Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.263 – 268

RESEARCH ARTICLE

An Implementation of a Novel Secret Image Sharing Algorithm

Shanu Sharma[1]

[1]Assistant Professor, Computer Science & Engineering Department, Amity School of Engineering & Technology, Amity University, Noida, Uttar Pradesh, India

[1] *shanu.sharma1611@gmail.com*

***Abstract**— Visual Cryptography is a new cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by human, without any decryption algorithm. This paper presents the study of the fundamental scheme of Visual Cryptography technique and proposes a novel method for sharing of images taking into account the untouched aspects with respect to the quality of the final image being received by the receiver. The proposed scheme directly focuses on the level of noise interference that deteriorates the final image obtained after decryption process and in turn changing the quality of the original image. The algorithm proposed suggests a novel method for the removal of noise from the final image and bringing it at par with the original image in terms of quality. The proposed technique includes for variant form of images including black and white, grey scale and coloured images. The Secret sharing (SS), which was initially proposed, encodes a secret into n shares. The secret can only be reconstructed from any k or more shares. Knowledge of k-1 or fewer shares provides absolutely no information about the secret. The algorithm can be applicable for any size of image and can reconstruct the secret image optimally. The proposed scheme includes no matrix multiplication for construction of shares, rather uses matrix addition which reduces the computational complexity. This algorithm is applicable on gray scale, color and binary images.*

Key Terms: - Secret Sharing; Matrix addition; cryptography

I. INTRODUCTION

Now a day's due to rapid development of internet everyone is used to share any information on the internet, however they are unaware that the network on which they are sharing files is secure or not. So information security becomes a very important issue nowadays. In recent years many information security techniques have been developed to protect information from hackers etc, which includes Steganography, Cryptography and other encryption techniques [1].

Steganography techniques can be applied on any type of digital media like text, video, audio or images. Visual cryptography and Secret Image Sharing is a cryptography technique used for encrypting the visual information like written materials, textual images, and handwritten notes etc. in secure way in which the decryption can be performed by human visual system without using any decryption algorithm. Following types of Visual Cryptography Schemes (VCS) are present [2].

(2, 2) – Threshold VCS: This is a simplest threshold scheme that takes a secret image and encrypts it into two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

(2, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.

(n, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that only when all n of the shares are combined will the secret image be revealed. The user will be prompted for n, the number of participants.

(k, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the threshold, and n, the number of participants.

The extension of Visual cryptography technique is further explained in next section.

II. LITERATURE REVIEW

Secret Sharing (SS) scheme is a method of sharing a secret among group of participants, The secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own. it was first proposed by Blakley [10] and Shamir [11]. It involved breaking up the image into n shares so that only someone with all n shares or some specified k shares could decrypt the image by overlaying each of the shares over each other. The Secret Sharing Scheme can be defined as follows:

A secret sharing scheme is a mean for n participants carry shares or parts si of a secret message s, where i is one to n. The basic idea is to split a secret message s into n shares, such that for any k shares determine the message s, where k (n and k is used as a threshold. The scheme can be defined as follows [1][3]:

1. Given any k or more out of n shares, it is easy to reconstruct a given secret s.

2. If a dishonest participant has only knowledge of any k-1 or fewer shares, then there is no information about the secrets can be determined

When k=n , it is called (n,n) secret sharing scheme.

According to different reconstruction approaches applied to the image in Secret Image Sharing (SIS) schemes, the existing SIS schemes can be divided into three categories [8].

The category I used the traditional SS schemes to share images by treating each pixel to be a value. They can reconstruct the secret image precisely, however, the complexity is quite high. Computational complexity of (n, n) scheme is $O(n\log^2 n)$.

The category II is visual secret sharing (VSS) schemes, proposed by Naor and Shamir [9]. This approach utilizes the human visual system to recover the secret image and requires little or no computation.

The category III utilizes XOR operation to recover the secret image, which was proposed by Tuyls. Tuyls proposed (n, n) scheme for binary images with no pixel expansion and precisely reconstructed image. Yi presented two (n, n) schemes for color image [3]. The schemes also have no pixel expansion; however the secret image was not precisely reconstructed with contrast 1/4. Wang proposed (n, n) scheme for grayscale image[4]. The scheme has no pixel expansion and gives an exact reconstruction. All schemes in are constructed based on Boolean operation, which need bit-wise operation when sharing grayscale and color images [5][6][7].

In this paper an algorithm is presented in which a secret image is encoded into N shares printed on transparencies. The shares appear random and contain no decipherable information about the underlying secret image, however if any 2 of the shares are stacked on top of one another the secret image becomes decipherable by the human eye.

