International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Secret Hiding Using Visual Cryptography

Rahul Gupta

Marathwada Institute of Technology, Department of Electronics & Communication Engg., Mundka, Delhi – 110041

Abstract: ***Visual Cryptography is the technique in which secret images or visual text are encrypted or hided in a manner such that only human visual system can decrypt the hided images or text without any help of cryptographic computations or algorithms. The human visual system can decode the secret image when all the shared cover images are stacked together. In this paper, we recover the color secret image from multiple cover images using Chang's and Yu visual cryptography scheme. This scheme gives lossless recovery and reduced noise. Also cryptographic computation complexity is very less.***

Keywords: Cryptography, Visual Cryptography, secret hiding, camouflage images

1. Introduction

Cryptography is the technique by which we can convert the data or information which we have to store or transmit into a particular form. This information can be read and processed by those to whom it is intended. Visual Cryptography is the technique in which the information is in visual form (images, video, etc) and the encrypted text or cipher text can be decoded by human visual system. There is no requirement of any cryptographic computations. Here the secret image which is to be transmitted is hidden in multiple images called shares or cover images. It can only be recovered when all the shares are combined together so that all the pixels are properly aligned. To achieve it, generally we use 2 out of 2 scheme, in which the secret image is hidden between two cover images. To recover the image, both cover images are needed. After that an improved scheme came which is called k out of n scheme, in which the secret image is hidden between n images, but only k shares are needed to decode the image where k≤ n. If k-1 shares are presented, we will get no information about the secret image. Earlier, this idea was applied by Naor and Shamir on black & white images only [2]. Few years later, Verheul&Tilborg applied this idea on color images. But it is not quite successful because the shares used are meaningless and the recovered plaintext is bad. Some advanced versions of this idea are also used in which secret image is hidden between multiple meaningful color images. In 2000, Chang introduced a new scheme for colored secret image sharing and hiding[3], in which the earlier and basic stacking operation of subpixels and interrelations of rows is modified. It can be easily used in real world applications. This scheme uses Color Index Table (CIT) to lossless recover the image. CIT requires space for storage and time to observe & analysis of the table. If number of colors increases in secret image, CIT becomes bigger and big loss of resolution occurs in the camouflage images due to bad pixel expansion factor.

Chang and Yu gives an advanced idea for hiding a colored imaged into multiple cover images without the requirements of a CIT. This technique recovers whole secret image without any loss but the produced shares contain very large noise. This paper presents an advanced scheme based on Chang's technique in order to improve the quality of the cover images with lossless recovery and without increasing the computational complexity of the algorithm.[1]

2. Related Work

The first visual cryptographic technique was pioneered by Moni Naor and Ad Shamir in1994. It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. Practically this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares revealed no information about the original image. In 1995 Naor and Shamir gives a new cryptographic scheme in which the human visual system decodes the encrypted text. There is no need to do any complex cryptographic computation to decode the text.They gave the idea to hide a secret visual message in different images called shares or cover images. It can only be recovered when all the shares are combined together so that all the pixels are properly aligned. To achieve it, generally we use 2 out of 2 scheme, in which the secret image is hidden between two cover images. To recover the image, both cover images are needed. After that an improved scheme came which is called k out of n scheme, in which the secret image is hidden between n images, but only k shares are needed to decode the image where k ≤ n. If k-1 shares are presented, we will get no information about the secret image. Few years later, Verheul&Tilborg applied this idea on color images. But it is not quite successful because the shares used are meaningless and the recovered plaintext is badIn 2000, Chang introduced a new scheme for colored secret image sharing and hiding, in which the earlier and basic stacking operation of subpixels and interrelations of rows is modified. It can be easily used in real world applications. This scheme uses Color Index Table (CIT) to lossless recover the image. CIT requires space for storage and time to observe & analysis of the table. If number of colors increases in secret image, CIT becomes bigger and big loss of resolution occurs in the camouflage images due to bad pixel expansion factor.[1][6]

3. Methodology

The methodology used here is given by Chang and Yu in 2000 [3].We take a gray image having 256 colors keeps a secret for hiding. We represent every color with 8-bit binary vector. Our main aim is to divide each colored pixel into p sub pixels and put them into q shares. In this scheme we use p=9 as aa factor of expansion. We can represent the resulting

structure of a pixel by a qx9 Boolean matrix S= [Sij] where ($1 \le i \le q$, $1 \le j \le 9$) and Rij =1, if and only if, the jth sub pixel in the ith share has a non-white color. The color of the original secret pixel can be recovered by applying an "XOR" operation on the stacked rows of the q shares.[1][6]

3.1 Hiding Algorithm

The idea of algorithm used here is proposed from the scheme used by Chang and Yu in 2000 and 2002 [1][3], further used by R.Youmaran, A. Adler, A. Miri which was published in 23rd Biennial Symposium on Communications [6]. For a 2 out of 2 scheme, the construction of scheme can be described by a collection of 2x9 matrices C. If a pixel with color L and O^2HL of size HxL [3][6].

