International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2015)

Conference Organized by Interscience Institute of Management and Technology,

Bhubaneswar, Odisha, India

Multiple Information Hiding using Circular Random Grids

Sandeep Gurung[*], Mrinaldeep Chakravorty, Abhi Agarwal, M K Ghose

[*]Sikkim Manipal Institute of Technology, Sikkim, India

Abstract

Security has become an inseparable issue as information technology is of vital importance. Information Security ensures mathematical techniques and related aspects to provide for confidentiality, data security, entity authentication and data origin authentication. However, apart from the mathematical models there are several schemes which provide information security ensuring high capacity and secrecy. These schemes are quintessential to provide a robust system that covers all aspects of information security at the same time involving high data capacity, ease of use and secrecy. Visual cryptography is a new technique which provides information security using simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. This technique allows visual information to be encrypted in such a way that their decryption can be performed by the Human Visual System (HVS), without any complex cryptographic algorithms. Circular Random Grids extends the functionality by hiding more data in circular grids to provide confidentiality and secrecy without risking suspicion of an intruder. The simple 2:2 secret sharing scheme is extended to hide more than one secret message. Thus a high data capacity is also achieved in the proposed scheme.

* Corresponding author. Tel.: 9733524124;
 E-mail address: gurung_sandeeep@yahoo.co.in

1. Introduction

In the era of information and communication technology, the needs for information sharing and transfer have increased exponentially. The threat of an intruder accessing secret information has been an ever existing concern for the data communication in the public domain. Cryptography and Steganography are the most widely used techniques to overcome these threats. With the availability of increasing computation power, it is only a matter of time before decrypting the information becomes simple. We therefore need an encryption mechanism which ensures confidentiality and authentication and is cost effective.

A secret sharing scheme suggested by Naor and Shamir's [1] enables distribution of a secret amongst 'n' parties, such that only predefined authorized sets will be able to reconstruct the secret. In a k out of n secret sharing problem 'n' shares are generated and it requires a minimum of 'k' shares to retrieve the original image (message). The image remains hidden if fewer than 'k' shares are stacked together.

Visual cryptography (VC) is a powerful technique that combines the notions of ciphers and secret sharing in cryptography with that of graphics. It implements the (k, n) secret sharing scheme as mentioned before on digital images. VC takes a binary image (the secret) and divides it into two or more pieces known as shares. When the shares are printed on transparencies and then superimposed, the secret can be recovered. No computer participation is required, thus demonstrating one of the distinguishing features of VC. VC is a unique technique in the sense that the encrypted message can be decrypted directly by the human visual system (HVS). The shares are a random collection of noise. The decoding can be done visually by overlaying all the defined or defined threshold number of shares. An expert cryptanalyst even cannot decode the secret with lesser than the threshold values of shares. However, this technique suffers from the following drawbacks:-

    i.   Pixel Expansion resulting in an increased size of the encrypted shares thereby generating greater traffic.

    ii.   Only one secret image can be encrypted.

    iii.   Requirement of a complex codebook to generate the cipher text.

Random Grids [2] extends the solution to the secret sharing problem by implementing a collection of 2-D transparent and opaque pixels arranged randomly which reveals the secret to the Human Visual System (HVS) when being superimposed. Unlike other visual cryptography approaches, random grid does not need the basis matrices to encode the shares thus eliminating the use of a complex code book. Pixel expansion is disallowed which is therefore a great advantage of using Random Grids. Also, the sizes of secret image and the shares are identical to each other thus maintaining the aspect ratio of the images.

To increase the security and the carrying capacity various multilevel schemes have been suggested. A hybrid model of visual cryptography and steganography [3] has been suggested to increase the efficiency of such systems. Recursive techniques [4] are also used to increase the number of secret images that can be hidden. However they tend to increase the size of the images as the number of hidden messages increases. The use of a Circular Random Grid creates an efficient technique to hide one or more secrets by simply rotating the grids at a particular angle.