III. DESIGN AND IMPLEMENTATION

A. Features of the Proposed System

- To guarantee the security of information and to reduce the possibility of secret inaccessible due to trouble or duplicity,
- To overcome the disadvantages of pixel expansion and low contrast in existing algorithms.
- To make sharing data process more resource friendly with respect to computing power availability.
- To develop secret sharing scheme with low computation complexity and high contrast is worth to study.
- To reduce the computational complexity.
- To cater the noise interference issue involved in sharing of images.

B. Design

1) Software Requirements

Mat lab 7.0

2) Hardware Requirements

- Processor: Intel Pentium 4-1.3GHz or faster or AMD
- Ram: 512 MB DDR-Win XP, 2GB DDR- Vista Business or Vista Ultimate
- Hard Drive : 1GB or more
- Memory : Minimum 512 MB
- Monitor: Any standard monitor

C. Implementation

Basic visual cryptography is based on breaking of pixels into some sub-pixels or we can say expansion of pixels.

- Every pixel from the secret image is encoded into multiple sub-pixels in each share image using a matrix to determine the color of the pixels.
-
- *1) Binary Secret Image Sharing Method:* A binary image described in Fig 1. is an image that has only two possible values for each pixel. Typically the two colors used for a binary image are black and white. Each pixel is stored as a single bit 1 or 0. For binary image, in order to use the proposed scheme, the grayscale level (k) should be taken as 2. The rest of the procedure is same for construction of shares and revealing phase to recover the secret image.

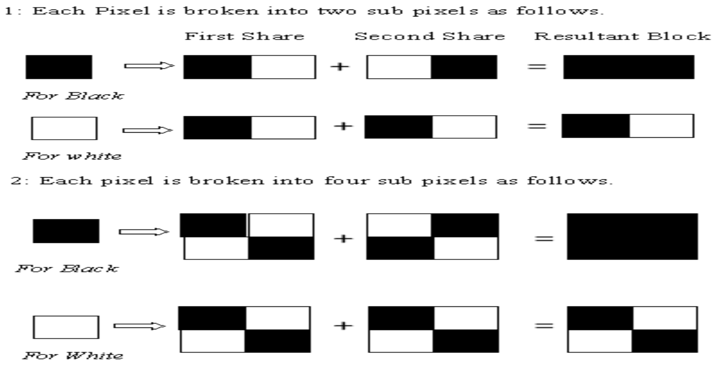
1: Each Pixel is broken into two sub pixels as follows.
First Share
Second Share
Resultant Block
For Black
For white
2: Each pixel is broken into four sub pixels as follows.
For Black
For White

Fig. 1 Fundamental Concepts of binary Image

Sharing Process

- Successively take the pixels of a binary image of h x w dimension.
- For every pixel, determine whether it is black or white.
- Now for every pixel, we use a random function to choose a set of pixels from the codebook which gives two set of pixels for every chosen pixel, one corresponding to share-1 while other corresponding to share-2 of the image. At the end of this step, two shares of size h x 2w are generated.

Reconstruction Process

- Collect both the shared images to reconstruct the original binary image.
- Taking the corresponding pixels from both the shared images we generate a new pixel by performing the following operation:

$$\sim (A+B)$$

Where, A is the pixel from share-1,B is the pixel from share-2, + represents the binary OR operation, and ~ represents the binary negation (NOT) operation[2].

2) Grayscale Secret Image Sharing Method: The process of share construction phase and image reconstruction phase of secret image sharing scheme for grayscale image are as follows[7]:

Share construction:

- get scrambled image PA by using a key to generate a permutation sequence to permute the pixels of A.
- generate n-1 random matrices R_1,……,R_{n-1}, each of which has size h x w and element be {0,…..,k-1} for an image with k grayscale levels.
- compute R_n = (kJ - R_1 -…….- R_{n-1})mod k, where J is unit matrix with size hxw.
- compute S_i = (Ri + PA)mod k, where " + " means matrix addition and i ϵ {1,….,n-1}.
- compute S_n = (Rn + kJ - (n-2)PA)mod k, where " - " means matrix subtraction.

Image Reconstruction:

- PA'= (S_1 +….+ S_n)mod k.
- apply inverse-scrambling operation to PA' to get the reconstructed image A'.

3). Color Secret Image Sharing Method: For color image, any desired colors can be obtained by mixing primitive colors red (R), green (G) and blue (B). In true color system, R, G and B are respectively represented by 8 bits which can represent 0-255 variation of scale. To extend the proposed schemes for grayscale image to color image, three steps are needed [4]. Firstly, decompose the color image into three components of R, G and B, each of which can be seen as grayscale image. Then perform the proposed scheme for grayscale image to each component R, G and B. Finally, compose R, G and B components to generate shares. In the revealing phase, again take the decomposed RGB components of the shares and perform the proposed scheme separately. Finally merge the generated RGB components to recover the secret image.