- Scan through I_{HL} and convert each pixel I_{ij} to an 8-bit binary string denoted as k= $k_1, k_2, \ldots k_8$)
- 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^1p, arrange the row "i" in S as a 3x3 block B^1p and fill the subpixels valued "1" with color k^1p. Do the same for O^2 and construct B^2p. The resulting blocks B^1p and B^2p are the sub pixels of p^{th} pixel after the expansion.
- After processing block B^1p and fill the subpixels valued "1" with the color k^1p
- Do the all the pixels in I_{HL}, two camouflage colored images $O^{1'}$ and $O^{2'}$ are generated. In order to losslessly recover I_{HL}, both $O^{1'}$ and $O^{2'}$ as well as a sequence of random bits R={$r_1, r_2, \ldots, r_{|l|}$}are needed.
- This process is repeated for all pixels in I_{HL} to construct both camouflage images $O^{1'}$ and $O^{2'}$[3][6].

3.2 Recovering Algorithm

k=($k_1,k_2,\ldots k_8$) 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:

$k_i = S_{1j}$ ex-or S_{2j} (1)

where$k_i = S_{1j}$ ex-or S_{2j} and

j= i if i<r & i+1 if i>r

Remember that the number of 1's in the first row of S must be greater than the number of 0's by one.[1][6]

Steps of the Algorithm

- First a colored secret image I_{HL} of size HxL is taken and choose any two arbitrary cover images O^1H

1) 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
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^1r and V^2r from both camouflage images $O^{1'}$and $O^{2'}$, respectively[3][6].
- Re-arrange V^1r and V^2r 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 function corresponding to equation (1).
- Recover k_p, the first pixel in I_{HL}.
- Repeat for all 3x3 blocks in $O^{1'}$and $O^{2'}$.

