ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)
International Conference on Recent Trends in Computing and Communication (ICRTCC 2015)
Cochin College of Engineering & Technology
Vol. 4, Special Issue 1, June 2015

Non-Expanded Share Generation Algorithm using RGVSS

Shyni T S[1], Anusree L[2]

M.Tech Scholar, Electronics and Communication Engineering Department, LBSITW, Trivandrum, India [1]

Assistant Professor, Applied Electronics and Instrumentation Engineering Department, LBSITW, Trivandrum, India [2]

Abstract: This paper presents a new algorithm for non-expanded share generation using RGVSS. In random grid visual cryptography scheme each pixel is treated as a grid. In probability based RGVSS the black appearing probability of each pixel with respect to cover image is used to generate non-expanded meaningful shares. The proposed method is modified form of probability based RGVSS. Here thresholding is applied to each of the blank shares to reveal its content. On overlapping blank shares the secret image is revealed. This will generate high contrast non-expanded shares which give almost perfect reconstruction of secret image.

Keywords: High contrast shares, Non-expanded shares, Random grids, Visual cryptography.

I. INTRODUCTION

Communication of secret images and texts through any communication channel requires additional methods to ensure security. The basic method used for communication of secret data is encryption. Here generally an encryption key is used and same key is required for decryption. The secrecy of communication lies in how safely the key is kept. Once the key is lost, it will become easy for the unauthorized user to access secret image.

To overcome this problem M. Naor and A. Shamir[6] proposed basic visual cryptography scheme. In visual cryptography the secret image is divided into multiple shares where each share does not convey any information individually. At the receiver side when these shares are overlapped the secret image is revealed. In (n,k) visual cryptography where $k \leq n$, the secret image is divided into n shares and to retrieve the secret image back at the receiver side only k shares are required. On overlapping k-1 shares no information is revealed.

Main disadvantage of this method is pixel expansion. As multiple pixels are used in shares to represent each of the secret image pixels, the size of shares will be greater than the secret image. Low contrast of stack image is another problem in this method. This results from the fact that white pixels in secret image can be represented in stack image only by using combination of black and white pixels.

Thus contrast of stack image decreased to 50%.The concept of basic (2,2) visual cryptography proposed by Naor and Shamir is shown in table I. To represent each pixel in secret image, two pixels are used in each share. For generating black pixel on stacking, share1 and share2 will have opposite combination of black white pixels. On stacking these shares two black pixels are obtained. On the other hand for generating white pixel in stack image both share 1 and share 2 use same combination of black and white pixels. On stacking these two shares one black pixel and one white pixel is generated.

Thus perfect reconstruction of white pixel is not possible. The white pixel in stack image will have only 50% contrast. This method is not preferred much as it suffers from pixel expansion problem. Corresponding to each pixel on secret image, the stack image will have two pixels. Hence size of stack image is twice that of secret image.

In order to overcome pixel expansion problem in conventional visual cryptography scheme several methods were proposed. R. Ito H. Kuwakado, and H. Tanaka [7] and C N Yang [4] used concept of probability to generate shares without pixel expansion. But due to random nature of probability, shares have low visual quality. Karfi and Keren [5] proposed random grid visual secret sharing scheme for generating non-expanded shares.

Encrypting images using random grid method completely eliminates pixel expansion problem and generate noise like shares. To avoid share management problem Chen and Tsao [2] developed user friendly random grid visual secret sharing scheme which generates meaningful shares without pixel expansion. But this method can only generate stack image with low contrast.

Later, as a solution to all problems in visual cryptographic encryption Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin [1] proposed new random grid based visual secret sharing method using probability concept. This paper proposes a modified form of Young-Chang Hou's method to generate non-expanded user friendly shares. Here black and white areas in secret image are perfectly reconstructed.

