# Secret Multimedia Information Sharing with Data Hiding Capacity by Simple Logic Operations

Chang-Chou Lin and Wen-Hsiang Tsai*

Department of Computer and Information Science, National Chiao Tung University

Hsinchu, Taiwan 300, Republic of China

## Abstract

An effective scheme for secret multimedia information sharing with data hiding capacity is proposed. A set of secret data is shared into an arbitrary number of sets of pre-designed camouflage data and a corresponding set of meaningless data. Utilizing the characteristic of visualization, we can employ the scheme to share, e.g., a landscape image into several portraits and a meaningless image. The scheme can as well be applied to other multimedia data, like voice, video, and so on. So we can share a paragraph of words into several pleasant melodies and share a section of a cartoon movie into several sections of science-fiction movies. When a set of secret data is shared, the effect of data hiding is achieved in the mean time from another point of view because the shares can be other meaningful camouflage data sets. For cases of small numbers of shares, a revised version of the scheme is proposed to improve the data hiding effect. An advantage of the proposed scheme is that only simple logic operations are used in creating the shares and recovering the secret data. Simple logic operations inherit the properties of fast computation and easy implementation, which make the scheme more practical for real applications. Security is also ensured. The secret key is distributed instead of being centralized. If not all shares are collected, no information about the original secret data can be gained.

* To whom all correspondences should be sent.

**Keywords:** information sharing, data hiding, secret data, camouflage data, logic operations.

## 1. Introduction

Due to fast growth of Internet applications, digitized information becomes more and more popular. Because of the ease of copying and tampering digital data, importance of information security reveals in the mean time. Differing from traditional schemes, some properties of multimedia data can be used in cryptology. Visualization is the most practical characteristic. Data hiding and watermarking techniques [1-4] use this characteristic to achieve security. They embed secret

information in a camouflage image imperceptibly to avoid attacks from invaders. Many tricks are applied to make the change of the original image invisible. This kind of scheme can be regarded as the first layer of security. Besides, it has been studied in cryptography [5-7] for a long time to share secret information. But it is restricted in the format of pure bit stream. Recently, visual secret sharing has been proposed. But some problems still remain. Loss of contrast and expansion of image size are the most critical issues.

In this paper, we propose a secret sharing scheme that utilizes the characteristics of multimedia data to securely share multimedia information, achieving the effect of data hiding in the mean time. The encryption and decryption processes of this scheme are simple. Only a logic operation, namely exclusive-OR (XOR), is used. For example, if we want to share a secret image into $n$ shares, we can assign any $n$-1 shares desired meaningful images and apply the proposed scheme to obtain the remaining share (the last share) a corresponding meaningless image. The value of each pixel in the last share is the XOR result of the values of the corresponding pixels of the other $n$-1 shares and the original image. Applying XOR to corresponding pixels of all shares results in the corresponding pixel of the original image. Insufficient copies of shares will gain no secret. Consequently, security is guaranteed. An advantage of this scheme is that it can be implemented with cheap and simple circuitry. This increases its practicality. Compared with existing techniques, the proposed method offer good effect.

The remainder of this paper is organized as follows. In Section 2, we introduce the process of encryption. In Section 3, the method of decryption is described. The scheme need be improved when the number of decomposed shares is small. So we propose a revised version in Section 4. Some experimental results are shown in Section 5. For ease of demonstration, we use image data as examples. But our scheme is actually general for any other bit-stream type of multimedia. Finally, some conclusions are given in Section 6.

