b) Histogram of Peppers image

Fig. 4. (a) Share 1 computed for $e_1 = 1$ and A ; (b) Share 2 computed for $e_2 = 2$ and A ; (c) Share 3 computed for $e_3 = 3$ and A ; (d) Share 4 computed for $e_1 = 1$ and B ; (e) Share 5 computed for $e_2 = 2$ and B ; (f) Share 6 computed for $e_3 = 3$ and B

Fig. 5. (a) Histogram of Share 1; (b) Histogram of Share 2; (c) Histogram of Share 3; (d) Histogram of Share 4; (e) Histogram of Share 5; (f) Histogram of Share 6

From the figures one can see that the histograms of the shares are fairly uniform and they are significantly different from that of the original image. It demonstrates that the secret sharing algorithm has covered up all the characters of the original image and shows good performance of balanced 0-1 ratio and zero correlation.

The following procedure will be carried out to test the correlation between two adjacent pixels in the original and the shared images: First of all randomly select 1.000 pairs of two adjacent pixels from the image, and then, calculate the correlation coefficient of each pair by using the following formula:

$$r_{xy} = \text{cov}(x, y) / \left(\sqrt{D(x)} \sqrt{D(y)} \right), \quad (3)$$

where x and y are the grey-scale values of the two adjacent pixels in the image and:

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x)) (y_i - E(y)), \quad (4)$$

Table 1. Correlation coefficients of two adjacent pixels

	Horizontal	Vertical	Diagonal
Peppers image	0.9377	0.9812	0.9090
Share 1	-0.0159	-0.0564	-0.0659
Share 2	0.0723	-0.0052	-0.0407
Share 3	-0.0095	-0.0235	0.0583
Share 4	0.0009	-0.0720	-0.0583
Share 5	-0.0159	-0.0044	0.0023
Share 6	0.0526	0.0084	-0.0166

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i, \quad D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2. \quad (5)$$

As a consequence, the results obtained are shown in Table 1.

The correlations coefficients of the original image and shared images are far appart (note that the correlation coefficients of Peppers' picture are close to 1, whereas the corresponding coefficients of the shared images are very close to 0). Consequently, the secret sharing algorithm satisfies zero co-correlation.

3.3 Computational Complexity

The number of bit operations involving the sharing phase and the recovery phase are different. Specifically, the following results hold: In the sharing phase, the number of bit operations necessary to compute only one share is $4 \cdot (2N^3 - N^2)$. Moreover, to compute all shares $4n \cdot (2N^3 - N^2)$ bit operations are necessary. Note that as A and B are random matrices the half of coefficients are zero. In the recovery phase, to get the secret image I , a qualified pair of users has to perform a XOR operation between eigh pairs of binary matrices. Consequently, to recover the orignal image $8 \cdot N^2$ bit operations are necessary. Note that the recovery phase is faster than the sharing phase, and it is an important and desirable feature of such protocols.

4 Generalization of the Protocol

As is stated in the protocol introduced above, only specific pairs of participants: those of the form $\{P_i^1, P_i^2\}$, $1 \leq i \leq n/2$, can recover the secret image by pooling their shares. As a consequence there exist only $n/2$ qualified subsets of participants. Nevertheless, this protocol can be easily generalized to obtain an access structure with $(n/2)^2$ qualified subsets: $\{P_i^1, P_j^2\}$, $1 \leq i \leq n/2, 1 \leq j \leq n/2$, as follows: The setup phase is exactly the same than in the first proposal. In the sharing phase, the dealer distributes the following data among the participants: $P_i^1 \leftrightarrow \{S_i^1, m_i = 2^{e_i}\}$, $P_i^2 \leftrightarrow \{S_i^2, m_i = 2^{e_i}\}$, $1 \leq i \leq n/2$. Finally, in the recovery phase the participants P_i^1, P_j^2 recover the secret image I as follows:

- They compare the integer numbers m_i and m_j .
- If $m_i < m_j$, then P_i^1 computes $A^{m_i+m_j-m_i} * J = A^{m_j} * J$. On the other hand, if $m_j < m_i$, then P_j^2 computes $B^{m_j+m_i-m_j} * J = B^{m_i} * J$.

- The secret is obtained by simply applying the Recovery Phase to these new shares.