This paper is structured as follows. Section II discusses basic concept of random grid visual cryptography and probability based RGVSS is discussed in section III. Proposed method is explained in section IV and the experimental result of this method is given in section V. Finally conclusion is given in section VI.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)
International Conference on Recent Trends in Computing and Communication (ICRTCC 2015)
Cochin College of Engineering & Technology
Vol. 4, Special Issue 1, June 2015

TABLE I. CONCEPT OF (2,2) VISUAL CRYPTOGRAPHY SCHEME

Pixel		Step 1
Probability	50% 50%	50% 50% Step 2
Share 1		
Share 2		
Stack image		

II. RANDOM GRID VISUAL CRYPTOGRAPHY

In 1987, Karfi and Keren proposed random grid visual cryptography scheme as a solution to pixel expansion problem in conventional visual cryptography. In random grid visual cryptography each pixel is treated as a grid and the input secret image is transformed into multiple cipher grids which provide no information about the secret image. The main advantage of random grid method is that it provides grids which have same size as the secret image and reveal secret image on overlapping.
In (2,2) random grid method two random grids are generated and stacking these grids the secret image is obtained. Let the secret image I is divided into two grids RG1 and RG2 such that RG1 and RG2 reveal no information on their own. Mainly 3 algorithms are proposed for random grid generation.

A. Algorithm 1

Step 1 RG1 is generated by randomly assigning 0's and 1's
to each pixel. Thus the probability of pixel being black or white is the same and is 1/2.
Step 2 Each pixel in RG2 is generated by looking on to the corresponding pixel in secret image O.
Step2.1 If O(i,j)=0 then
RG2(i,j)=RG1(i,j)
Step2.2 If O(i,j)=1 then
RG2(i,j)= complement of RG1(i,j)

B. Algorithm II

Step 1 RG1 is generated by randomly assigning 0's and 1's
to each pixel. thus the probability of pixel being black or white is the same and is 1/2.
Step 2 Each pixel in RG2 is generated by looking on to the corresponding pixel in secret image O.
Step2.1 If O(i,j)=0 then
RG2(i,j)=RG1(i,j)
Step2.2 If O(i,j)=1 then
RG2(i,j) is generated by randomly assigning o's and 1's to each pixels.

C. Algorithm III

RG1 is generated by randomly assigning 0's and 1's to each pixel.thus the probability of pixel being black or white is the same and is 1/2.
Each pixel in RG2 is generated by looking on to the corresponding pixel in secret image O.
Step2.1 If O(i,j)=0 then
RG2(i,j) is generated by randomly assigning 0's and 1's to each pixels
Step2.2 If O(i,j)=1 then
RG2(i,j)= RG1(i,j)

III.PROBABILITY BASED RGVSS

In probability based RGVSS method proposed by Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin the black appearing probability of share pixels with respect to secret image pixel is used. This black appearing probability is used to control the contrast of both shares and stack image. In order to generate a dark area in share higher black appearing probability is assigned. Like wise to generate a white area in share low black appearing probability is assigned.

A. User friendly visual secret sharing

In user friendly secret sharing scheme the share images are generated in such a way that shares have cover image on them. Thus it will reduce the management problem and shares can be easily handled. There are mainly four probabilities defined in this method, X, Y, Z and W. X is the probability that a pixel in share is black while the pixel in corresponding location in cover image white. Y is the probability that a pixel in share image is black while the corresponding pixel in cover is also black. Obviously Y has greater value than X. In the same way Z, W are also defined for stack image.
When two share images are stacked, the stack image pixels will have different black appearing probabilities given the different color combinations of the two share images. The variations are described below.

1) When the pixel color in the two cover-images is black, each pixel has Y probability to be black. When the black pixels in the two share images are overlapped, the possibilities vary from total overlapping to zero overlapping. Thus the black-pixel-appearing-probability in that area of the stack image will be in between Y and 2Y.