The rest of the paper is organised as follows: In section 2 a brief overview of random grids and the method of generating random grids is discussed. Section 3 gives a review of the various techniques used for hiding multiple information. Section 4 contains the proposed methodology and section 5 contains the detailed design strategy used to achieve the goal. The final section 6 and 7 contains the experimental results and the conclusion of this article respectively.

2. Random Grids

Random grid suggested by Kafri et al consists of a transparency comprising of transparent and opaque pixels arranged randomly which is designed that when being superimposed, it reveals the secret to the Human Visual System (HVS) without the help of any computational parameters. A random grid can also be defined as a transparency comprising a two-dimensional array of pixels. Every pixel is either transparent or opaque. Transmission of light through these chosen pixels is random. Opaque pixels block out light whereas transparent pixels allow light to pass through. The number of white pixels is approximately equal to the number of black pixels making its average light transmission as half. This scheme of encrypting the images is in a way similar to one-time

pad techniques, which adds to its security. The probability of a pixel being either black or white is completely random. Thus there is no correlation among the various pixels in the random grid. The number of opaque pixels where O denotes opaque is equal to P(O)=1/2; similarly the number of transparent pixels where Tr denotes transparent is equal to P(Tr) = 1/2. Thus the average light transmission of a random grid is also ½. If we assume 'R' to be the random grid then T(R) = ½. For a certain pixel 'r' in random grid R the probability of r to be transparent is equal to that of r being opaque. The algorithm for implementing random grids is given below with an example (Figure 1). There are variations on the algorithm used; here we have taken the algorithm from [2] that offers the highest contrast value of 1/2.

Input: A w × h binary image B where B[i, j] ∈ {0, 1}(white or black), $1 \le i \le w$ and $1 \le j \le h$
Output: Two shares of random grids R1 and R2 which reveal G when superimposed where $R_k[i, j] \in B$, $1 \le i \le w$ and $1 \le j \le h$ and $k \in \{1, 2\}$

Algorithm 1

1: Generate R_1 as a random grid
// **for** (each pixel $R_1[i, j]$, $1 \le i \le w$ and $1 \le j \le h$) **do**
// $R_1[i, j]$ = random_pixel(0, 1)
2: **for** (each pixel B[i, j], $1 \le i \le w$ and $1 \le j \le h$) **do**
2.1: {   **if** (B[i, j] = 0) $R_2[i, j] = R_1[i, j]$
        else $R_2[i, j] = 1 - R_1[i, j]$
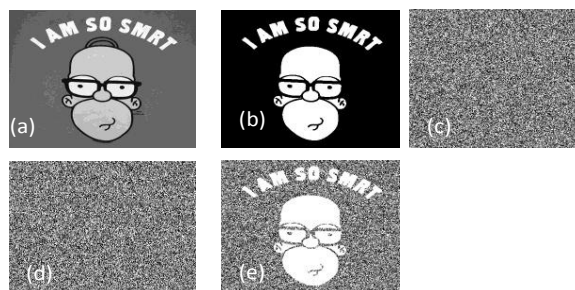   }
3: output (R_1, R_2)

Figure 1. Implementation details [3] of Algorithm 1 for encrypting image B: (a) Input image B; (b) Threshold image; (c) and (d) Encrypted Shares using random grids; (e) Final output image with PSNR value 4.2661.

3.   Multiple Information Hiding

The problem with random grids is that it is only possible to encrypt a single image. However this concept was extended to encrypting two images by Chen et al [5] in which the two different hidden images were obtained by stacking the shares on top of each other and then rotating the grids. For this, the user was required to possess both the grids as well as the knowledge about the angle of rotation for which the images would be obtained. The limitation in this scheme was that the angle of rotation to obtain the second secret image could either be 90, 180 or 270 degrees as the grids were rectangular in shape; also the idea included pixel expansion to implement the scheme. Since there were only three available options, an intruder could easily decrypt the information simply by using Brute- Force technique. To eliminate this limitation of random grids and to encrypt multiple images within the same grids so that the capacity of secret communication is increased, H.C. Hsu et al [6] proposed the concept of circular random grids. This scheme encrypts multiple images into two circular random grids such that in order to decrypt the images we superimpose the two grids and keeping one grid fixed, we rotate the other grid by a certain fixed angle to obtain the multiple secret images. Other schemes suggested by Jeanne Chen et al [7] and Chang et al [8] gave new directions of representing images as circular grids.

