



A Survey on Random Grid based Cryptography Schemes

Ankita Bhimrao Patkure , Prof. Nikita J. Kulkarni

Computer Department

ZES's Dnyanganga College of Engineering and research,
Narhe, pune-411041

ankitapatkure@rediffmail.com , nikita.kulkarni@zealeducation.com

Abstract— A random grid based non-expanded Visual cryptography scheme used to generate meaningful secret image into n meaningless shares. According this well as meaningless shares. First, analyze the original image is decrypted by human eyes when k or more than k share images are stacked together. The main advantage is that neither any complex computation nor any knowledge about Visual cryptography is needed during decryption process. Visual Cryptography uses a pixel expansion method to decompose the secret image, share image are larger than secret image. The of both secret and stack images to their theoretical maximum. This method is superior to past methods for visual secret sharing.

Keywords—random grids, visual cryptography, meaningful shares, Visual Secret Sharing Scheme, contrast

I. INTRODUCTION

In previous years the people from all over world depends on internet to transmit and share their own information. To protect the data from unauthorized hacking process, people mostly concerned with information security. For security issue people choose for secret data with symmetric and asymmetric cryptography. These cryptography methods supposed to have high computation cost in encryption and decryption process. Hence, many visual secret sharing schemes and random grids schemes were stated where visual secret sharing is an efficient secure method for encryption a secret image by dividing it in meaningful or meaningless shares. Thus it can't leak any information of shared secret image and any decoder can decode it easily by human visual system without using complex computation. The other is Random Grid (RG) scheme which takes an input image and convert it into multiple cipher grids which not provide any information about original image. It has an extra advantage that they require no pixel expansion.

A secret key and any complicated computation is used by traditional cryptography to convert plaintext into encrypted text which make sure confidentiality, security and availability of data transmission over the internet. The biggest main disadvantage is a computer is required for encryption and decryption mechanism which result into extensive execution time and wasted computational resources.



Fig1: General Structure of visual cryptography

Ito et al. [2] and Yang [3] used the concept of probability to understand the meaning of Boolean matrices and proposed a pixel non-expansion method which is suitable for binary image. Tu and Hou [4] adopted Ita's [2] method but utilizes multiple pixel in secret image as unit of encryption. An innocent looking share of invariant size for gray-level secret image was generated by them. A Random Grid Visual Secret Sharing method was proposed by Kafri and Keren [5] in 1987. According to this method every pixel of image is considered as grid, from which random variable used to encrypt the secret image. The great advantage of RGVSS method for encryption is that it generates unexpanded share images.

In RGVSS [5], every pixel of share image is considered as grid. The color of grid is randomly fixed. The color of grid R_1 is first share image is randomly fixed. After R_1 is determined the color of grid R_2 in second share image is either complementary color or same color depending on color of corresponding secret pixel. Each pixel in each share image has same

probability of becoming black and white, making it needed and no pixel expansion problem. When XOR impossible to see secret content from any single decryption is applied, large contrast or better visual share image. If there will be 50 % black pixels with in quality is obtained.

the area that should look white, meaning that the light transmission is $\frac{1}{2}$ and area that should be black fully black i.e. light transmission is 0. When two share images are stacked together. It creates 50% contrast between black and white areas, which is sufficient to see the reconstructed secret image.

II. LITERATURE REVIEW

1. Extended Visual Cryptography [12]

Extended visual cryptography [12] is the type of cryptography. In which reconstruction of secret image by stacking some meaningful shares together. Mostly visual cryptography based on Boolean operation, so that halftoning is necessary when applying visual cryptography on grayscale image.

Let, t is the pixel in the entire region.

$t(x)$ is the transparency within region

So, Average transparency is

$$t_{\Omega} = \frac{\int_{\Omega} t(x) dA}{A\Omega}$$

Equation 1[12]

But average transparency for each target pixel is

$$t_T = \frac{\int_{\Omega} t_1(x).t_2(x)}{A\Omega}$$

Equation 2 [12]

In EVC, on each share cover image is provided to convert meaningless shares into meaningful shares. The trade-off between contrast and security are assessed by observing result of this method

