Pseudo - Randomized Visual Cryptography Algorithm for Visual Information Security in grey scale image

Sudipta Chakraborty, Sunanda S Rao, Swathi S Raikar, Trishla Thakur, Mrs. Anitha Suresh

Abstract— **'Visual cryptography' means providing security to the cover image, cover image is divided into 'n' shares, and stacking back of 'n' shares will give the image back. 'Pseudo-randomization algorithm' is used to generate these two shares using two random numbers. These shares are just noise like images which do not reveal any secret information. Using this encryption algorithm we provide security to the cover image. For the decryption, we perform simple computation to get back our original image. As an extension the decryption part is also carried out in VHDL. So that in future this can be implemented using hardware.**

I. INTRODUCTION

As technology progresses, the transmission of personnel digitized data through the network is rapidly increasing. Therefore there is more emphasis required on data security. Encryption methods usually provide information security. Moni Naor and Adi Shamir introduced the concept of visual cryptography (VC) in 1994 [1], which requires no complex computations except human visual system (HVC) for the decryption. They proposed a basic (2, 2) (VC) visual cryptography scheme that encrypts a secret image into 2 shares, and decrypting the secret image by stacking the 2 shares[2]. The main advantage of visual cryptography scheme is that it decrypts the secret image just by stacking the shares and no other complex computations are required. It reads the secret information from stacking the shares, thereby removing the need for complex computation which is the main drawback of traditional cryptography.

The model for visual cryptography given by Naor& Shamir is as follows: A page of cipher text and a printed transparency is secret key. The original text is revealed by placing transparency with key over the ciphered text page, though they are indistinguishable from random noise. The visual secret model sharing is as follows[3]: The secret image is split up into number of shares and transmitted to the number of Participants. A visual secret sharing scheme is a technique used to encrypt the secret image by splitting the shares into several random shares and distribute it among the participant.

Manuscript received May 18, 2015

Sudipta Chakraborty, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

Sunanda S Rao, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

Swathi S Raikar, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

Trishla Thakur, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

Mrs. Anitha Suresh, Associate Professor, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

A set of qualified participants would be able to retrieve or recover the secret image by overlapping or just by stacking the shares.

A traditional VC takes the secret image as the input and number of shares as the output, it also has to satisfies two important conditions 1) secret images can be recovered by any qualified subset of the shares; 2) any forbidden subset of shares cannot gain any kind of information about the secret image. For example, In traditional visualcryptography (k,n)-VC, the secret image is revealed if k of n shares are known if not any number of n shares less than k is not sufficient to reveal secret image where, k is the number of participants and n is the number of shares This ensures that the secret picture is viewed as a set of black and white pixels with each pixel being handled separately.

Visual cryptography is now a days regularly used for image encryption. Encryption starts with the use of secret sharing concepts where the secret image is split into shares which are random indistinguishable noise-like and secure images. These images are then transmitted or distributed over an entrusted or insecure transmission channel.

II. ENCRYPTION AND DECRYPTION METHOD IN MATLAB

Encryption algorithm

Step 1. Start
Step 2. Generate two keys
Step 3. Read the input image
Step 4. If the input image is coloured,convert it to gray scaled image
Step 5. Create two shares of the same size as the input image
Step 6. Using Jarvis halftone function ,the gray scaled image is converted to a halftone image
% inImg - Input Gray Image
% outImg - Output Halftone Image

% function outImg = jarvisHalftone (inImg)

Using all these function we will do conversion
Step 7. This halftone image is then preprocessed to get the preprocessed image
Step 8. The pseudo randomized cryptographic algorithm is applied to the above image

Pseudo randomised cryptographic algorithm working is as shown,
Step 1. Considered Pixel Sij with position i and j
Step 2. Apply pixel reversal i.e. Sij' = 255 – Sij.
Step 3. Use pseudo - random number generator,which generates values between or equal to (0.1 to 0.9) to reduce Sij' to sij'' (i.e. Sij'' = 255 – Sij')

Step 4. Take the difference of Sij'' with original pixel which is Sij.

Step 5. Use pseudo-random number generator is used to reduced Sij''' .

Step 6. Now apply pixel reversal (255 – Sij''')

Step 7. obtain share 1.

Step 8. Take the difference between two random number generators with original pixel Sij.

