VISUAL SECRET SHARING OVER NATUARAL IMAGES

Hyoung Joong Kim, Yong Soo Choi

Department of Control and Instrumentation Engineering
Kangwon National University
Chunchon 200-701, Korea

ABSTRACT

In this paper a new secret sharing scheme based on natural image visual cryptography. The visual cryptography is free from dithering which degrades image quality considerably. The (n, n) visual cryptography takes n grayscale input images to cover a target image. The secret image of the target is distributed across n input images to produce innocuous n output images. However, the natural image visual cryptography exhibits a so-called negative photo artifact. In order to overcome this weakness the target pixels are expanded over neighbor pixels and permuted randomly. The strong point of this scheme is its similarity between input and output images. The reason why the negative artifact arises is explained.

1. INTRODUCTION

Visual cryptography is a kind of cryptographic technique as one of the secret sharing methods which share a visual secret among n participants by breaking up an image into n shares so that only he or she who has all of n shares can decrypt the image by overlaying each of the shares over each other. Since the secret is distributed over n shares, each share cannot disclose anything on the secret. Secret can be kept since collecting all n shares will be almost impossible. Secret sharing is a technique to distribute a secret among a group of participants. Shamir [10] and Blakley [2] independently invent this technique in 1979.

On the other hand, in 1994 Naor and Shamir [9] propose the visual cryptographic technique first. A generalized version of the visual cryptography is the (k, n)-threshold visual cryptography that encodes a target image into n shares such that any k or more shares enable the visual recovery of the hidden image. However, by inspecting less than k shares one cannot gain any information on the secret image. The 2-out-of-2 visual cryptography can be thought of as a private key system. One of the two shares will be a private share and the other serves as a public share.

A visual cryptography that reveals the target image by stacking meaningful images is called Extended Visual Cryptography [1]. Nakajima and Yamaguchi [8] introduce two definitions: the sheets are the output images and the target image is the resulting image reconstructed by stacking the sheets all together. An access structure is a rule, which defines how to share a secret. Tzeng and Hu [11] define a general access structure by three components: P is the set of participants, F is a collection of forbidden sets, and Q is a collection of the qualified sets. An element of a forbidden set or a qualified set represents a sheet held by the corresponding participant. Stacking all the forbidden sheets of a forbidden set cannot reveal any information about the target image while stacking all the sheets of a qualified set can reproduce the target image.

The basic model of the conventional visual cryptography assumes that a ciphertext is printed on each transparency that is indistinguishable from random noise. However, noise-like sheets seem to be suspicious and thus are susceptible to attacks by wardens in the middle. Naor and Shamir [9] have mentioned an extension of the visual cryptography scheme that conceals the very existence of the secret message (that is, target), which is important from the point of secret communications like steganography. Thus, producing meaningful sheets like natural images rather than random dots is important.

In the black-and-white visual cryptography (that is, with binary images) the pixel is *black* if the number of black subpixels is more than a constant threshold t, and *white* if the number of black subpixels is less than the threshold when the transparencies are stacked together. The threshold visual cryptography is a visual cryptography based on the threshold value used as a criterion of determining black dots or white dots. However, white or black color is the logical concept. Note that, in case of grayscale images, the pixel value 0 represents the darkest black and the value 255 the brightest white color.

Most of the visual cryptographic schemes need to expand pixels; that is, the pixel of the target images is reproduced by m subpixels on the sheets, where $m \geq 2$. Consequently, the sheet is m times the size of the target image, and that leads to not only distortion of images but also inconvenience of carrying large size of sheets and waste of the storage space. This situation is more serious for grayscale or color images. The parameter m is called *pixel expansion*, and the case of "m = 1" refers to situation that

the size of the sheets is same to the target. A few of studies have been done on this situation including Hou et al. [3], Hou and Tu [4], and Ito et al. [6]. Existing schemes are mostly based on the half-toning or dithering methods to expand the binary or grayscale images. However, halftone images are still unnatural and low in visual quality.

Previous works on the extended visual cryptography has dealt with binary images such as text. Recently, Hou et al. [3], Ito et al. [6], and Nakajima and Yamaguchi [8] have handled natural images for visual cryptography. Generally it has been believed that visual cryptography suffers from severe deterioration of the sheet images. Henceforth, existing schemes are not free from image deterioration. Lin and Tsai [7] convert the grayscale image into an approximate binary image by using dithering technique first, and then existing visual cryptography schemes for binary images are applied to create sheets. Even though this scheme takes grayscale images, it produces sheets of random dots. Hou et al. [3], Ito et al. [6], and Nakajima and Yamguchi [8] have taken grayscale images and produced relatively low quality sheets due to dithering. Kim and Choi [5] introduce natural image visual cryptography with $m = 1$. However, the scheme can exhibit a negative photo effect which may disclose part of the secret information through the negative image obtained by stacking $n-1$ sheets together. This artifact is a vital weakness of the secret sharing scheme and visual cryptography as well. One contribution of this paper is to make it extremely difficult to guess the target image from less than $n-1$ sheets.

