AN IMPROVED VISUAL CRYPTOGRAPHY SCHEME FOR SECRET HIDING

R.Youmaran, A. Adler, A. Miri
School of Information Technology and Engineering (*SITE*),
University of Ottawa, Ontario, Canada

ABSTRACT

Visual Cryptography is based on cryptography where *n* images are encoded in a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all shares are stacked together. This paper presents an improved algorithm based on Chang's and Yu visual cryptography scheme for hiding a colored image into multiple colored cover images. This scheme achieves lossless recovery and reduces the noise in the cover images without adding any computational complexity.

Keywords: Image processing, visual Cryptography, secret sharing

I. INTRODUCTION

Visual cryptography, introduced by Naor and Shamir in 1995 [2], is a new cryptographic scheme where the ciphertext is decoded by the human visual system. Hence, there is no need to any complex cryptographic computation for decryption. The idea is to hide a secret message (text, handwriting, picture, etc…) in different images called shares or cover images. When the shares (transparencies) are stacked together in order to align the subpixels, the secret message can be recovered. The simplest case is the 2 out of 2 scheme where the secret message is hidden in 2 shares, both needed for a successful decryption [2]. This can be further extended to the k out of n scheme where a secret message is encrypted into n shares but only k shares are needed for decryption where $k \leq n$. If k-1 shares are presented, this will give no information about the secret message. Naor and Shamir applied this idea on black and white images only. Few years later, Verheul and Tilborg [4] developed a scheme that can be applied on colored images. The inconvenient with these new schemes is that they use meaningless shares to hide the secret and the quality of the recovered plaintext is bad. More advanced schemes based on visual cryptography were introduced in [1, 3, 5] where a colored image is hidden into multiple meaningful cover images. Chang et al. [3] introduced in 2000 a new colored secret sharing and hiding scheme based on Visual Cryptography schemes (VCS) where the traditional stacking operation of subpixels and rows interrelations is modified [5]. This new technique does not require transparencies stacking and hence, it is more convenient to use in real applications. However, it requires the use and storage of a Color Index Table (CIT) in order to losselessly recover the secret image. CIT requires space for storage and time to lookup the table. Also, if number of colors c increases in the secret image, CIT becomes bigger and the pixel expansion factor becomes significant which results in severe loss of resolution in the camouflage images.

Chang and Yu introduced in [1] an advanced scheme for hiding a colored image into multiple images that does not require a CIT. This technique achieves a lossless recovery of the secret image but the generated shares (camouflage images) contain excessive noise. This paper introduces an improved scheme based on Chang's technique in order to enhance the quality of the cover images while achieving lossless recovery and without increasing the computational complexity of the algorithm.

II. DEVELOPMENT

1. Chang's et al. Algorithm

Chang et al. proposed in 2002 a new secret color image sharing scheme [1] based on modified visual cryptography. The proposed approach uses meaningful shares (cover images) to hide the colored secret image and the recovery process is lossless. The scheme defines a new stacking operation (XOR) and requires a sequence of random bits to be generated for each pixel. Chang's scheme can be generalized to an *n* out of *n* approach as opposed to Chang Tsai's scheme presented previously.

Method description

Assume that a gray image with 256 colors constitute a secret to be hidden. Each color can be represented as an 8-bit binary vector. The main idea is to expand each colored pixel into *m* subpixels and embed them into *n* shares. This scheme uses m=9 as an expansion factor. The resulting structure of a pixel can be represented by an nx9 Boolean matrix $S=[S_{ij}]$ where $(1 \leq i \leq n,\ 1 \leq j \leq 9)$ and S_{ij} =1, if and only if, the j^{th} subpixel in the i^{th} share has a non-white

color. To recover the color of the original secret pixel, an "XOR" operation on the stacked rows of the *n* shares is performed.

1.1 Hiding Algorithm

For a 2 out of 2 scheme, the construction can be described by a collection of 2x9 Boolean matrices *C*. If a pixel with color $k=(k_1k_2...k_8)_2$ needs to be shared, a dealer randomly picks an integer r between 1 and 9 inclusively as well as one matrix in C. The construction is considered valid if the following conditions are satisfied:

$$k_i = S_{1j} \oplus S_{2j} \quad (1)$$

where $k_i = S_{1j} \oplus S_{2j}$ and $j = \begin{cases} i & if\ i < r \\ i+1 & if\ i > r \end{cases}$

Note that the number of 1's in the first row of S must exceed the number of 0's by one.