Step 9. Apply again pixel reversal

Step 10. obtain share 2.

Step 11. Repeat point 1 to 10 for all the pixels from original image

Decryption algorithm

Step 1. Generate matrix of random number between 0.1 to 0.9 based on the key using twister function

Step 2. Combine the two shares using a mathematical formula comprising of two shares and random number

Step 3. The output image matrix will be in double format.

Step 4. To avoid the truncation of decimal values it is changed from double to uint8(unsigned integer) format.

Step 5. Post processing is carried out in the same way as preprocessing,to obtain the decrypted image

Decryption in VHDL

Algorithm

Step 1: input the pixel values of the two share images S1,S2 and the random number R1 from the MATLAB code.

Step 2: calculate pixel values by using the equation

$$S=(510-S1-S2+(255\times R1))(1+R1)$$

Step3: simulate the result using ModelSim

Step 4: obtain the output values (S)

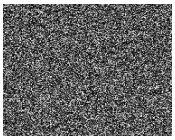
Step 5: using the obtained values(s) from VHDL ,get the pixel values from MATLAB code

Step 6: compare the pixel values obtained through decryption in MATLAB code and the pixel values from **step 5**.

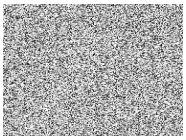
SNAPSHOTS OF RESULTS

1

2



3



4

5

6

In these figures, fig 1 represents the original grey scale image. Fig 2 represents the half-tone image obtained by 'Jarvis half-tone' algorithm. Following the pseudo-randomization algorithm two noise like images are obtained. These are called as shares.(fig 3,4). Fig 5 represents the combined shares image obtained from simple computation. And finally fig 6, is the final tuned image after removal of noise.

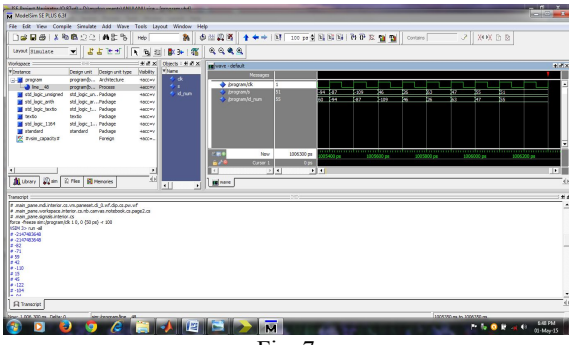


Fig. 7

Fig 7 spcifies the transcript values obtained from Modelsim. We verify the values obtained from Modelsim to that obtained from MATLAB.

CONCLUSION

It is seen that the (2, 2) pseudo - randomized cryptography which generates shares pixels, based on pixel reversal, random reduction in original pixel and subtractions of the original pixel. The original secret image is divided so that it reveals the secret image after OR operation of qualified shares. The proposed scheme reveals reduced pixel expansion, required for retrieval of the image.

As the memory space required for an image is very vast, we cannot use a normal 128*128 size of an image in VHDL. Hence we have reduced the size of an image to the minimum. We have rounded-off the values (specifically the random number values) obtained from MATLAB. Hence this affects the resolution of the image. As MATLAB and VHDL tools use different environment, it is observed that as the pixel size increases there is more of noise and the image obtained by using VHDL code is corrupted. Hence for pixel comparison we have considered 64 pixel values generated by both codes. It was observed that the pixel values were almost same in both cases. The proposed schemes revealed good security due to its randomness.

REFERENCES

[1] M. Nair and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT" 94, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.

[2] Information Hiding in Gray Scale Images using Pseudo - Randomized Visual Cryptography Algorithm for Visual Information Security

[3] Ch.Ratna Babu Dept.of C.S.E R.V.R. & J.C College of Engg., Guntur, India.

[4] M.Sridhar Dept.of Computer Applications R.V.R. & J.C College of Engg., Guntur, India.

[5] Dr. B.Raveendra Babu Dept.of C.S.E VNR VJIET Hyderabad, India.

[6] International Journal of Computer Applications (0975 – 8887) Volume 92 – No.8, April 2014 11 Visual Cryptography Schemes for Secret Image Sharing using GAS Algorithm Bharanivendhan N Department of computer science Dhanalakshmi College of Engineering Chennai, India Amitha T, Ph. D Department of computer science Dhanalakshmi College of Engineering Chennai, India.