Simple recursive techniques as suggested in [9] can be implemented to hide any number of information. It

simply tried to utilize the Least Significant Bits (LSBs) of images to hide the Most Significant Bits (MSBs) of other secret images. Recursive information was also implemented on circular grids to implement a multi information hiding scheme [10]. The scheme uses a grid as a guide line to represent the images in a circular fashion an idea of which is listed below.

4.   Proposed Methodology

Most of the techniques that deal with multiple information hiding utilize the traditional visual cryptography schemes thus using pixel expansion as a basis and the construction of a complex code book. The proposed methodology uses the traditional random grids as suggested by Kafri as a basis for generating the shares as mentioned in Figure 2. This would omit the problem of pixel expansion and creation of the code book which would guide us to construct the shares. The aspect ratio of the secret image would also be unaffected by the scheme. The grids are represented in a circular manner as mentioned in Figure 3 and are then used to hide more number of secret information using the idea of rotation. The proposed idea is simple and easy to use unlike the mechanism in [11, 12] which would still involve a computer to decrypt the secret information.
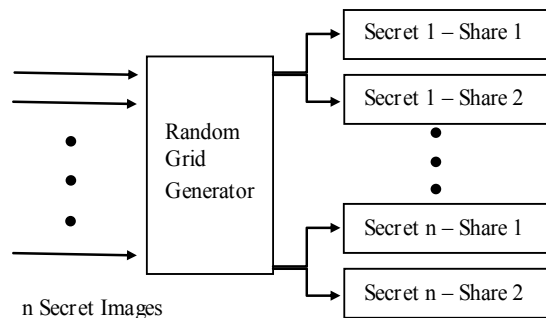

Figure 2. Generation of Random Girds [10]

5.   Design Strategy

Under this section the overall stratagem of approaching the solution is reviewed. This segment dispenses the process of encryption and decryption of the image with the secret embedded in it. In order to improve the quality of the reconstructed image the natural (continuous-tone) images must be first converted into half tone images by using the density of the net dots to simulate the original gray of color levels in the target binary representation, also the VC scheme by nature is lossy. The Floyd-Steinberg Error Diffusion [13] technique is used to convert the original colored image to gray scale. To implement this scheme for multiple secret hiding, the binary image for the first secret which is generated by using the concept of thresholding is fed to the Random Generator to generate the first two grids. The grids are then given as an input to the Circular Grid Generator; both the grids are rotated at a particular angle to hide the first secret. The first grid is then used as a basis for hiding other secret information. The first grid is rotated at an angle known to both the sender and the receiver. The second secret information and the first grid are then used to create the second grid for the second secret information. Similarly by rotating the first grid at various angles more number of information can be hidden with acceptable results. The block diagram of the overall procedure as mentioned above is given in Figure 4. Once the circular grids have been generated, the secret can be revealed by simply stacking the two circular grids on each other for the correct angle of rotation (or orientation).

More variations on this architecture can be made to increase the idea for a n:n scheme i:e the idea of choosing the basis can be made according to the design to achieve more information hiding with acceptable results.

The idea of representing the grids in a circular fashion is given below:

1.   Starting from the first (row, column), map all the values stored in the random grid in a row-wise manner to a circular form beginning from an angle of 0 degrees. Whenever a 1 is stored in the grid, a black pixel is mapped onto the circle, and no mapping is done for a value of 0.

2.   Generate a completely filled black circle of the same dimension as the circular random grid generated in the preceding step.

