An Innocuous Visual Cryptography Scheme

Conference Paper · July 2007

DOI: 10.1109/WIAMIS.2007.19 · Source: IEEE Xplore

4 authors, including:

Vasily Sachnev
Catholic University of Korea
23 PUBLICATIONS **511** CITATIONS

An Innocuous Visual Cryptography Scheme

Hyoung Joong Kim, Vasiliy Sachnev, Su-Jeong Choi, Shijun Xiang

Center for Information Security Technologies
Korea University
Seoul, 136-701, Korea
khj-@korea.ac.kr

Abstract

An innocuous visual secret sharing scheme over natural images is presented in this paper. Secret sharing scheme allows a group of participants to share a secret (i.e., an image) among them. In case of (k, n) visual cryptography any group of k qualified participants among n (where $k \leq n$) can reconstruct the secret. This paper presents (n, n) visual cryptography scheme. This scheme does not apply dithering techniques to hide a secret image. Thus, it does not degrade quality of the secret image and in particular, this scheme is far from negative photo effect. Instead of dithering, this scheme spreads data by applying simple arithmetic operations. The rationale of arithmetic operations is presented.

1 Introduction

Original *visual cryptography* [13] is a kind of cryptographic technique that encrypts the secret U (i.e., a visual image) by producing shares, S_k, $k = 1, \cdots, n$. The hidden secret can be reconstructed from the shares usually by stacking them. The binary image U is usually expanded and dithered. The recovered secret image is poor in image quality due to dithering and expansion. In addition, U may be different from the recovered secret image. Of course, it can deliver sufficient visual information regarding U. One of many advantages of this visual cryptography is its secret sharing capability: the hidden secret can be recovered correctly if all the pieces are collected, exactly aligned and stacked. The secret cannot be recovered when even a single share is missed. Disadvantage of this scheme is its noise-like shares. Early visual cryptography techniques have produced shares which are too suspicious and awkward to pass censors. Random transparencies with one bit deep images are very unusual [4]. Thus, they are suspect to censors. Visual cryptography is unreliable in the context of censors. Since they are noise-like or unusually poor in image quality, it may be easy to be censored. Images should be natural in order to evade inspection.

Innocuous visual cryptography is a visual cryptography or visual secret sharing scheme that produces innocuous shares. In that sense the shares, S_k, $k = 1, \cdots, n$, are innocuous and natural as the given input images, P_k. Due to their improved innocuousness the shares are highly likely to pass censors easily. Similar idea has been proposed by Biham and Itzkovitz [2] in 1997, and Desmedt et al. [4] in 1998. Biham and Itzkovitz [2] have exploited polarized lights to achieve the innocuousness. The cerebral cryptography [4] utilizes the depth perception property of the human visual system. However, image quality is not perfectly regular and distortion of the images is noticeable, which makes it difficult to pass censors.

In addition, in case of original visual cryptography schemes [13], [14], the reconstructed image quality is not satisfactory due to one bit of depth in image resolution. The recovering process does not pose a problem, but the encoding process does as it causes distortion to the original image. Even though Viet and Kurosawa [16] have improved the visible quality of reconstructed secret images, it is not perfectly the same as the original one. Lukac et al. [10] and Lukac et al. [11] have proposed a visual cryptography scheme which can recover images perfectly identical to the input images. However, their shares are dithered and far from real-life images. Chang et al. [3] also have hidden a binary image into two gray-scale images. Thus, shares are innocuously natural images. Hou et al. [5], Ito et al. [6], Lin and Tsai [9], and Nakajima and Yamaguchi [12] have handled natural images as input images. However, they have produced relatively low quality shares from gray-scale images due to the nature of dithering.

The first model of the visual cryptography scheme [13], [15] produces n pieces of ciphertext printed on each transparency (i.e., a share) that is indistinguishable from random noise. However, noise-like shares seem to be suspicious and

Eight International Workshop on Image Analysis for Multimedia Interactive Services(WIAMIS'07)
0-7695-2818-X/07 $20.00 © 2007 IEEE

thus are susceptible to attacks by wardens-in-the-middle. Therefore, producing meaningful shares like innocuously natural images rather than a set of random dots is important. Naor and Shamir [13] have mentioned an extension of the visual cryptography scheme that conceals the very existence of the secret message. It is important from the point of secret communications like *steganography*. *Extended visual cryptography* [1] is a method that encodes a number of images so that when the images are superimposed, a hidden image appears, whereas the original images disappear. However, the shares of the first extended visual cryptography scheme [1] were dithered, binary images. On the other hand, some visual cryptography techniques produces natural images as shares [7], [8]. Since these shares are relatively innocuous, they are unlikely to be attacked by wardens-in-the-middle. Some visual cryptography schemes have hidden secret into natural images (i.e., [7]) based on the concept of extended visual cryptography.