2. OUTLINE OF VISUAL CRYPTOGRAPHY SCHEME

The proposed algorithm in this paper consists of two major phases: the encoding phase and the decoding phase. In the encoding phase, n grayscale images and one target image are processed to produce n output images, that is, sheets, which are very close to the input images. Since the sheets are so innocuous and natural that warden may pay little attention as Alice and Bob intend. In the decoding phase, the n sheets are stacked to reproduce target image.

2.1. Encoding scheme

Let there be n input images P_k, $k = 1, \ldots, n$. Let $P_k(i, \mathrm{j})$ denote the pixel of P_k in location (i, j). Now, we introduce a new value $P(i, j)$ such

$$P(i, j) = \sum_{k=1}^{n} P_k(i, j) \bmod v \tag{1}$$

where v is the grayscale value. When the image is an 8-bit gray-level, the value v is 255. The main idea of the encoding phase is to make the value $P(i, \mathrm{j})$ equals zero before generating sheets. It is obvious that $P(i, j)$ rarely zero. Therefore, we have to modify the values so that

$$\sum_{k=1}^{n} \{P_k(i, j) \pm x(i, j)\} \equiv 0 \bmod v \tag{2}$$

Equation (2) is a necessary step to hide target image over the input images. Equation (2) is the preliminary step for encoding.

Let I be the target image. The target I is expanded by m times to produce the expanded target T. Permutation and expansion schemes of I over T are a secret for decoding and extracting target image. The encoding step is very simple. Encoding step is just modifying the pixel values so that

$$\sum_{k=1}^{n} \{P_k(i, j) \pm x(i, j) \pm y(i, j)\} \equiv T(i, j) \bmod v \tag{3}$$

The values $x(\mathrm{i}, j)$ and $y(\mathrm{i}, j)$ should be chosen carefully so that sheets do not have noticeable artifacts. Needless to say, human visual system characteristics for each input image are considered to choose $x(i, \mathrm{j})$ and $y(i, j)$. Another important fact is the basic requirement of the secret sharing schemes: stacking all n sheets reveals the target, but any combination of less than n sheets reveals nothing close to the target image. Thus, choosing $x(i, \mathrm{j})$ and $y(i, j)$ well is a key of the encoding scheme. Let S_k be the kth sheet image. Then, the sheet image is obtained as follows:

$$S_k(i, j) = P_k(i, j) \pm x(i, j) \pm y(i, j) \tag{4}$$

The following example may illustrate how the proposed encoding scheme works. Let the pixel in (1, 1) position of 5 input images be 100, 110, 120, 60, and 150. $P(1, 1) \equiv \{100 + 110 + 120 + 60 + 150\} \bmod 255 \equiv 30$ as given in Equation (1). Then, we can subtract 6 from each pixel value. So the resulting pixel values are given as 94, 104, 114, 54, and 144. Now, let the target image value in position (1, 1) be 36. Thus, the pixel values of sheets are 101, 111, 121, 61, and 151.

2.2. Decoding scheme

The decoding phase is also very simple. Simply computing the following Equation (5) produces the expanded target image.

$$T(i, j) = \sum_{k=1}^{n} S_k(i, j) \bmod v \tag{5}$$

The target image can be recovered from the expanded target by applying the inverse operations of permutation and expansion. It is quite obvious from the Equations (3) and (4). The sheets have been designed to produce the expanded target in Equation (3). In addition, even though the sheets are attacked, it is obvious from the Equations

(3), (4) and (5) that the target image can be recovered. Of course, the recovered target image quality may be slightly degraded due to malicious attacks.

3. EXPERIMENTS

In this experiment the target image is "Tank" (grayscale image with 128×128 pixels) as shown in Fig. 1 and 30 grayscale images with 256×256 pixels are used as input images, where n = 30. Fig. 2 shows the input images.

FIGURE 1. TARGET IMAGE "TANK" OF TIFF FORMAT.

Encoding phase follows the modification scheme according to the Equation (3). After the encoding phase, the average PSNR is 34.02 dB. The average PSNR (that is, the average image quality of sheets) depends on the types of input images and target image. For example, the darker target image is, the higher the PSNR is. In addition, pixel value modification algorithm also affects the average PSNR. Needless to say, the extracted image at the decoding phase based on the Equation (5) is exactly the same as the target image. It is obvious from the statement given in Section II.