IV. Experimental Results

Fig 2. Shows results of experiments performed on binary image. It shows the original secret image in binary form and two shares generated from the image and the final reconstructed image from those two shares

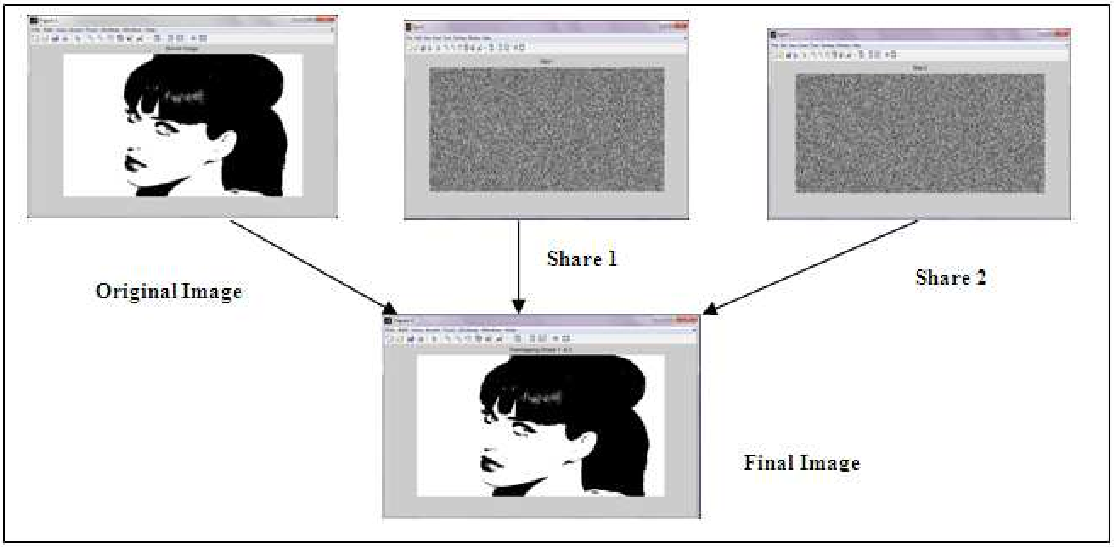

Fig 2. Image sharing scheme in binary secret image

Fig 3. Shows results of experiments performed on gray scale image. It shows the original secret image in binary form and two shares generated from the image and the final reconstructed image from those two shares.