## 2. The process of encryption

In the proposed scheme, the operation used in the process of encryption is XOR. Let symbol $\oplus$ represent XOR. The function of XOR for two binary numbers is as follows:

$$1 \oplus 1 = 0; \qquad 1 \oplus 0 = 1;$$
$$0 \oplus 0 = 0; \qquad 0 \oplus 1 = 1. \tag{1}$$

When a certain operand is 1, the XOR result may be 0 or 1. It is also true if a certain operand is 0. This means that invaders cannot find out the result if they know only one operand. If we want to encrypt the original data into two shares, we may decompose the original data bit by bit. We use an example for demonstration. Assume that the original data is 01. We choose 11 as the camouflage data. Then we compute the other share by Eqs. (1) with one operand coming from the camouflage data and the other operand from the original data. The result is 10. When the share 11 (the camouflage) is stolen, four combinations (00, 01, 10, 11) are possible as

solutions for lack of the other share. This phenomenon holds if the stolen share is 10.

Extending to the general case, we can express the function of XOR as follows:

$$b_{ni} = b_{1i} \oplus b_{2i} \oplus b_{3i} \oplus \cdots \oplus b_{n-1i} \oplus O_i \quad (2)$$

where $b_{ji}$ represents the $i$th bit of the $j$th share, $O_i$ represents the $i$th bit of the original data, and $b_{ni}$ is the corresponding last share. When an invader gets arbitrary $n$-1 shares, the remaining unknown share hides the solution. When he gets arbitrary $n$-2 shares, the remaining two unknown shares may have four combinations. The XOR of four combinations forms two solutions 0 and 1, which is equal to an unknown share. So they hide the result as well. By induction, we can prove that the XOR of any number of shares can be treated as a new share. Therefore, any number of unknown shares can hide the original data. We cannot get any information about the original data unless we get all shares. Besides security by way of encryption, our scheme allows one to use desired data as shares. So we may use some unrelated data as shares to achieve the goal of hiding data. In this way, our scheme can protect the original data more effectively.

## 3. The method of decryption

Decryption in our scheme is easy. When all shares are collected, the XOR of corresponding bits in all shares decrypts the secret. The expression of the operation is

$$O_i = b_{1i} \oplus b_{2i} \oplus b_{3i} \oplus \cdots \oplus b_{ni}. \quad (3)$$

That is, we apply XOR to all $b_{ji}$ values and take the result as the original secret data. Why the original data $O_i$ can be computed from XORing all $b_{ji}$ is proved as follows. Substituting $b_{ni}$ of (2) into the term $b_{1i} \oplus b_{2i} \oplus b_{3i} \oplus \cdots \oplus b_{ni}$, we get

$$\begin{aligned}
&b_{1i} \oplus b_{2i} \oplus b_{3i} \oplus \cdots \oplus b_{ni} \\
&= b_{1i} \oplus b_{2i} \oplus b_{3i} \oplus \cdots \oplus (b_{1i} \oplus b_{2i} \oplus b_{3i} \oplus \cdots \oplus b_{n-1i} \oplus O_i) \\
&= (b_{1i} \oplus b_{1i}) \oplus (b_{2i} \oplus b_{2i}) \oplus \cdots \oplus (b_{n-1i} \oplus b_{n-1i}) \oplus O_i \\
&\text{(By the commutative law and associative law of } \oplus) \\
&= 0 \oplus 0 \oplus \cdots \oplus 0 \oplus O_i \\
&\text{(By the facts } 0 \oplus 0 = 0 \text{ and } 1 \oplus 1 = 0) \\
&= O_i \quad \text{(By the facts } 0 \oplus \text{b} = \text{b where b} = 0 \text{ or } 1)
\end{aligned}$$

Our scheme possesses a high degree of security. First, we distribute secret information to several shares without centralizing it. Second, the length of each share (key length) is equal to the secret itself. It is difficult for invaders to use a brute-force way to solve it. Also, the secret is allowed to be any form of multimedia. For example, the secret may be an image of a house. If invaders use brute force to guess all possible pixel values, they may get an image of a jet or any other image. They cannot decide which meaningful image is the secret image. Extending to other types of multimedia, this characteristic holds as well. Finally, invaders might even be unaware of any secret behind it because of the effect of data hiding.