2. Random-grid-based visual secret sharing with abilities of OR and XOR decryption. [6]

Visual cryptography mostly has the pixel expansion problem and has lower visual quality. This pixel expansion problem is solved by probabilistic visual secret sharing and random grid based visual secret sharing (RGVSS). But in probabilistic visual secret sharing codebook are needed in encryption phase this drawback is overcome by RGVSS. XOR based RGVSS [6] is a method to carry out secret sharing via Boolean XOR operation, where reconstructed image has better visual quality. In RGVSS [6], secret image is recovered by stacking sufficient number of shares one to other. The visual quality of recovered image is not competitive because background becomes darker when more shares are stacked together. In XOR based RGVSS, computational

device are needed to perform decryption. Here, (k, n) VSS with capability of OR and XOR decryption [6] problem which can be solved by extended visual method provide ability of stacking and XOR decryption. In EVC scheme, meaningful cover images decryption. Advantage of this method is no codebook are providing over shares which are obtained after

Pixel expansion and visual quality are major problems in VSS. To solve the pixel expansion problem random grid approach is used, which consider share as big as original secret image. Here, Contrast enhanced VSs [8] and void-and-cluster base post processing [8] methods are introduced to improve contrast of reconstructed image. In VAC algorithm, arrays are constructed which works in terms of majority pixel and minority pixel. If less than half pixels are black then they are minority pixels and majority pixels are white. Cluster and void are used for arrangement of minority pixel in background of majority pixel. In homogeneous distribution, minority pixels are added in center of large void and majority pixels are added in center of tight cluster. So, optimal visual quality is obtained by applying contrast enhanced RGVSS and reconstruction of secret image is obtained by VAC based post processing method.

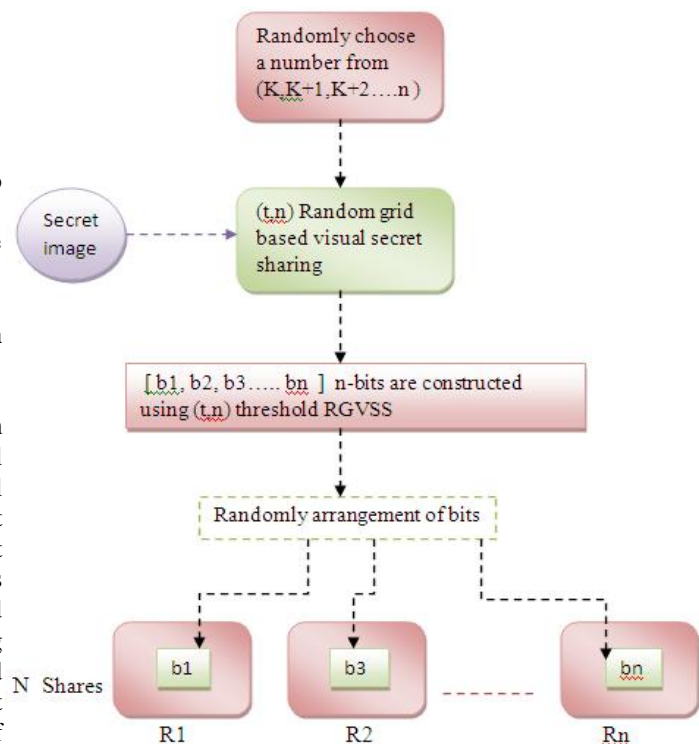


Fig 2: Share construction using novel VSS based Scheme

4) An Extended color Visual Cryptography algorithm for general access structure. [8]

encryption. But EVC scheme also suffer from pixel of secret image, but these contrasts should not be visible expansion problem. This problem is removed by in share image which should represent noise like shares. general access structured method which is applicable. This is obtained by having equal probability of each for color images. This method is introduced in two phases; first phase uses optimization technique for pixel in share image being black, having no regard of constructing meaningless shares. In second phase, whether corresponding color of cover image is black and add cover image over meaningless shares to create white. meaningful shares using stamping algorithm. Benefits of using these methods are as follows as:

Advantage of this method is that no codebook design is required, modularity and another advantage is this method is not only capable for Extended Visual Cryptography scheme but also used in conventional Visual Cryptography.

III METHODS USED IN RANDOM GRID VC

1) USER FRIENDLY VISUAL SECRET SHARING [9]

Using this method each share image is cover image are used in encryption process and it is not covered with the cover images on it. It having two necessary that color of these share images are different probabilities to produce the contrast complementary each other. Using encryption codebook, between the dark and light area in cover image will it is easy to change the probability of appearing black appear black in share image. These different pixel on both share and stack image which proves this probabilities are called A and B, where A represents method is more flexible.

probability of appearing black when pixel in cover

image is white and B represents probability of appearing black when pixel in cover image is black.