2) When the pixel color in the two cover-images is white, each pixel has X probability to be black. When the black pixels on the two share images are stacked, the possibilities vary from total overlapping to zero overlapping. Thus the black pixel appearing probability in that area of the stack image will be in between X and 2X. When the pixel color in one of the two cover-images is

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)
International Conference on Recent Trends in Computing and Communication (ICRTCC 2015)
Cochin College of Engineering & Technology
Vol. 4, Special Issue 1, June 2015

black and the other is white, then the first pixel has Y probability to be black and the other pixel has X probability to be black. When the black pixel and white pixel on the two share images are stacked, the possibilities vary from total overlapping to zero overlapping. When two share images are stacked, black-appearing-probability in that area of stack image will be in between Y and X + Y.

The ideal values of X and Y are defined as 0.5 and 1.5X since this value gives maximum contrast shares. Z is taken same as Y and W are equal to 2X. These values will give high contrast stack image. The shares are generated by analysing secret image, cover 1, cover 2 pixel combinations and choosing corresponding black appearing probability from user friendly visual secret sharing codebook.

B. Meaningless visual secret sharing scheme.

In meaningless visual secret sharing scheme random noise like shares are generated. Here the contrast between black and white areas in stack image should be visible indicating the secret, but such contrast should not be visible in shares. When the value of probability X is equal to Y the user friendly visual secret sharing code book reduces to meaningless visual secret sharing code book.

Corresponding to each pixel in secret image both share 1 and share 2 will have X percentage of black pixels. When two shares are stacked pixels corresponding to black areas in secret image will have W probability of being black and pixels corresponding to white areas will have Z probability of being black. Thus on overlapping the shares, the secret image with high contrast between black and white areas is generated.

IV. PROPOSED METHOD

Here a new algorithm for non-expanded share generation is proposed. This method utilizes the concept of probability based RGVSS with some modifications. Using this algorithm non-expanded user friendly shares are generated. The main advantage of proposed method is perfect reconstruction of white pixels which is not achieved in probability based RGVSS method.

In this method first secret image is converted to black and white image. Two cover images of size same as that of the secret image is selected and converted to black and white images. These cover images will appear on the shares that are generated later. Thus the user friendly secret sharing is achieved.

To generate share pixel in (i,j)th location the pixels in secret image, cover 1 and cover 2 on the same location is examined. Once the pixel combination is identified the probability of pixel in share image to appear black is determined from the visual secret sharing codebook shown in table II. After encrypting all pixels in this way two blank shares are generated. When these shares are converted to black and white format by applying proper threshold the cover image in both shares are revealed. Thus share management problem is avoided and the scheme becomes user friendly.

On overlapping the two blank shares the secret is not perfectly revealed. To get a stack image same as original secret image thresholding is done. Here threshold value is selected by averaging all pixel values in stack image. On applying this threshold to the stack image, secret image is revealed which is exactly same as the original secret image. Thus a perfect reconstruction of secret data is done via this new algorithm.

ALGORITHM

INPUT: An H×H secret image I, two H×H cover-images C1 and C2, and probability parameters X, Y, Z and W.
OUTPUT: Two H×H share images S1 andS2.

Step 1 Read the pixel color of I(i, j), C1(i, j) and C2(i, j) and identify the combination

Step 2 Based on the combination, appropriate black appearing probability of pixels in S1 and S2 is assigned based on new user friendly secret sharing codebook shown in table II

Step 3 Repeat steps 1 and 2 for all the pixels of I.

Step 4 generated blank shares of size H×H are converted to black and white image by applying proper threshold

Step 5 Xor the blank shares and apply proper threshold to generate secret image.

The same algorithm can be used for meaningless visual secret sharing scheme. Here two meaningful cover images are not required. Instead random noise like images are used as cover images. The same code book can be used for both meaningful and meaningless visual secret sharing. After modifying the cover pixels based on the code book two blank shares are generated. On applying proper threshold to these images random noise like shares are generated.

