A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme

Chao-Wen Chan† and Yi-Da Wu†,

† Dept. of Computer Science and Information Technology, National Taichung Institute of Technology, Taiwan, R.O.C.

Summary
This paper presents a new visual cryptography scheme for secure digital transmission. Visual cryptography can be seen as a one-time pad system. Then, it cannot be reused. In this paper, we apply Diffie and Hellman (D-H) key agreement method and toral automorphism (TA) such that visual cryptography can be reused. Both secret and symmetry-key are represented in binary image. The proposed scheme is simple and easy to be implemented for shadow images. Therefore, it can be used in many electronic business applications.

Key words:
Visual cryptography, secret sharing, toral automorphism, key agreement

1. Introduction

In recent years, there has been a rapid growth of information technology for human to communication on the Internet. Since Internet is public, any one can easily read information and perform successful transmissions without protection. In order to avoid sensitive information being illegally read or modified, the information must be encrypted before transmission. The observations from recent electronic business applications on the Internet, point out that the amount of exchanged data is small, but the exchanged data requires secrecy.

In 1995, Naor and Shamir proposed a visual secret sharing scheme. The scheme provides secrecy to avoid being illegally read or modified, it is called visual cryptography [4]. Visual cryptography is a clever and simple scheme that partitions a secret image into a set of shadow images, and a dealer distributes those shadow images to participants. The scheme uses the human visual system to recover secret images by stacking several shadow images. Several studies have improved the quality of images [6] and visual format such as gray-level images [10] or color images [2].

Visual cryptography can be seen as a one-time pad system. We consider that the secret image S is partitioned into two shadow images $S1$ and $S2$ for each participant Alice and Bob, respectively. While S is recovered by stacking $S1$ and $S2$, Alice remembers $S2$, and Bob remembers $S1$. To encrypt twice, we assume that $S1$ is fixed, and a new secret image S' is partitioned into two shadow images $S1$ and $S3$ for Alice and Bob, respectively. Because Bob has the ability to infer $S1$, he can recover S' without communicating with Alice; therefore, we define it as a reusable problem in visual cryptography if one of the shadow images is the same as a previous one. However, there is very limited study on reusable visual cryptography.

In 1976, Diffie and Hellman (D-H) proposed a key agreement scheme that two parties can agree on a common session key. In this paper, we apply Diffie and Hellman (D-H) key agreement method [9] and toral automorphism (TA) [3] to improve the reusable problem. In [1], Chang et al. showed a scheme to permute coordinates of the image by using toral automorphism [3] to protect the image. According to the concept of Chang et al.'s scheme, we generate a common image without revealing the shadow images. The main idea of our method is that a D-H key agreement scheme is used to compute a common image for encryption and decryption with two parties. We suppose that the two parties are sender Alice and receiver Bob. The two parties select a common shadow image, and they can generate a common image from a common session key with the toral automorphism algorithm. The common image is computed from a D-H key agreement scheme, thus, it is random and independent. Alice computes an encrypted image from the common image and the secret image, and she sends the encrypted image to Bob. Bob can recover the secret image from the encrypted image and the common image. An attacker would have a hard time discovering the secret image and the common session key, even if he obtains the encrypted image.

The rest of this paper is organized as follows. In Section 2, we give a brief review of the D-H key agreement scheme, visual cryptography and toral automorphism algorithm. In Section 3, we present our proposed scheme. Experimental results with the proposed scheme are presented in Section 4. The security analysis is given in Section 5. Finally, some conclusions are given in Section 6.

Manuscript received April 5, 2008
Manuscript revised April 20, 2008

2. Preliminaries

Before a new a visual information encryption scheme is proposed, we first introduce the properties of D-H key agreement scheme, visual cryptography and toral automorphism that will allow us to discuss our scheme's security in Section 4.