## 4. A revised version of proposed scheme

The scheme need be improved when the number of shares is few. When there are smooth areas in the chosen shares, the corresponding

share may leak out part of the secret to observers. We use an extreme example where the number of composed shares is two to demonstrate this phenomenon. By Eqs. (1), if we choose a share with an area of bit value 0, the bit value of the corresponding share will be the same as the bit value of the secret data in this area. An example of gray-level images is depicted in Figure 1. We can observe that *share*2 (the corresponding share) reveals the secret information in the smooth area of *share*1.

(a)

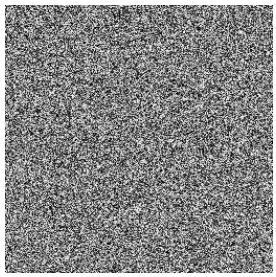
(b)

(c)

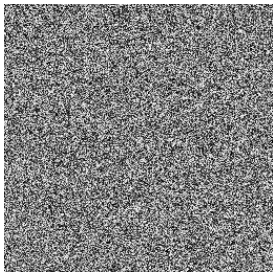
Fig. 1: (a) The *share*1. (b) The *share*2. (c) The original image.

But with an increase of the number of shares, overlapping of shares destroys the smooth area. Therefore, we can get a more random and so meaningless corresponding share. Nonetheless, we introduce a *noise share* to solve this problem when the number of shares is few. For gray-level images, we design a noise share as one composed of pixel values randomly chosen. The reason to randomly choose the gray values is to create a confusing pattern. An example of a noise share is shown in Figure 2. We observe that the secret leaking phenomenon is effectively removed.

(a)



(b)



(c)

(d)

Fig. 2: (a) The *share*1. (b) The *share*2 (*noise share*). (c) The *share*3 (corresponding share). (d) The original image.

## 5. Experimental results

In this section, more experimental results are shown to prove the feasibility of the proposed scheme. For ease of demonstration, we use image data to evaluate our scheme. But it is intuitive and easy to apply our scheme to other types of media because our method handles bit streams essentially. First, we evaluate the effect of our scheme when the number of decomposed shares is five. The result is depicted in Figure 3. The corresponding share is close to a meaningless one. It is hard to discover the original image from it. With the

increase of the number of decomposed shares, the corresponding share randomizes more clearly. Figure 4 is an example with the number of decomposed shares being nine. The original image is “peppers”. We can see that the number of block areas in Figure 4(a) is smaller than in Figure 3(e). Finally, we use another combination of shares to evaluate the effect of *noise share*. The result is shown in Figure 5. It is satisfactory.

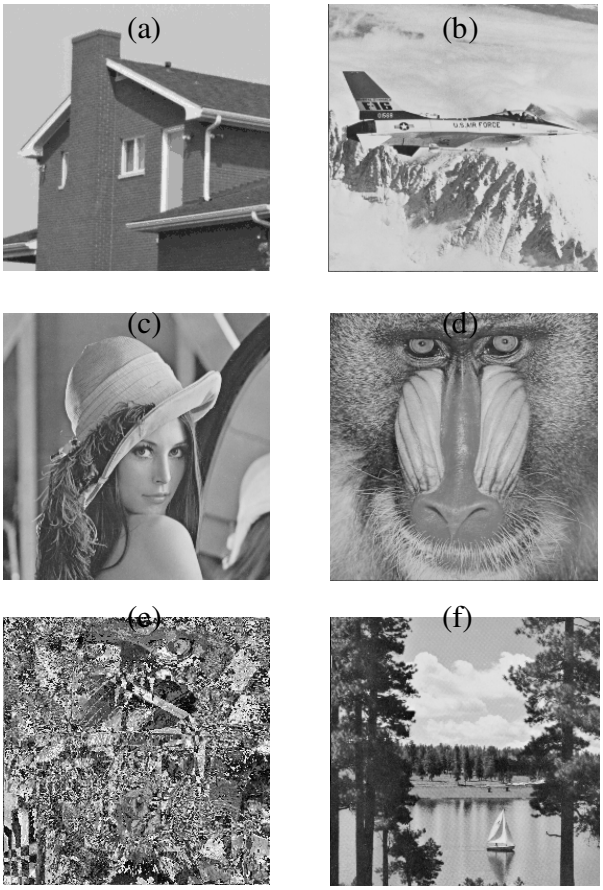
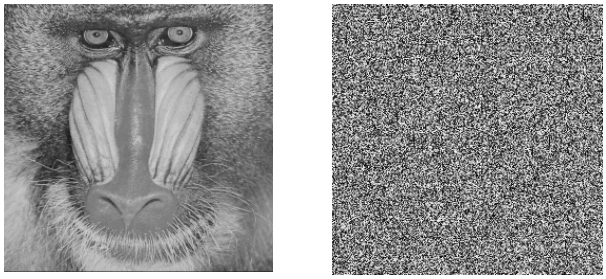