Steps of the Algorithm

- Take a colored secret image I_{HL} of size *HxL* and choose any two arbitrary cover images O^1_{HL} and O^2_{HL} of size *HxL*
- Scan through I_{HL} and convert each pixel I_{ij} to an 8-bits binary string denoted as $k=(k_1k_2...k_8)_2$
- Select a random integer r_p, where $1 \le r_p \le 9$ for each pixel I_{ij}
- According to r_p and *k* for each pixel, construct S to satisfy equation (1)
- Scan through O^1 and for each pixel of color k^1_p, arrange the row "i" in S as a 3x3 block B^1_p and fill the subpixels valued "1" with the color k^1_p
- Do the same for O^2 and construct B^2_p. The resulting blocks B^1_p and B^2_p are the subpixels of the p^{th} pixel after the expansion
- After processing all the pixels in I_{HL}, two camouflage colored images $O^{1'}$ and $O^{2'}$ are generated. In order to losselessly recover I_{HL}, both $O^{1'}$ and $O^{2'}$ as well as a sequence of random bits $R=\{r_1, r_2, \dots, r_{|I|}\}$ are needed.

Figure 1 describes the (2,2) scheme for hiding one pixel. This process is repeated for all pixels in I_{HL} to construct both camouflage images $O^{1'}$ and $O^{2'}$.

1.2 Recovering Algorithm

In order to recover the secret image in a 2 out of 2 scheme, both camouflage images $O^{1'}$, $O^{2'}$ as well as the string of random bits R are required for the recovery process (Fig. 2). The camouflage images are *t* time bigger than I_{HL} due to the expansion factor of subpixels.

Steps of the Algorithm

- Extract the first 3x3 blocks V^1_r and V^2_r from both camouflage images $O^{1'}$ and $O^{2'}$, respectively.
- Re-arrange V^1_r and V^2_r in a 2x9 matrix format S_r
- Select the first random bit r_p corresponding to the first encrypted pixel
- Input S_r and r_p to the *F(.,.)* function corresponding to equation (1).
- Recover k_p, the first pixel in I_{HL}
- Repeat for all 3x3 blocks in $O^{1'}$ and $O^{2'}$