3.   The black circle is divided into concentric circles, and segments. The number of concentric circles must be equal to the number of rows in the random grid, and the number of segments must be equal to the number of columns of the random grid.
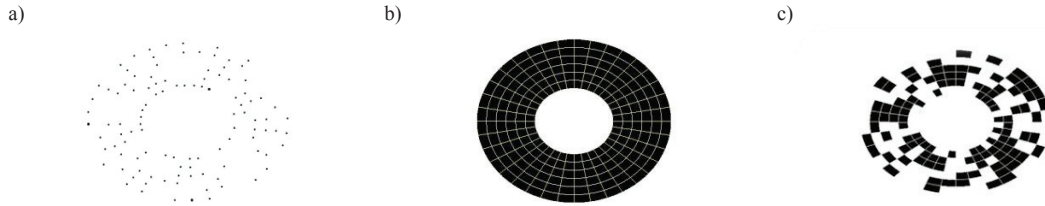
a)   b)   c)

Figure 3. Generation of Circular Random Grid [10] using the reference circle and the filled circle, a) Reference Circle, b) Filled Circle and c) Resultant Circular Grid
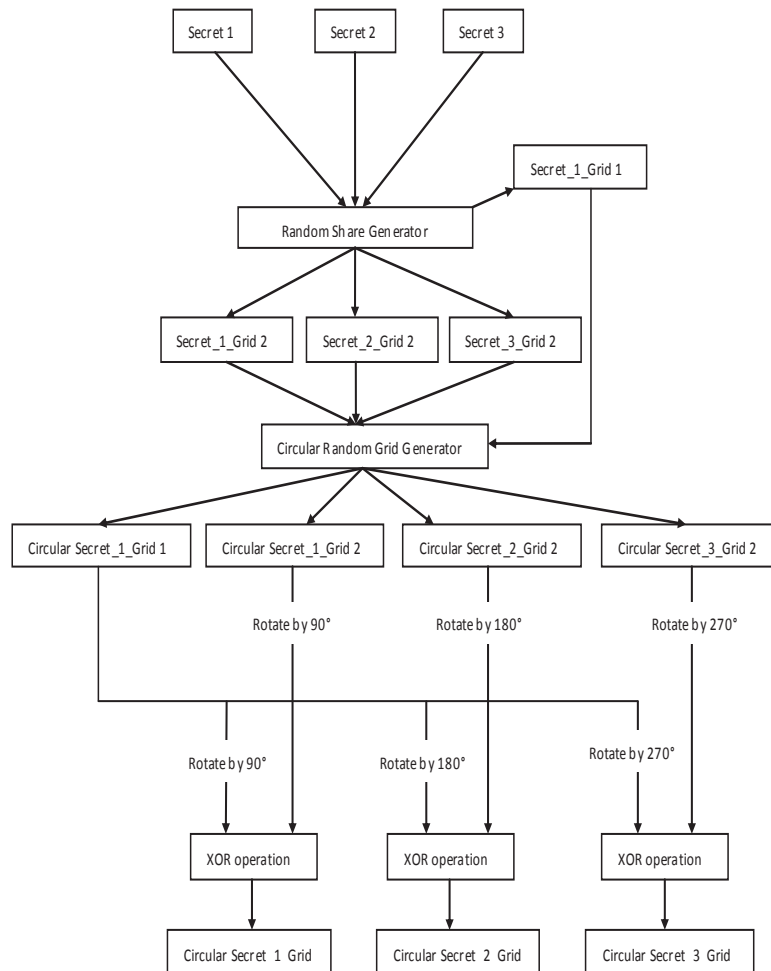
Figure 4. Basic Block diagram of the strategy