FIGURE 2. INPUT IMAGES (30 TIFF FORMAT IMAGES).

Fig. 3 shows a negative image, which demonstrates a so-called negative photo artifact. We process 30 input images by the Equation (2) first and stack 29 images processed and get the negative image in Fig. 3. Of course, the negative image is not an exact negative of the first image in Fig. 2 due to the processing by Equation (2). Fig. 4 shows another image processed similarly. Note that the negative image is a composite of two images, the first and second images in Fig. 2. This negative artifact can reveal the secret of the target image as is shown in Fig. 5.

FIGURE 3. AN EXAMPLE OF NEGATIVE ARTIFACT WHICH IS RECONSTRUCTED FROM 29 IMAGES PROCESSED.

FIGURE 4. ANOTHER EXAMPLE OF NEGATIVE ARTIFACT WHICH IS RECONSTRUCTED FROM 28 IMAGES PROCESSED.

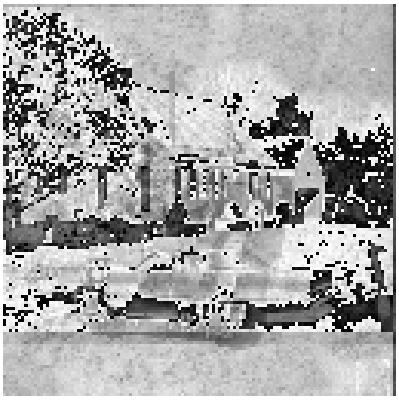

FIGURE 5. AN IMAGE RECONSTRUCTED BY 29 SHEETS SHOWING TANK IMAGE FAINTLY IN FIG. 1.

Note that silhouette of the Fig. 1 is observed faintly from the Fig. 5 with $m = 1$. Of course, permutation of the target image can make the decoding of it difficult to reconstruct. The reason why the negative artifact is observed is obvious: Equation (2) is the clue. Due to the modulus operation to the stack of n images to 0 it is obvious that reconstruction by $n-1$ images makes the remaining one image negative.

4. CONCLUSIONS

In this paper a new secret sharing scheme based on natural image visual cryptography. The visual cryptography is free from dithering which degrades image quality considerably. The (n, n) visual cryptography takes n grayscale input images to cover a target image. The secret image of the target is distributed across n input images to produce innocuous n output images. However, the natural image visual cryptography exhibits a so-called negative photo artifact. In order to overcome this weakness the target pixels are expanded over neighbor pixels and permuted randomly. The strong point of this scheme is its similarity between input and output images. The reason why the negative artifact arises is explained. Various expansion and permutation schemes are considered, but not reported in this paper due to the page limitation. Robustness against various attacks is simulated, but not reported in this paper due to the page limitation (refer to [5]).

5. REFERENCES

[1] G. Ateniese, C. Blundo, A. de Santis, and D. Stinson, "Visual cryptography for general access structures," Information and Computation, vol. 129, no. 2, pp. 86-106, 1996.

[2] G. R. Blakley, "Safeguarding cryptographic keys," *American Federation of Information Processing Proceedings*, vol. 48, pp. 313-317, 1979.

[3] Y. C. Hou, C. F. Lin, and C. Y. Chang, "Visual cryptography for color images without pixel expansion," *Journal of Technology*, vol. 16, no. 4, pp. 595-603, 2001.

[4] Y. C. Hou, and S. F. Tu, "A visual cryptographic technique for chromatic images using multi-pixel encoding method," private communication, 2004.

[5] H. J. Kim, and Y. S. Choi, "A new visual cryptography using natural images," under preparation.

[6] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Transactions on Fundamentals*, vol. E82-A, no. 10, pp. 2172-2177, 2002.

[7] C.-C. Lin, and W.-H. Tsai, "Visual cryptography for gray-level images by dithering techniques," Pattern Recognition Letters, vol. 24, issue 1-3, pp. 349-358, 2003.

[8] M. Nakajima, and Y. Yamaguchi, "Extended visual cryptography for natural images," *Proceedings of the.10th International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision*, University of West Bohemia, Czech Republic, pp. 303–340, 2002.

[9] M. Naor, and A. Shamir, "Visual cryptography," *Lecture Notes in Computer Science*, vol. 950, Springer-Verlag, pp. 1-12, 1995.

[10] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612-613, 1979.

[11] W. G. Tzeng, and C. M. Hu, "A new approach for visual cryptography," *Designes, Codes and Crryptography*, vol. 27, pp. 207-227, 2002.