Friendly-RGVSS is extends from analyze visual quality. is the parameter. If value of is RGVSS by designing procedure of different light greater then, it having better visual quality. If value if transmission on random grid based on different pixel is less then, it having relatively less contrast.

values on logo (cover) images. In encoding phase, a.

secret image S and logo image M i.e. cover image

both having size $m \times n$, are encoded into two secret sharing method, it is not necessary whether color meaningful shares or random grids G1 and G2 with of cover image black or white. If color of the cover the same size of secret image S. In decoding phase, image is black we have B % of chance to produce black participants simply stack G1 and G2 and secret S is pixel at corresponding position on share image. If color recovered. of cover image is white then it having A % of being

black. In meaningless share image codebook, share problem of pixel expansion and unfriendly image will produce A % of black pixel, having no regard management of meaningful share image. In this, whether secret pixel in corresponding position are black visual quality between meaningful random grids and or white. Hence, no information about secret image is recovered results can be adjusted to be friendlier for disclosed in the share image.

dealer by different value of . FRGVSS have three

advantages: 1) No pixel expansion 2) wide image format 3) having formal proof.

2) Meaningless share images in visual secret sharing [9]

The main part of meaningless share method not only security is provided but pixel expansion image visual secret sharing is that it should be easily problem is also removed. It also produces meaningful understood the contrast between black and white shares which is easy to carry and manage. Encryption is areas in the stack image in indication of the pattern performing on all pixels in the cover image and secret image, which guarantees that visual quality of share and

a. Improved contrast in share and stack images

All pixels of the secret and share image are used for encryption; hence the image produce by user friendly secret sharing is better than the image produced by the method that only takes pixel from the secret image and cover image.

b. Reduction of restriction for encryption process

With user friendly secret sharing, one or more

Visual quality analysis

Here contrast () is used to measure or

Security Analysis

According to codebook of user-friendly

secret sharing method, it is not necessary whether color

image is black we have B % of chance to produce black

of cover image is white then it having A % of being

black. In meaningless share image codebook, share

image will produce A % of black pixel, having no regard

whether secret pixel in corresponding position are black

visual quality between meaningful random grids and or white. Hence, no information about secret image is

recovered results can be adjusted to be friendlier for disclosed in the share image.

IV CONCLUSION

In day to day life, it is important to provide

security to digital information. Since, Visual

Cryptography is one of the techniques used for secret

sharing of images. In this user-friendly secret sharing

method not only security is provided but pixel expansion

problem is also removed. It also produces meaningful

shares which is easy to carry and manage. Encryption is

performing on all pixels in the cover image and secret

image, which guarantees that visual quality of share and

stack image can reach the theoretical maximum.
Also, Encryption method is flexible to use.

V. REFERENCES

1. M. Naor and A. Shamir, "Visual cryptography," in Proc. Adv. Cryptology EUROCRYPT'94, LNCS 950, 1995, pp. 1–12.
2. R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Trans. Fund. Electron, Communication Computer Science.
3. C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit. Lett., vol. 25, no. 4, pp. 481–494, 2004.
4. S. F. Tu and Y. C. Hou, "Design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images," Imag. Sci. J., vol. 55, no. 2, pp. 90–101, 2007.
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. Xiaotian Wu, Wei Sun, "Random grid-based visual secret sharing with abilities of OR and XOR decryptions", J. Vis. Commun. Image R. 24 (2013) 48–62
7. Xiaotian Wu, Wei Sun, "Improve visual quality of Random grid based Visual Secret Sharing", Signal Processing 93 (2013) 977–995
8. Kai-Hui Lee and Pei-Ling Chiu, "An Extended color Visual Cryptography algorithm for general access structure", IEEE Transactions On Information Forensics And Security, Vol. 7, No. 1, February 2012
9. 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
10. 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.
11. D. C. Lou, H. H. Chen, H. C. Wu, and C. S. Tsai, "A novel authenticatable color visualsecret sharing scheme using nonexpanded meaningful shares," Displays, vol. 32, no. 3, pp. 118–134, 2011.
12. mizuho nakajima, yasushi yamaguchi, "extended visual cryptography for natural images",