In general probability based RGVSS method, the generated shares are similar to cover images but white pixels will have only 50% contrast. But the proposed algorithm generates two blank shares. Thus security of this method increased.

V. EXPERIMENTAL RESULTS

The experiments are performed in a personnel computer of 4GB memory using windows 7 platform. The development language was MATLAB. The images used in experiments are shown in fig.1

A. Experiment 1: meaningless share generation using basic visual cryptography

The experimental results are shown in fig. 2. From the results it is clear that the basic visual cryptographic scheme can generate stack image same as secret image but with low contrast of white pixels. The sizes of generated shares are double the size of secret image. Thus the reconstructed image also has double size of secret image.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)
International Conference on Recent Trends in Computing and Communication (ICRTCC 2015)
Cochin College of Engineering & Technology
Vol. 4, Special Issue 1, June 2015

TABLE II. NEW USER FRIENDLY VISUSAL SECRET SHARING CODE BOOK

Secret pixel	Cover 1	Cover 2	Share 1	Share 2
■	■	■	Y	(2*Y-W)/Y
	■	□	Y	(X+Y-W)/Y
	□	■	X	(X+Y-W)/X
	□	□	X	(2*X-W)/X
□	■	■	Y	(2*Y-Z)/Y
	■	□	Y	(X+Y-Z)/Y
	□	■	X	(X+Y-Z)/X
	□	□	X	(2*X-Z)/X

B. Experiment 2: Generation of user friendly, non-expanded shares

The experimental results of new algorithm for user friendly (meaningful) non-expanded share generation using RGVSS is shown in fig. 3

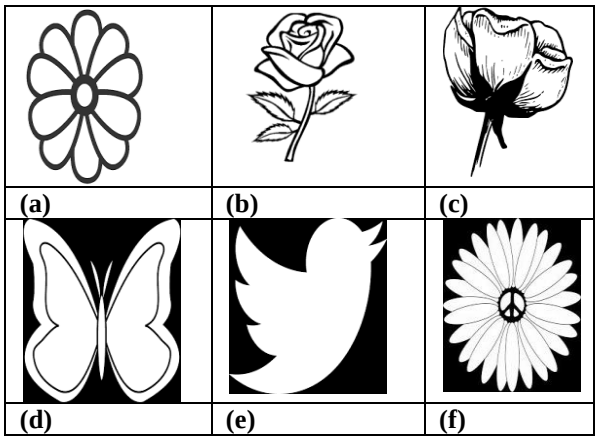

Fig.1 (a)- (f) Experimental images (a)- secret image (b) cover 1 (c) cover 2 (d) secret image (e) cover 1 (f) cover 2(g) secret image (h) cover 1 (i) cover 2.