6. Simulation and Experiment

6.1 PSNR Comparison

This section evaluates the PSNR value of the input image and the secret that is revealed at the end using the formula:

$$MSE = \frac{1}{m*n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

$$= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. For Binary image it is 1. The PSNR comparison of the three secret images is given on Table 1.
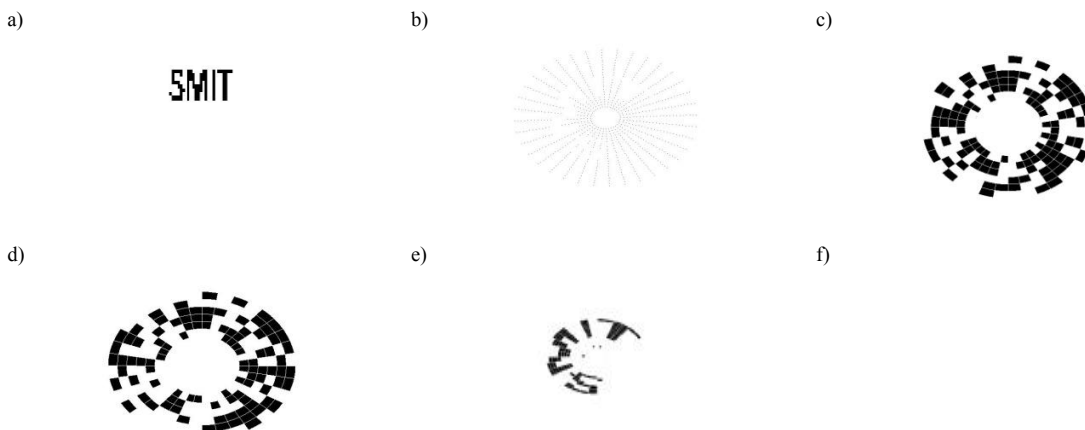
a)   b)   c)

d)   e)   f)

Figure 5. The implementation for a secret binary image 'SMIT'. a) Binary image, b) Circular reference for Share 1, c) Circular Share 1 for 'SMIT' d) Circular Share 2 for 'SMIT' e) Overlapped image
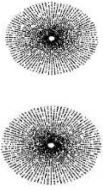
6.2 Experiment

An example of the circular share representation is shown in Figure 5. The circular reference is used as a basis to generate two independent noisy shares. The final output is revealed by stacking the two shares.

Figure 6, 7 and 8 represents the implementation of the proposed methodology. In the experiment three binary image of size 90 by 90 is taken as an input. The first secret image is sent through the random grid generator which in turn generates two random shares. These shares are fed into a circular random grid to generate the grids in a circular representation at a rotation angle of 90°. This ensures that the first secret image can be extracted by aligning the two circular at a particular orientation as shown in Figure 6. The first share of the first secret image is then rotated at an angle of 180° and it serves as a basis for generating the second share for the second secret information as shown in Figure 7. Similarly the first share of the first secret information is then rotated at an angle of 270° and is used to generate the second share for the third secret information as shown in Figure 8. The PSNR comparison of the three secret images is shown in Table 1.

7. Conclusion

1.   Generation of circular random grids which correspond to the rectangular grids generated.
2.   The circular shares are rotated at multiple angles using one of the grids as a basis to hide more secret information.
3.   Both confidentiality and authentication can be achieved by this method of encryption.
4.   The project can be extended further to incorporate the encryption of gray scale and colored images rather than just binary images.

INPUT	INTERMEDIATE SHARES	OUTPUT	PSNR
CODE			3.4758
GRID			3.4424
MAIN			3.4353

Table 1: PSNR Comparison for three binary images
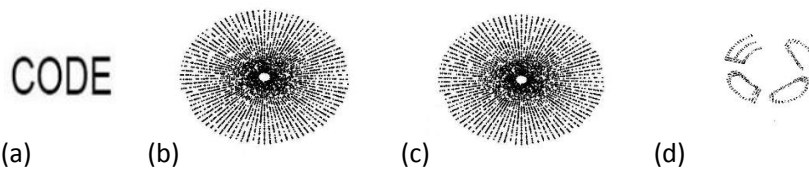