2.1 Diffie-Hellman (D-H) Key Agreement

The famous key agreement scheme was proposed by Diffie and Hellman in 1976. If Alice and Bob want to transfer a secret by Diffie-Hellman key agreement scheme, then Alice selects a random secret α and sends $g^{\alpha} \pmod N$ to Bob, where N is a large prime number. Then, Bob selects another random secret β and sends $g^{\beta} \pmod N$ to Alice. Finally, Alice and Bob compute a common session key $K = g^{\alpha\beta} = g^{\beta\alpha} \bmod N$. Thus, Alice and Bob can use the common key K for encryption and decryption in the session. No one can derive the session key K from the public information $g^{\alpha} \pmod N$ and $g^{\beta} \pmod N$. The Security is based on the computational Diffie-Hellman problem.

2.2 Visual Cryptography (VC)

VC is a secret sharing scheme for digital images which uses the human visual system to recover secrets; therefore, it has low computation. A (k, n)-threshold VC scheme is defined as a dealer who partitions a secret image into n shadow images, and the dealer distributes one of those shadow images for each participant. Each participant obtains a distinct shadow image. In order to recover the secret information, any k or more participants can reconstruct the secret image by stacking any k or more shadow images, but the secret image can not be reconstructed by less than k shadow images. For example: when $k = n = 2$, we can partition an $N \times M$ secret image into two $2N \times 2M$ shadow images. Formally, we can represent the encrypt/decrypt function as shown in following formula (1) and (2), where S denotes the secret image, and (S_1, S_2) denotes the shadow images.

$$(S_1, S_2) = \text{Partition}^{N \times M}(S) \quad (1)$$

$$S = \text{Recover}^{N \times M}(S_1, S_2) \quad (2)$$

2.3 Toral Automorphism (TA)

TA is a two-dimensional matrix that permutes a set of coordinates [1]. It can be used to generate a chaotic arrangement of digital images. Voyatzis and Pitas [3] defined a two-dimensional matrix as shown in formula 3.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod N \quad (3)$$

Here (x', y') is a new position for a two-dimensional coordinate after randomly selecting its permutation, $N \times N$ is denoted as the image size, and k is denoted as the secret key of TA matrix M. For instance, we assume that the secret image size is 2×2 pixels, and k is 3. The TA matrix is shown in Table 1 (a). The pixel value of the image is shown in Table 1 (b).

Table 1: (a) TA matrix, (b) Pixel value of image before using TA, (c) Pixel value of image after using TA

$$\begin{pmatrix} 1 & 1 \\ 3 & 3+1 \end{pmatrix} \quad \begin{matrix} p_1 & p_2 \\ p_3 & p_4 \end{matrix} \quad \begin{matrix} p_1 & p_4 \\ p_2 & p_3 \end{matrix}$$

(a) (b) (c)

For example, the pixel value of the image is p_3 at location (1, 2) before using TA. The location (1, 2) moves to location (2, 2) after using TA.

3. The Proposed Scheme

Before introducing our proposed scheme, we present the notations firstly. The notations are listed in below Table 2.

Table 2: The notations are used in the proposed scheme

N	N is a large prime integer such that discrete logarithm problem in Z_N is hard.
g	g is a public primitive integer in modular N, where g is not equal to 1.
k	k is a secret integer appearing in the shadow image chosen by both Alice and Bob.
α	α denotes a secret integer randomly selected by Alice.
β	β denotes a secret integer randomly selected by Bob.
$I, I(x, y)$	I denotes a common image decided by two parties, and *I(x, y)* denotes the pixel value of the image *I* at location *(x, y)*.
M_k	M_k denotes the two-dimensional TA matrix, where M_k equals $\begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix}$.
$I_{k,n}$	$I_{k,n}$ denotes an image *I* permutated *n* times by TA, where k is the secret key of TA matrix.
$\pi^n_{M_k}(.)$	$\pi^n_{M_k}(.)$ denotes an image permutation function derived from n and M_k, and its permuted coordinates of the image n times with the TA algorithm. Where $I_{k,n} = \pi^1_{M_k}(I_{k,n-1}) = \pi^2_{M_k}(I_{k,n-2}) = \ldots = \pi^{n-1}_{M_k}(I_{k,1}) = \pi^n_{M_k}(I)$, $I_{k,1}(x', y') = I(x, y)$, and $\begin{pmatrix} x' \\ y' \end{pmatrix} = M_k \begin{pmatrix} x \\ y \end{pmatrix} \pmod N$ for all (x, y).