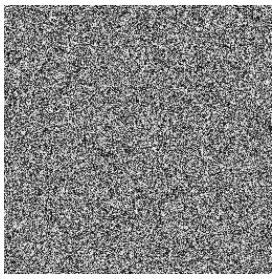

Fig. 3: (a) The *share*1. (b) The *share*2. (c) The *share*3. (d) The *share*4. (e) The *share*5 (corresponding share). (f) The original image

(a) (b)

Fig. 4: (a) The corresponding share. (b) The original image.



(a) (b)




(c) (d)

Fig. 5: (a) The *share*1. (b) The *share*2 (*noise share*). (c) The *share*3 (corresponding share). (d) The original image.

## 6. Conclusions

In this study, we have developed a scheme with the capacities of sharing information and hiding data as well. The scheme is useful for dealing with multimedia and any other bit-stream data. The proposed approach is based on the idea of decomposing all bits of the secret data by the XOR operation. This scheme possesses the advantage of high degree of security because it distributes the secret to all shares and is hard to decrypt by brute-force methods. Besides, invaders might even be unaware of something different behind the shares because the technique of data hiding is adopted. But the image quality yielded by our scheme is superior to traditional data hiding schemes. The quality of our camouflage image is lossless. However, secret lacking will occur when there is a great amount of smooth areas in the pre-designed shares. The number of decomposed shares must be large enough to randomize this phenomenon. For the case of only a few decomposed shares, we have proposed a revised scheme to solve the problem. We introduce a noise share to aid randomization of smooth areas. Some experiments are used to evaluate the effect of the proposed method. Good results prove the feasibility of our approach. Our scheme also inherits the properties of fast computation and easy implement. It can be implemented by simple electrical circuitry, which can be used both in encryption and in decryption. These properties are important for mobile equipments like the PDA which are small without powerful computation capacity.

## 7. References


[1] W. Bender, D. Gruhl, N. Morimoto, and A. Liu, "Techniques for Data Hiding," *IBM System Journal*, vol. 35, nos. 3&4, pp. 313-336, 1996.

[2] A. Tewfik, M. Swanson, "Data Hiding for Multimedia personalization, Interaction, and Protection," *IEEE Signal Processing Magazine*, vol. 14, no. 4, July 1997.

[3] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, December 1997.

[4] M. Swanson, M. Kobayashi, A. Tewfik, "Multimedia Data-embedding and Watermarking Technologies," *Proceeding of the IEEE*, vol. 86, no. 6, pp. 1064-1087, June 1998.

[5] A. Shamir, "How to Share a Secret," *Commun. Assoc. Comput. Mach.*,vol. 22, pp.612-613, 1979.

[6] M. Naor, A. Wool, "Access Control and Signatures via quorum secret sharing," *IEEE Transactions on Parallel and Distributed*

*System*, vol. 9, no. 9, September 1998.

[7] A. Beimel, B. Chor, "Secret Sharing with Public Reconstruction," *IEEE Transactions on Information Theory*, vol. 44, no. 5, September 1998.