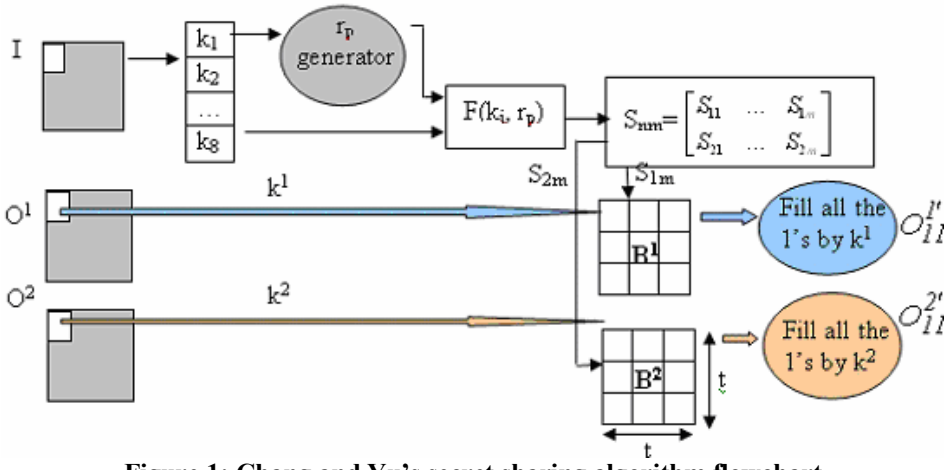

Figure 1: Chang and Yu's secret sharing algorithm flowchart

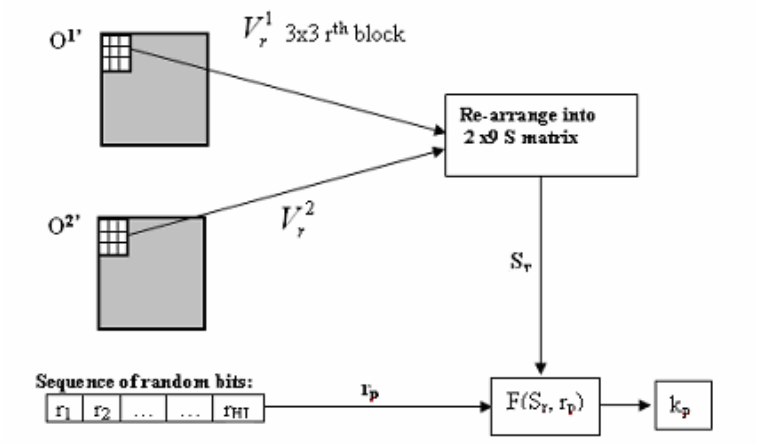

Figure 2: Chang Tsai secret sharing recovering algorithm

2. Improved image generation scheme

In this section, we introduce a modification of Chang's algorithm to generate better quality camouflage images. Most of the modifications are applied to the subpixel expansion block described in the next section.

2.1 Hiding Algorithm

Before subpixel expansion, add one to all pixels in the cover images and limit their maximum value to 255. This ensures that no "0" valued pixels exist in the images. When the images are expanded, replace all the 0's in S_0, S_1 by values corresponding to k_1-*1* in B_1 and k_2-*1* in B_2 (Figure 3) instead of leaving them transparent. Also, adjust all pixel values to be between 0-255

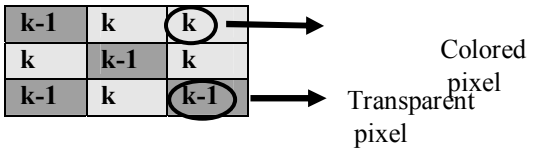

Figure 3: Improved block subpixel expansion technique

2.2 Decryption algorithm

To recover the secret image, both camouflage images $O^{1'}$, $O^{2'}$ and the string of random bits R are required.

Steps of the Algorithm

- Take all regions of size *txt* in the camouflage images
- Re-structure the square matrices as 1xm vectors
- Scan through the 9 subpixels in the vector and note the coordinates of the k^1 and the k^1-*1* colors previously encrypted
- Count the number of *k* and *k-1* pixels in the processed vector, denoted as $count_{k-1}$, $count_k$, respectively.
- If $count_{k-1} < count_k$, the transparent pixel is color *k*-1, otherwise, set it to *k*
- Use the k^1 and k^2 colors to find the secret pixel using the *F(.,.)* function and the random number previously transmitted
- Repeat for all *txt* block pixels in the camouflage images

III. RESULTS

A 100x100 secret image (forest) is hidden into two 100x100 cover images (snow and jet). As seen in Figure 4 (d, e), the camouflage images obtained using the original algorithm are noisy and of poor resolution. However, the recovery process is lossless and the used cover images are meaningful. Figure 5 (a, b) shows the camouflage obtained using the enhanced algorithm where noise is considerably reduced while achieving lossless recovery of the secret message.

To quantify the improvement in image quality using the new algorithm, the improvement signal to noise ratio (ISNR) [6] is used. The ISNR is defined as:

$$ISNR = 10\log\left[\left\|O_1' - O_1\right\|_2^2 \Big/ \left\|O_1'' - O_1\right\|_2^2\right] \quad (2)$$

where O_1 is the original cover image, O_1' and O_1'' are the camouflage images obtained from Chang's and the new algorithm, respectively. An ISNR of 9.3 dB and 19.97 dB are obtained for the 1st and 2nd camouflage images, respectively.