The proposed scheme consists of initialization phase, session key generation phase, encryption phase, and decryption phase. The details of these phases will be described as follows.

3.1 Initialization Phase

Alice and Bob agree on a $2N \times 2N$ common image *I* and a secret integer *k*, where *I* includes $N \times N$ blocks. Each block consists of 2 × 2 pixels arranged in a random position, then all pixels of the corresponding block are two black and two white.

3.2 Session Key Generation Phase

The session key generation phase is based on the D-H key agreement scheme [9]:

(1) Alice selects a random integer α and sends $g^\alpha \pmod N$ to Bob.

(2) Bob selects a random integer β and sends $g^\beta \pmod N$ to Alice.

(3) Alice computes $k = g^{\beta\alpha} \equiv (g^\beta)^\alpha \pmod N$.

(4) Bob computes $k = g^{\alpha\beta} \equiv (g^\alpha)^\beta \pmod N$.

After performing the above steps, Alice and Bob can obtain a common session key $g^{\beta\alpha}$ or $g^{\alpha\beta}$. That is

$$k = g^{\beta\alpha} \equiv (g^\beta)^\alpha \equiv (g^\alpha)^\beta \equiv g^{\alpha\beta} \pmod N \quad (4)$$

Alice and Bob keep the common session key *k* for later encryption and decryption.

3.3 Encryption Phase

The encryption phase is based on VC. Given a secret image, a (2, 2)-threshold VC can be partitioned it into two shadow images. If one shadow image is randomly selected, the other shadow image is determined uniquely. Suppose that Alice wants to send a secret, say *S*, to Bob. Then, Alice computes a common shadow image $S_1 = I_{k,g^{\beta\alpha}} = \pi^{g^{\beta\alpha}}_{M_k}(I)$. The common shadow image S_1 is computed by a computer. According to the (2, 2)-threshold VC, the other shadow image S_2 can be computed by *S* and the common shadow image S_1 as shown in the following formula:

$$S_2 = E^{\mathrm{VC}(2,2)}_{S_1}(S) = E^{\mathrm{VC}(2,2)}_{I_{k,g^{\alpha\beta}}}(S) \quad (5)$$

such that (S_1, S_2) = Partition $^{N \times N}$ (*S*) and S_1 equals $I_{k,g^{\alpha\beta}}$ or $I_{k,g^{\beta\alpha}}$. S_2 can be inferred from *S* and S_1. In formula 5, the shadow image S_2 is also computed by a computer. Alice sends S_2 to Bob.

3.4 Decryption Phase

When Bob receives the shadow image S_2, he can recover the secret image by stacking S_1 and S_2, where $S_1 = I_{k,g^{\alpha\beta}} = \pi_{M_k}^{g^{\alpha\beta}}(I)$. The decryption phase can be shown in the following formula (6):

$$S = D_{S_1}^{\mathrm{VC}}(S_2) = D_{I_{k,g^{\alpha\beta}}}^{\mathrm{VC}}(S_2) \tag{6}$$

such that S = Recover $^{N \times N}$ (S_1, S_2).

4. Experimental Results

This section, we will present the experimental results of our scheme. One of the experimental results is shown in Fig. 1. We tested a number of 100 × 100 pixel images. The secret image expands to 200 × 200 shadow images. To simply encrypt the secret image, we assume that all the keys (α, β, and k) and a public primitive integer g are chosen randomly. In initialization phase, Alice and Bob agree on a common image I and a secret integer k. In session key generation phase, Alice selects a random integer α, and Bob selects a random integer β. Two parties exchange an agreement key with each other and then establish a common shadow image $I_{k,g^{\beta\alpha}} = \pi_{M_k}^{g^{\beta\alpha}}(I)$ as shown in Fig. 1 (b). In Fig. 1 (c) we illustrate the corresponding shadow image, which is created by a secret image and a common shadow image. Fig. 1 (d) shows that the decrypted image's message can be recovered by stacking two shadow images. In the same way, we also tested English and Chinese as shown in Fig. 2 and Fig. 3, respectively.