Kim and Choi [7] have introduced innocuous visual cryptography with $m = 1$. However, the scheme can exhibit a *negative photo effect* which may disclose some secret information through the negative image obtained by stacking less than n sheets together [8]. It is a fatal weakness of this secret sharing scheme. Thus, if the negative photo effect can be removed, the method can be quite remarkable in many respects. In addition, the scheme of Kim and Choi [7], [8] requires lots of natural images to generate innocuous shares. The main objective of this paper is to present an innocuous visual cryptography which is free from the negative photo effect. In addition, this scheme requests a small number of shares.

This paper introduces a new innocuous visual cryptography scheme based on the number representation system in Section 2. Section 3 presents experimental results. Section 4 concludes the paper.

2 New Scheme

The previously mentioned scheme [7] has significant drawbacks. First, this method is not free from the negative photo effect which reveals the hint or clue of the hidden image if less than n shares are stacked and processed. The negative photo can be easily generated from the original photo by reversing the pixel values. The negative photo effect should be avoided since it violates the basic assumption of the secret sharing scheme.

The second weakness of the previous method is its huge number of shares. In order to make the shares innocuous, the number of shares should be large. When two shares are used, the maximum error for the worst pixel case is about 128, which is very significant. For example, if all pixels in an image have the same degree of errors, its predictive signal-to-noise ratio (PSNR) is no more than 6 dB. Increasing number of shares can be a solution in the previous scheme [7].

The goal of the innocuous visual cryptography is to keep the share S_k as close as the input image P_k such as $S_k \simeq P_k$ and recover the hidden image U by manipulating n valid shares and applying simple mathematical operations. Now, note that stacking shares cannot recover U. A simple mathematical operations can recover U. This is the main difference between the original visual cryptography and the innocuous visual cryptography. Of course, the computational requirements for this recovering process is negligible. In addition, the innocuous visual cryptography scheme should be free from the negative photo effect and request a small number of shares.

An example can be useful for easy understanding of the proposed scheme. Let the pixel values in the (1, 1) position of 5 input images be 100, 110, 120, 60, and 150, respectively. Let the secret image value in position (1, 1) be 36. For example, assume that the arithmetic rule should be $A = A_4(i,j) \times \{A_3(i,j) \times A_2(i,j)\} + A_1(i,j) + A_0(i,j)$, where $A_k(i,j)$ is a decimal number. There are many ways to make 36 by doing simple decimal arithmetic with 5 numbers, for example:

Case 1: $3 \times (3 \times 4) + 0 + 0 = 36$,
Case 2: $4 \times (3 \times 3) + 0 + 0 = 36$, or
Case 3: $5 \times (2 \times 3) + 3 + 3 = 36$.

Assigning the arithmetic rule and decimal numbers is totally up to the encoder. They can be decided according to the number of shares, desirable image quality of the shares, and robustness against attacks. In this case, the arithmetic rule is an important secret key for recovering the secret image. The sequences of images can be another secret key for decoding according to the arithmetic rules. For example, the encoding rule by Kim and Choi [7], [8] is independent of the image sequences because the used arithmetic operations are additions which are commutative. However, if the sequence of n images is not known for the proposed scheme in this paper, $n!$ brute-force trials are necessary to find the exact solution. Thus, the sequence information is inevitably important.

Let the coefficient sequence of $A_k(i,j)$s be {3, 3, 4, 0, 0}. Then, the corresponding pixel values of input images should be changed as {103, 113, 124, 60, 150}. Needless to say, the decoder should recover the same sequence as encoder such as {3, 3, 4, 0, 0}. The simplest way is as follows: $A_k(i,j) \equiv S_k(i,j) \bmod \nu$, where $\nu = 5$ in this case. Based on this decoding rule, the encoding rule for the decimal numbers can be designed such as $S_k(i,j) = P_k(i,j) \pm X_k(i,j)$ where $A_k(i,j) \equiv P_k(i,j) \pm X_k(i,j) \bmod \nu$. Thus, {98, 108, 119, 60, 150} can be another solution with $\nu = 5$. Then, note that {98, 108, 119, 60, 150} is better than {103,

0-7695-2818-X/07 $20.00

113, 124, 60, 150} in terms of magnitude of errors. However, there are much more valid solutions such as {98, 113, 124, 60, 150}, or {103, 113, 124, 60, 155}, where the last one is the worst among them in terms of the magnitude of errors.