Note that this modification of the protocol allows one to obtain an access structure given by two disjoint subsets, $A_1 = \{P_i^1, 1 \leq i \leq n/2\}$, $A_2 = \{P_j^2, 1 \leq j \leq n/2\}$, such that to recover the secret it is necessary that two participants (one from A_1 and other from A_2) pool their shares.

5 Conclusions

In this work a novel $(2, n)$ -secret sharing scheme for digital images has been presented. It is based on the use of two binary singular matrices A and B such that $A \oplus B = Id$. The protocol consists of three phases: The setup phase where the matrices are determined; The sharing phase where the shares are computed to obtain the shares; and the recovery phase where the original image is computed by means of XOR operations.

Its main features are the following: There is neither data expansion nor loss of resolution; It is a perfect scheme since it involves singular matrices. Moreover, the shares exhibits good statistical properties; The computational complexity is low.

Further work is aimed at designing an $(2, n)$ -threshold scheme with a more general access structure and a secret sharing (m, n) -scheme, with $m > 2$.

Acknowledgements

This work has been partially supported by the Consejería de Educación (Junta de Castilla y León, Spain) under grant SA110A06.

References

1. Álvarez, G., Hernández, L., Martín, A.: A New Secret Sharing Scheme for Images based on Additive 2-Dimensional Cellular Automata. In: Marques, J.S., Pérez de la Blanca, N., Pina, P. (eds.) IbPRIA 2005. LNCS, vol. 3522, pp. 411–418. Springer, Heidelberg (2005)
2. Alvarez, G., Hernández Encinas, A., Hernández Encinas, L., Martín del Rey, A.: A secure scheme to share secret color images. *Comput. Phys. Comm.* 173, 9–16 (2005)
3. Blakley, G.R.: Safeguarding cryptographic keys. In: *AFIPS Conf. Proc.*, vol. 48, pp. 313–317 (1979)
4. Chang, C., Hwang, R.: Sharing secret images using shadow codebooks. *Inform. Sciences* 111, 335–345 (1998)
5. Chen, Y., Chan, Y., Huang, C., Tsai, M., Chu, Y.: A multiple-level visual secret-sharing scheme without image size expansion. *Inform. Sciences* 177, 4696–4710 (2007)
6. Cimato, S., De Prisco, R., De Santis, A.: Colored visual cryptography without color darkening. *Theor. Comput. Sci.* 374, 261–276 (2007)

7. Feng, J., Wu, H., Tsai, C., Chu, Y.: A new multi-secret image sharing scheme using Lagrange's interpolation. *J. Syst. Software* 76, 327–329 (2005)
8. Fredkin, E.: Digital mechanics. An informal process based on reversible universal cellular automata. *Physica D* 45, 254–270 (1990)
9. Lin, S., Lin, J.: VCPSS: A two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches. *Pattern Recogn.* 40, 3652–3666 (2007)
10. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) *EUROCRYPT* 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995)
11. Menezes, A., van Oorschot, P., Vanstone, S.: *Handbook of Applied Cryptography*. CRC Press, Boca Raton (1997)
12. De Santis, A., Masucci, B.: New results on non-perfect sharing of multiple secrets. *J. Syst. Software* 80, 216–223 (2007)
13. Shamir, A.: How to share a secret. *Commun. ACM* 22, 612–613 (1979)
14. Shyu, S.: Efficient visual secret sharing scheme for color images. *Pattern Recogn.* 39, 866–880 (2006)
15. Thien, C., Lin, J.: Secret image sharing. *Comput. Graph.* 26, 765–770 (2002)
16. Toffoli, T., Margolus, N.: *Cellular automata machines*. The MIT Press, Cambridge (1987)
17. Tsai, D., Chen, T., Horng, G.: A cheating prevention scheme for binary visual cryptography with homogeneous secret images. *Pattern Recogn.* 40, 2356–2366 (2007)
18. von Neumann, J.: *Theory of self-reproducing automata*. Burks, A.W. (ed.). University of Illinois Press, Illinois, 1966.
19. Wang, R., Su, C.: Secret image sharing with smaller shadow images. *Pattern Recogn. Lett.* 27, 551–555 (2006)
20. Wolfram, S.: *A new kind of science*. Wolfram Media, Champaign, Illinois (2002)
21. Wu, Y., Thien, L., Lin, J.: Sharing and hiding secret images with size constrain. *Pattern Recogn.* 37, 1377–1385 (2004)
22. Yang, C., Chen, T.: Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation. *Pattern Recogn.* 39, 1300–1314 (2006)