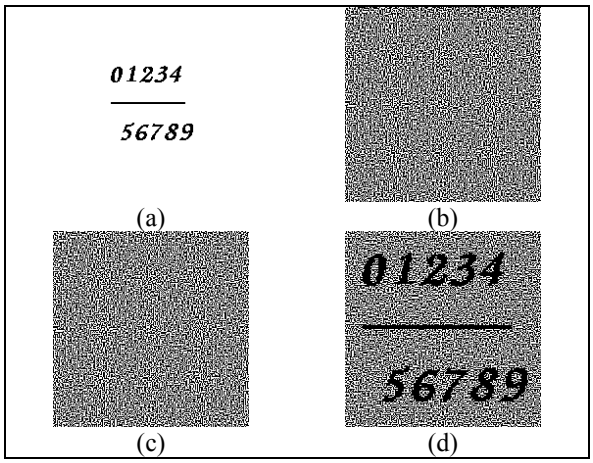

Fig. 1. Number image: (a) Secret image, (b) Common shadow image, (c) Corresponding shadow image , (d) Decrypted image

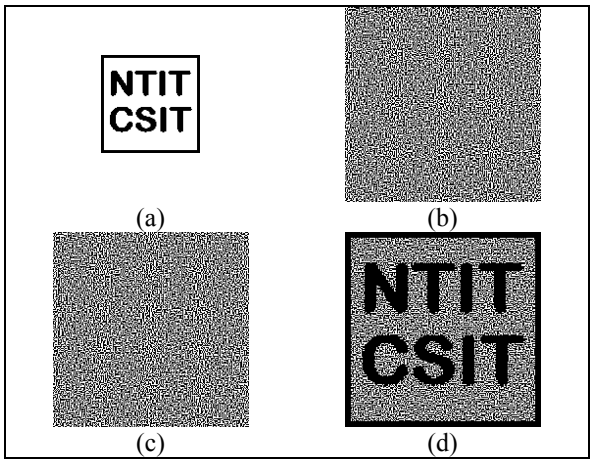

Fig. 2. English image: (a) Secret image, (b) Common shadow image , (c) Corresponding shadow image (d) Decrypted image

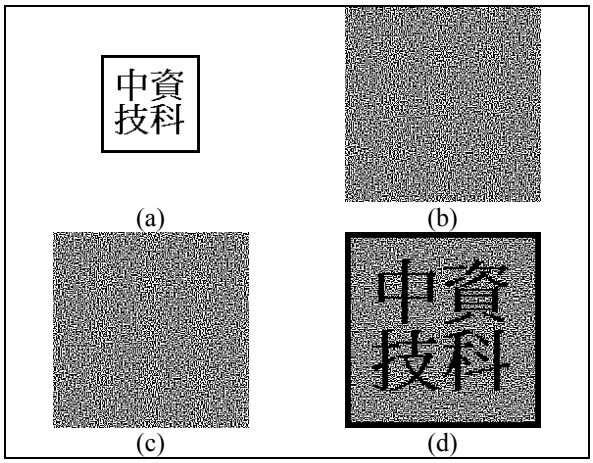

Fig. 3. Chinese image: (a) Secret image , (b) Common shadow image, (c) Corresponding shadow image, (d) Decrypted image

5. Security Analysis

In this section, we will analyze the security of the proposed scheme. In (2, 2)-threshold conventional VC, the major problem of security is reusable. When Alice and Bob stack two shadow images, S_1 and S_2, to recover secret image S, Alice/Bob remembers the shadow image S_2/ S_1 of the other party Bob/Alice. We assume that a new secret image S' is partitioned into two shadow images, S_1 and S_3, for Alice and Bob, respectively. They want to recover and use information a second time. Bob can compute S_1 from

the previously recovered image and S_2 to recover the secret without getting S_1 from the other party. The (2, 2)-threshold conventional VC can not reuse the shadow image S_1, but our proposed scheme successfully recycles shadow images by using TA.