Let the number of available input images be just 4. Assume that the image quality should be high. Then, the encoding rule should be different from the above one. One possible solution is $4^3A_3(i,j) + 4^2A_2(i,j) + 4^1A_1(i,j) + 4^0A_0(i,j)$. When the secret number is 244, one of the desirable coefficient sequences is $\{3, 2, 4, 4\}$. In this case, the minimum valid value of ν is 5 and maximum pixel error is 4. Thus, the worst case PSNR is just 36.1 dB. Of course, $\{3, 2, 1, 0\}$ can also be a solution when ν is 4. In this case, the maximum pixel error is 3 and the worst case PSNR is 38.5 dB. When ν is 4, this representation gives the unique solution.

Obviously, this innocuous visual cryptography scheme is free from the negative photo effect. This method can reduce the magnitude of errors even though the number of shares is small. There are many ways to represent the given numbers using simple arithmetic operations. Thus, this data hiding scheme can be a representation problem. The best representation method needs to be developed for optimizing the performance. The representation problem should take the image quality of shares into consideration. The number system can be either binary, octal, decimal, hexadecimal, or whatever. Those issues are open problems. One weakness of this scheme is susceptibility to attacks. In case of the arithmetic rule of $4^3A_3(i,j) + 4^2A_2(i,j) + 4^1A_1(i,j) + 4^0A_0(i,j)$, the decimal number $A_3(i,j)$ is most vulnerable to error because its multiplicative constant 4^3 is very large while $A_0(i,j)$ is least because its multiplicative constant 4^0 is small. The procedure for the design of this innocuous visual cryptography scheme is as follows:

- The number of shares n should be decided. Image quality of shares and robustness against the malicious attacks depend on the number of shares.
- The arithmetic rule and the number representation system should be decided. In this case, the number of shares, image quality of shares, and robustness against the malicious attacks should be considered.
- The encoder should decide the distributed secret number $A_k(i,j)$ based on the arithmetic rule. The share $S_k(i,j)$ can be produced such as $P_k(i,j) \pm A_k(i,j) \bmod \nu \equiv 0$. The magnitude of the error should be minimized.

In general, the encoding procedure is relatively more complicated than the decoding procedure. The decoder can derive the the distributed secret number $A_k(i,j)$ by applying $A_k(i,j) \equiv S_k(i,j) \bmod \nu$. The hidden secret can be recovered by the arithmetic rule and the the distributed secret numbers.

3 Experimental Result

The theory proposed in this paper is verified in this section by experiments through different groups of images based on the arithmetic representation system. Four images are used to hide a secret image. For instance, the four input images are Barbara, Mandrill, F-16, and Pepper, respectively, in the first group. The Lena image is used as a secret image.

The secret image Lena can be successfully embedded into 4 images. Note that the distortion of shared images is almost imperceptible. The PSNR of the shared images is mostly over 44 dB. Experimental results with different groups of input images are tabulated in Table 1. It is noted that the image quality of all images after the embedding is higher than 43 dB, which demonstrates that the proposed innocuous visual cryptography scheme makes distortion little. When a is 4 and ν is 4 with 4 shares, the worst PSNR is predicted to be 38.59 dB in the previous section.

These experiments show that actual PSNR is always quite higher than 38.59 dB and the secret image can be recovered perfectly as long as there are no malicious attacks, the shared images are visually innocuous, and the secret image can be shared distributively. Of course, the proposed scheme has some drawbacks. One of them is its susceptibility against malicious attacks. However, such a problem will be solved if the number of shares is increased, a robust rule of arithmetic representation system is devised, or robust embedding schemes against malicious attacks are used. The main purpose of this paper is only to show the possibility of innocuous visual cryptography scheme based on the arithmetic representation system. Novel embedding schemes are beyond the scope of this paper.