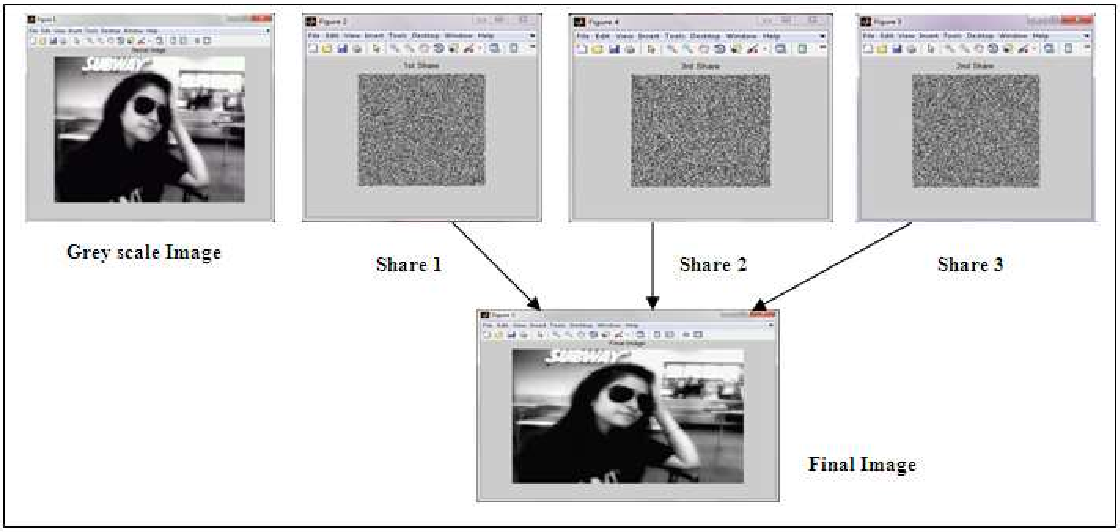

Fig 3. Image sharing scheme in Grayscale secret image

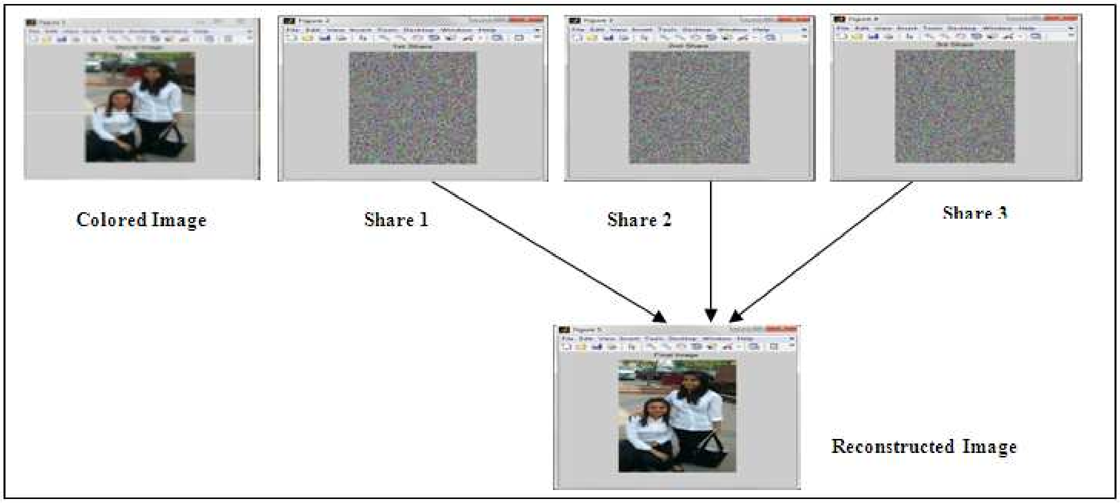

Fig 4. Image sharing scheme in color secret image

Similarly Fig 4. Shows results of experiments performed on color scale image. It shows the original secret image in binary form and two shares generated from the image and the final reconstructed image from those two shares.

V. CONCLUSION

Visual Cryptography technique is used to protect image-based secret information. This paper proposes a novel visual secret sharing scheme for any type of images and directly focuses on the level of noise interference that deteriorates the final image obtained after decryption process and suggests a novel method for the removal of noise from the final image and bringing it at par with the original image in terms of quality. The proposed technique divides an image into n number of shares which are then sent through different communication channels from sender to receiver so that the probability of getting sufficient shares by the intruder minimizes. But the distorted shares may arise suspicion to the hacker's mind that some secret information is passed. The original image can be encrypted using a key to provide more security to this algorithm. The key may be a text or a small image. Steganography can be used by enveloping the secret shares within apparently innocent covers of digital picture. This technique is more effective in providing security from illicit attacks.

REFERENCES

[1] Bhaskar Mondal, Deep Sinha, Navin Kumar Gupta, Nishant Kumar and Pankaj Goyal, "An Optimal (n,n) Secret Image sharing Scheme", UACEE International Journal of Computer Science and its Applications Volume 2: Issue 3, 2012, pp 61-66.

[2] Lin Dong, Min Ku, “Novel (n,n) secret image sharing scheme based on addition,” Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010, iih-msp, pp.583-586.

[3] F. Yi, D.S. Wang, P. Luo, Y.q. Dai, “Two new color (n, n)-secret sharing schemes,” Journal on Communications (Chinese), vol.28(5), 2007,pp.30-35.

[4] R. Z. Wang, C. H. Su, “Secret image sharing with smaller shadow images,” Pattern Recognition, vol.27,2006, pp.551-555.

[5] S. Cimato, R. De Prisco, A. De Santis, “Optimal colored threshold visual cryptography schemes,” Designs Codes and Cryptography, vol.35(3), 2005, pp. 311–335.

[6] P. Tuyls, H.D.L. Hollmann, J.H.van Lint, L. Tolhuizen, “Xor-based visual cryptography Schemes,” Designs Codes and Cryptography, vol.37, 2005, pp.169–186.

[7] M. Iwamoto, H. Yamamoto, “The optimal n-out of-n visual secret sharing scheme for gray-scale images,” IEICE Trans. Fundam. E85-A(10) , 2002, pp.2238–2247.

[8] C. C. Thien, J. C. Lin, “Secret image sharing, ” Computers and Graphics, vol.26(5) , 2002, pp.765-770.

[9] M. Naor, A. Shamir, “Visual cryptography,” Advances in Cryptology-EUROCRYPTO’94, Springer-Verlag, vol.950, 1995, pp.1-12.

[10] G. R. Blakley, “Safeguarding cryptographic keys,” Proc. AFIPS NCC, vol.48, 1979, pp.313-317.

[11] A.Shamir, “How to share a secret,” Commun. ACM, vol.22 (11) , 1979, pp.612-613.