In encryption phase, two parties agree on a common shadow image $S_1 = I_{k,g^{\beta\alpha}} = \pi_{M_k}^{g^{\beta\alpha}}(I)$. The common session key k then has two parties' information. If the two parties choose to reuse the scheme, they can reserve and reuse their common image I. When they want to communicate again, they agree on a permuted times value γ for the common session key. They compute the new common shadow image $S_1^{'} = I_{k,\gamma} = \pi_{M_k}^{\gamma}(I)$. Alice computes a new corresponding shadow image $S_2^{'}$ according to the secret image $S^{'}$ and $S_1^{'}$. Alice sends $S_2^{'}$ to Bob. Then, Bob can recover the secret information $S^{'}$ by stacking $S_1^{'}$ and $S_2^{'}$. Moreover, TA is limited by the image size. If the image size is small, the permuted image easily permutes the same as the original image. Therefore, we use Diffie-Hellman key agreement scheme to solve this problem.

Suppose that an attacker wants to compute the long-term secret I and k from S_2. There is very limited study on the attack to compute I and k. However, we will suppose the attacker has guessed I and k, but the attacker still can not compute α and β from $g^{\alpha} \pmod N$ and $g^{\beta} \pmod N$, respectively. That is based on DLP. To compute the secrets α and β, the attacker must achieve the hardness problem of DLP. On the other hand, if the common session key is tampered with by an attacker, the stacked image display is unclear and the secret is unidentified. Therefore, the proposed scheme is secure.

6. Conclusion

In this paper, we propose a new visual cryptography scheme which combines the key agreement scheme with a shadow image without building a secure connection. Even if many eavesdroppers listen over the public communication channel, we can immediately transmit a secret message to others. Moreover, we enhance shadow image structure to reduce the chances for an attacker to guess the secret. The proposed scheme involves Diffie and Hellman and toral automorphism such that it can be reused. Hence, the proposed scheme is flexible, easily implemented, and more secure for shadow images.

References

[1] Chin-Chen Chang, Jun-Chou Chuang and Pei-Yu Lin, "Sharing a Secret Two-Tone Image in Two Gray-Level Images", *11th International Conference on Parallel and Distributed Systems - Workshops (ICPADS'05)*, pp. 300-304, 2005.

[2] G. Alvarez, A. Hernández Encinas, L. Hernández Encinas and A. Martín del Rey, "A secure scheme to share secret color images", *Computer Physics Communications*, vol. 173, issue 1-2, pp. 9-16, Dec. 2005.

[3] G. Voyatzis and I. Pitas, "Applications of toral automorphisms in image watermarking", *Proceedings of International Conference on Image Processing*, vol. 2, pp. 237–240, 1996.

[4] M. Naor and A. Shamir, "Visual cryptography," *Adv. Cryptol.: EUROCRYPT, Lecture Notes Comput. Sci.*, vol. 950, pp. 1-12, 1995.

[5] R. L. Rivest and A. Shamir, "How to expose an eavesdropper", *Communications of the Association for Computing Machinery*, vol. 27, no. 4, pp. 393-395, 1984.

[6] R. Lukac and K. N. Plataniotis, "Bit-level based secret sharing", *Patter Recognition*, vol. 38, no. 5, pp. 767-772, 2005.

[7] S. Blake-Wilson and A. Menezes, "Authenticated Diffie-Hellman Key Agreement Schemes", *SAC '98: Proceedings of the Selected Areas in Cryptography*, pp. 339-361, 1999.

[8] U. Maurer, "Towards the equivalence of breaking the Diffie-Hellman scheme and computing discrete logarithms", *Advances in Cryptology - Crypto '94, Springer-Verlag*, pp. 271-281, 1994.

[9] W. Diffie and M. E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, vol. 22, issue 6, pp. 644-654, 1976.

[10] Z. Zhou, G. R. Arce and G. D. Crescenzo, "Halftone visual cryptography", *Image Processing, IEEE Transactions*, vol. 15, pp. 2441-2453, 2000.

Chao-Wen Chan received the Ph.D. degree in Computer Science and Information Engineering from National Chung Cheng University, in 2005. His current research interests include cryptography, information security and network operating system.

Yi-Da Wu received the B.S. degree in Management Science from National Taichung Institute of Technology, in 2006. His current research interests include cryptography and visual cryptography.