| (a) | (b) | (c) | (d) |

Figure 6. Implementation details of Algorithm 1 for encrypting image B: (a) Input image B; (b) and (c) Encrypted Shares using circular random grids; (d) Final output image with PSNR value 3.4758.
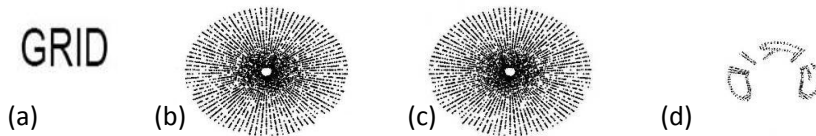
Figure 7. Implementation details of Algorithm 1 for encrypting image B: (a) Input image B; (b) and (c) Encrypted Shares using circular random grids; (d) Final output image with PSNR value 3.4424.

Figure 8. Implementation details of Algorithm 1 for encrypting image B: (a) Input image B; (b) and (c) Encrypted Shares using circular random grids; (d) Final output image with PSNR value 3.4353.

8. Acknowledgement

References

[1] Naor, M., and Shamir, A. (1995), Visual cryptography, in ''Advances in Cryptogoly Eurocrypt '94'' (A. De Santis, Ed.), Lecture Notes in Computer Science, Vol. 950, pp. 1 12, Springer-Verlag, Berlin.
[2] Kafri, O., Keren, E., "Encryption of pictures and shapes by Random Grids." Optics, Letters, 1987, 377–379.
[3] Sandeep Gurung, Pratarshi Saha and Kunal Krishanu, "Hybridization of DCT based Steganography and Random Grids" , International Journal of Network Security & Its Applications , Volume 5, Issue 5, ISSN : 0974 - 9330[Online]; 0975- 2307 [Print] , AIRCC Publications May 2013.
[4] Meenakshi Gnanaguruparan , Subhash Kak , "Recursive Hiding Of Secrets In Visual Cryptography" in Cryptologia, Volume XXVI ,Issue 1(2002).
[5] T.H. Chen, K.H. Tsao, K.C. Wei, "Multiple-image encryption by rotating random grids", Proceedings of the 8th International Conference on Intelligent System Design and Applications (2008).
H.C. Hsu, J. Chen, T.S Chen, Y.H. Lin, "Special type of circular visual cryptography for multiple secret hiding", The Imaging Science Journal 55(3)(2007) 175-179.
[6] H.C. Hsu, J. Chen, T.S Chen, Y.H. Lin, "Special type of circular visual cryptography for multiple secret hiding", The Imaging Science Journal 55(3)(2007) 175-179.
[7] Jeanne Chen, Tung-Shou Chen, Hwa-Ching Hsu, Hsiao- Wen Chen, "New visual cryptography system based on circular shadow image and fixed angle segmentation", Journal of Electronic Image(413), 033018 (Jul-Sep 2005).
[8] Hsien-Chu Wu, Chin–Chen Chang, "Sharing visual multi- secrets using circle shares", Computer Standards and Interfaces 28 (2005) 123- 135.
[9] Lekhika Chhetri, Sandeep Gurung, "Recursive information hiding in threshold visual cryptography scheme", International Journal of Emerging Technology and Advanced Engineering, Vol. 3, Issue 5 (May 2013).
[10] Sandeep Gurung, G. Ojha, M.K. Ghose, "Multiple Image Encryption using Random Circular Grids and Recursive Image Hiding", Vol 86 No 10, 2013.
[11] Tzung-Her Chen , Kuang-Che Li, "Multi-image encryption by circular random grids", Department of Computer Science and Information Engineering, National Chiayi University, Chiayi City 60004, Taiwan. 2011.
[12] B. Feng, H. C. Wu, C. S. Tsai, and Y. P. Chu, "A new multi-secret images sharing scheme using Lagrange's interpolation", The Journal of Systems and Software, Vol. 76, No. 3, pp. 327-339. 2005.
[13] Floyd, R. W. and L. Steinberg. "An adaptive algorithm for spatial *greyscale"*, Proc. SID, vol. 17/2, pp. 75-77. 1976.