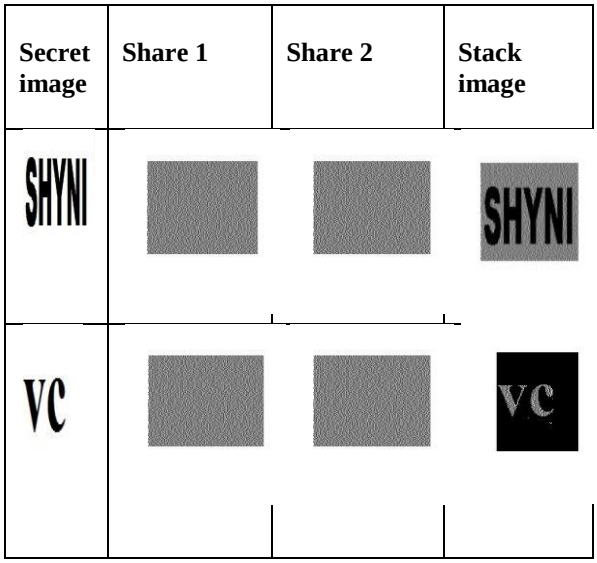

Fig.2. Basic visual cryptography

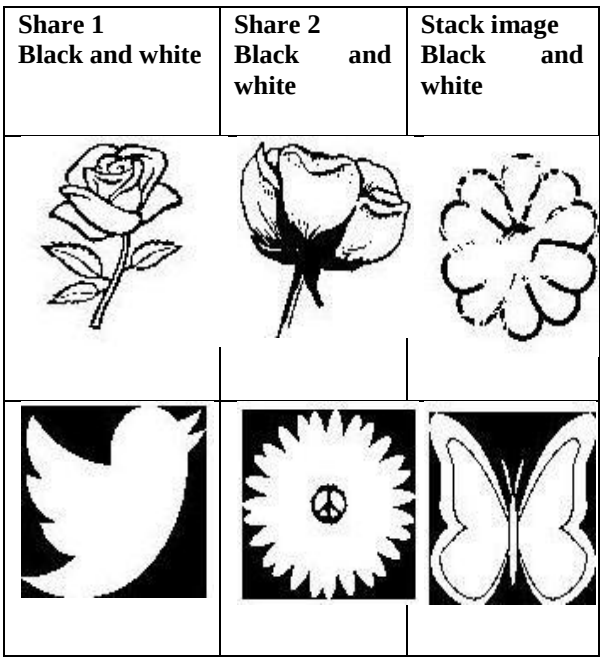

Fig.3. Experimental results of new probability based RGVSS algorithm.

ADVANTAGES

The shares are generated in blank form but when converted to black and white form, cover images are displayed on them. Thus the shares can be used as both meaningless white shares and meaningful shares. In other methods white pixels can't be perfectly reconstructed on stacking. But here both black and white pixels are perfectly reconstructed. Thus perfect reconstruction of secret image is achieved through this method.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)
International Conference on Recent Trends in Computing and Communication (ICRTCC 2015)
Cochin College of Engineering & Technology
Vol. 4, Special Issue 1, June 2015

VI. CONCLUSION

This paper proposes a new method for generation of non-expanded shares using RGVSS. The shares have high contrast and size is equal to that of secret image. When thresholding is applied to the blank shares cover images are revealed. Stacking the blank shares and applying thresholding will give secret image the reconstructed image have only black and white pixel. Low contrast of white pixels in probability based RGVSS method is completely eliminated using this proposed method. Thus this method is perfect solution for generating non-expanded user friendly shares and reconstructing secret image with high contrast.

REFERENCES

[1] Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin "Random-Grid-Based Visual Cryptography Schemes", IEEE transactions on circuits and systems for video technology, vol. 24, no. 5, may 2014
[2] T. H. Chen and K. H. Tsao, "User-friendly random-grid-based visual secret sharing," IEEE Trans. Circuits Syst. Video Technol., vol. 21. no. 11, pp. 1693–1703, Nov. 2011.
[3] T. H. Chen and K. H. Tsao, "Visual secret sharing by random grids revisited," Pattern Recognit., vol. 42, no. 9, pp. 2203–2217, 2009.
[4] C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit. Lett., vol. 25, no. 4, pp. 481–494, 2004
[5] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Opt. Lett., vol. 12, no. 6, pp. 377–379, Jun. 1987
[6] M. Naor and A. Shamir, "Visual cryptography," in Proc. Adv. Cryptology-EUROCRYPT'94, LNCS 950, 1995, pp. 1–12
[7] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Trans. Fund. Electronics, Commun. Computer. Sci., vol. E82-A, no. 10, pp. 2172–2177, 1999

BIOGRAPHIES

Shyni T S received B.Tech in Electronics and Communication Engineering degree from University of Kerala in 2013. At present she is a fourth semester M.Tech student at LBS Institute of Technology for Women, Trivandrum, India.

Anusree L received B. Tech in Applied Electronics and Instrumentation Engineering and M. Tech in Signal Processing from University of Kerala. She is currently working as assistant professor in department of AE&I Engineering at LBSITW, Trivandrum, India.