4 Concluding Remarks

In this paper a new (n, n) innocuous visual cryptography scheme without dithering is proposed. This scheme takes n gray-scale input images, P_k, $k = 1, \cdots, n$ into consideration to cover a secret image, U, produces n gray-scale shares, S_k, which are very close to the input images, respectively. This technique does not expand pixels to hide the secret image across the shares. This scheme can expand pixels to enhance robustness or its security. The most important contribution of this paper is that the shares are so

Table 1. Experimental results with 4 images for each group

Input images	Secret Image	PSNR (dB)
Barbara		45.07 dB
Mandrill	Lena	44.18 dB
F-16		44.07 dB
Pepper		44.05 dB
Aeral		45.13 dB
Boat	Lena	44.02 dB
Bridge		44.18 dB
Camera		44.41 dB
Clock		45.00 dB
Couple	Lena	44.05 dB
Resolution Chart		43.02 dB
Lady		44.20 dB

close to the input images and keeping high image quality that it makes the shares visibly almost innocuous and natural. This fact is very important from the perspective of steganography to fool the wardens in the middle between Alice and Bob. In addition, the scheme is free from the negative photo effect. Lastly, note that it requests a small number of shares to hide a natural secret image. The scheme can be extensible to the (k, n) case.

The scheme is very useful when the secret message U itself is an encrypted text. The secret message can be distributed across shared images innocuously based on the secret sharing philosophy. Thus, stacking shares is meaningless because the hidden message is not an image. The recovered secret message should be exactly the same as U since the hidden message is an encrypted text. From the perspective of cryptanalysis, this scheme can be a nightmare. Locating all suspicious shares among a tremendously large number of images, correctly collecting all of them, recovering secret messages, and decrypting the messages are far more difficult than decrypting the encrypted text itself. Visual cryptography can be a good tool for exchange of highly secret messages. A number of cover images can hide the presence of the hidden message. Thus, innocuous visual cryptography is useful to improve the security, but it should be different from stacking shares. As long as highly secret messages are exchanged, negligible computing computing power for recovering U will not be burdensome. This scheme will enhance security far more than existing secret communication schemes. It is the important rationale of this scheme based on the number representation system.

In order to enhance robustness against malicious attacks, this scheme should incorporate the robust data hiding schemes. It is an open problem to be solved. However, securing robustness is another challenging problem to be solved.

Acknowledgment

This research was supported by Korean Ministry of Information and Communication under the project funded by the Information Technology Research Center (ITRC).

References

[1] G. Ateniese, C. Blundo, A. De Santis, and D. Stinson. Extended capabilities for visual cryptography. *Theoretical Computer Science*, 250:143–161, 2001.

[2] E. Biham and A. Itzkovitz. Visual cryptography with polarization. *Proceedings of the Weizmann Workshop on Cryptography*, 1997.

[3] C. C. Chang, J. C. Chuang, and P. Y. Lin. Sharing a two-tone image in two gray-level images.

[4] Y. G. Desmedt, S. Hou, and J. J. Quisquater. Cerebral cryptography. *Lecture Notes in Computer Science*, 1525:62–72, 1998.

[5] Y. C. Hou, C. F. Lin, and C. Y. Chang. Visual cryptography for color images without pixel expansion. *Journal of Technology*, 16(4):595–603, 2001.

[6] R. Ito, H. Kuwakado, and H. Tanaka. Image size invariant visual cryptography. *IEICE Transactions on Fundamentals*, E82-A(10):2172–2177, 2002.

[7] H. J. Kim and Y. S. Choi. A new visual cryptography using natural images. *Proceedings of the IEEE International Symposium on Circuits and Systems*, 6:5537–5540, 2005.

[8] H. J. Kim and Y. S. Choi. Secret sharing by natural image visual cryptography. *Proceedings of the International Workshop on Image Analysis for Multimedia Interactive Services*, 2005.

[9] C. C. Lin and W. H. Tsai. Visual cryptography for gray-level images by dithering techniques. *Pattern Recognition Letters*, 24:349–358, 2003.

[10] R. Lukac, K. N. Plataniotis, B. Smolka, and A. N. Venetsanopoulos. A new approach to color image secret sharing. *Proceedings of the 12th European Signal Processing Conference*, pages 1493–1496, 2004.

[11] R. Lukac, K. N. Plataniotis, and A. N. Venetsanopoulos. $\{k, n\}$-secret sharing scheme for color images. *Lecture Notes in Computer Science*, 3039:72–79, 2004.

[12] 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*, pages 303–340, 2002.

[13] M. Naor and A. Shamir. Visual cryptography. *Lecture Notes in Computer Science*, 950:1–12, 1995.

[14] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[15] D. Stinson. Visual cryptography and threshold schemes. *IEEE Potentials*, 18(1):13–16, 1999.

[16] D. Q. Viet and K. Kurosawa. Almost ideal contrast visual cryptography with reversing. *Lecture Notes in Computer Science*, 2964:353–365, 2004.