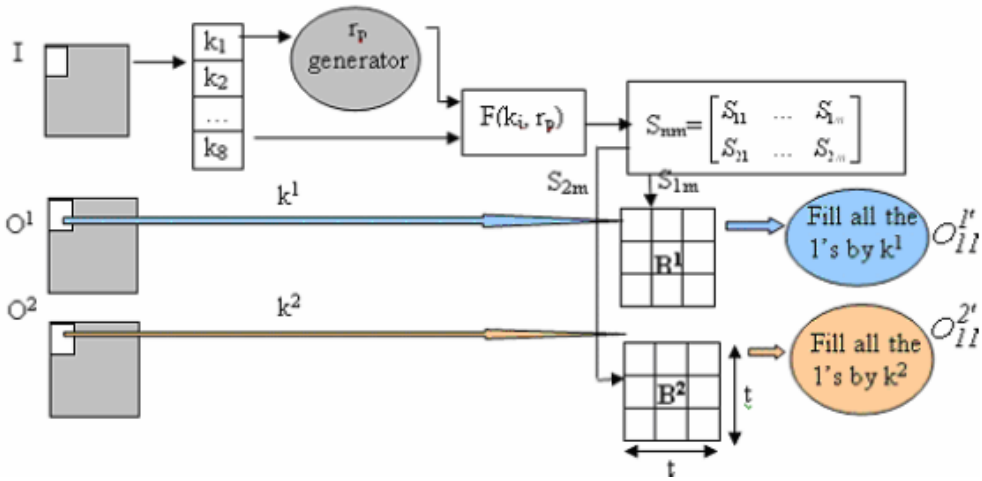

Figure 1: Chang's and Yu's Secret sharing algorithm flowchart

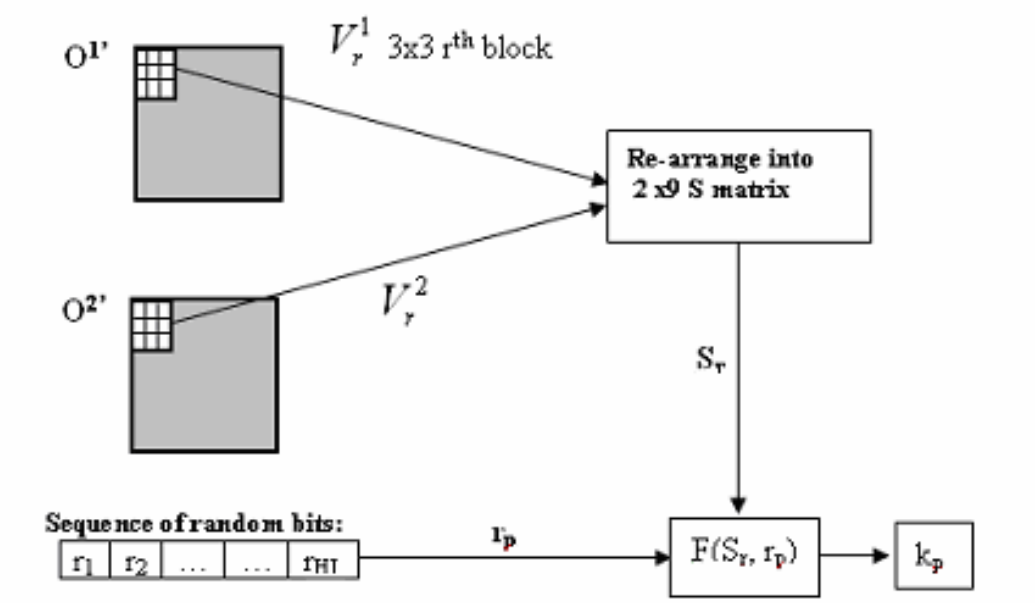

Figure 2: Chang's and Yu's recovery algorithm

3.3 Improved image generation scheme

In this section, algorithm to generate better quality camouflage images is given. This scheme was used by R.Youmaran, A. Adler, A. Miri in Improved Visual Cryptographic Scheme For Secret Hiding [6]. Most of the modifications are applied to the subpixel expansion block described in the next section.

3.3.1 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 S0, S1 by values corresponding to k1-1 in B1 and k2-1 in B2 (Figure 3) instead of leaving them transparent. Also, adjust all pixel values to be between 0-255[3,6].

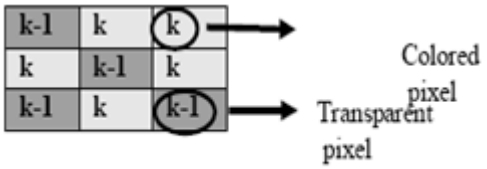

Figure 3: Improved block subpixel expansion technique

3.3.2 Decryption algorithm

To recover the secret image, both camouflage images $O^{1'}$, $O^{2'}$ and the string of random bits R are required [6].

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 k1 and the k1-1 colors previously encrypted
- Count the number of k and k-1 pixels in the processed vector, denoted as countk-1, countk, respectively.
- If countk-1 <countk, the transparent pixel is color k-1, otherwise, set it to k
- Use the k1 and k2 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.

4. Comparison with Other Related Work

The algorithm here we applied was used by R.Youmaran, A. Adler, A. Miri, in Improved Visual Cryptographic Scheme For Secret Hiding[6].This algorithm is better than algorithm applied by Naor and Shamir in 1994 [2][6], as it can be used for hiding color secret images. Also it improves subpixel expansion factor and gives better quality reconstructed images[3,6].

5. Simulation Performed

In this algorithm, simulations are performed using software MATLAB 2013. A 95x100 color secret image is hidden between two 80x80 color cover images. The camouflage images obtained having lot of noise and poor resolution, but the recovery is lossless and color cover images are meaningful. In improved algorithm, the noise is considerably reduced and resolution is improved [6].

6. Simulation Results

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

7. Conclusion

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) 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. 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 of k 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.Youmaran, A. Adler, A. Miri, An Improved Visual Cryptographic Scheme For Secret Hiding: School of Information Technology and Engineering (SITE), University of Ottawa, Ontario, Canada.

Author Profile

Rahul Gupta received the B,Tech degree in Electronics & Communication Engineering from Guru Gobind Singh Indraprastha University, Delhi in 2010. He also completed Diploma in Electronics & Communication Engineering from Board of Technical Education, Delhi in 2007. He is now pursuing in M.tech final year in Electronics & Communication Engineering from Guru Gobind Singh Indraprastha University, Delhi. He is working as a Lecturer in Marathwada Institute of Technology, Delhi in Electronics & Communication Engineering Department.