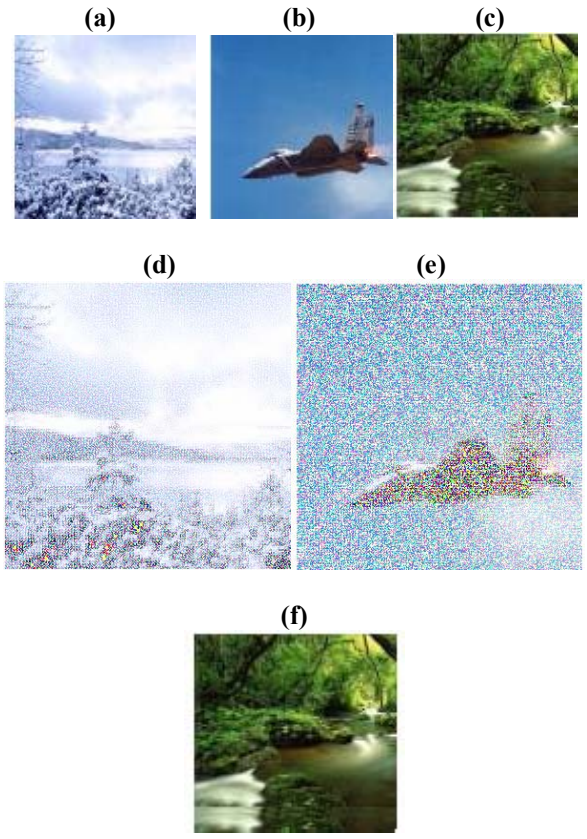

Figure 4: Chang's secret sharing algorithm results: (a) cover image #1, (b) cover image #2, (c) secret Image(d) camouflage #1 (e) camouflage #2, (f) recovered image

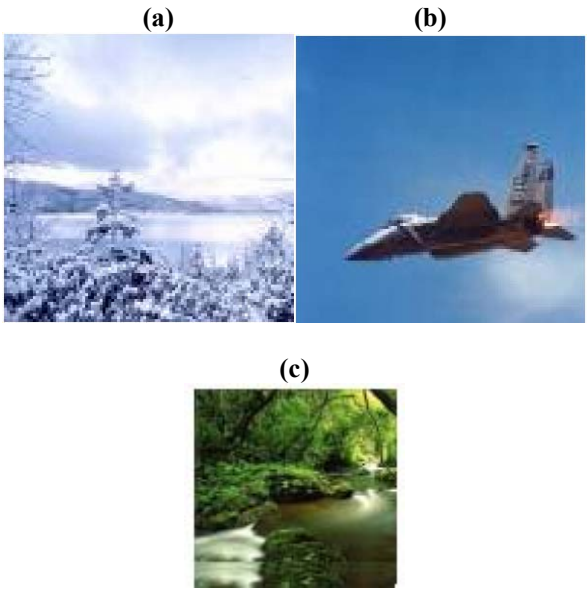

Figure 5: Improved Chang's sharing algorithm results: (a) camouflage #1, (b) camouflage #2, (c) recovered image

IV. DISCUSSION AND CONLUSION

This paper presented a new technique based on Chang et al. algorithm [5] to hide a color secret image into multiple colored images. The generated camouflage images contain less noise compared to the ones previously obtained (Fig. 4, 5) using the original Chang's embedding algorithm. This results in a considerable improvement in the signal to noise ratio of the camouflage images by producing images with similar quality to the originals. An improvement in signal to noise ration of 9.3 dB and 19.97 dB were obtained for the initial camouflage images used for hiding the secret image. This developed method does not require any additional cryptographic computations and achieves a lossless recovery of the secret image. In addition, the camouflage images obtained using the modified algorithm look less susceptible of containing a secret message than the ones obtained using the original method.

As future work, this scheme can possibly be modified to hide two independent colored secret images into n meaningful colored cover images. The recovery process of both secret images should remain lossless while using the same expansion factor as described in this paper.

REFERENCES

[1] Chang, C. C. and Yu. T. X., Sharing a Secret Gray Image in Multiple Images, *in* the Proceedings of International Symposium on Cyber Worlds: Theories and Practice, Tokyo, Japan, Nov. 2002, pp.230-237.

[2] M. Naor and A. Shamir, Visual cryptography. Advances in Cryptology EUROCRYPT '94. Lecture Notes in Computer Science, (950):1–12, 1995

[3] C. Chang, C. Tsai, and T. Chen, A new scheme for sharing secret color images in computer network. In the Proceedings of International Conference on Parallel and Distributed Systems, pages 21–27, July 2000.

[4] E. Verheul and H. V. Tilborg., Constructions and properties ofk out of n visual secret sharing schemes. Designs, Codes and Cryptography, 11(2):179–196, 1997.

[5] C. Yang and C. Laih., New colored visual secret sharing schemes. Designs, Codes and Cryptography, 20:325–335,2000.

[6] R.L. Lagendijk and J. Biemond, Iterative Identification and Restoration of Images. Norwell, MA: Kluwer Academic Publishers, 1991.