Multiple Image Encryption using Random Circular Grids and Recursive Image Hiding

Sandeep Gurung[1] Gaurav Ojha[2] M K Ghose[3]
[1,2,3]Department of Computer Science and Engineering
Sikkim Manipal Institute of Technology, Majhitar, Sikkim
India

ABSTRACT
The visual secret sharing (VSS) scheme encrypts the secret information into various meaningless shares. These shares are distributed to the authorized participants and the secret information can be retrieved by any k out of n participants by stacking their respective shares on top of each other. This scheme uses HVS (Human Visual System) to decrypt the information, and thus no technical or financial investment is required. Moreover, it is a one-time pad technique, so decrypting the information by an attacker is almost impossible. This paper proposes an improved visual secret sharing technique in which we aim to build upon the random grid approach of visual cryptography and test the feasibility of Recursive Image Hiding to hide multiple secrets at varying levels of the grids generated. Since we are using circular random grids, it is even possible to hide multiple images in the same grids and obtain the secret images for different angles of rotation of the grids. The participants need to be in possession of both the shares, as well as the fixes angle of rotation for which the secret can be obtained, in order to decrypt the image. In case of recursive image hiding, numerous secrets are hidden recursively in the shares of the original images at each level. Shares carry information for the subsequent secrets as well, thus leading to increased capacity. Also, the limitation on the number of secrets that can be hidden can be overcome because for each grid, multiple secrets can be recursively hidden. Thus, not only will we be able to hide multiple images, but multiple grids as well which in turn carry the information for multiple images.

General Terms
Visual cryptography, visual secret sharing scheme

Keywords
Recursive image hiding, secret message, shares, random grids, threshold, hidden image, rotation**.**

1. INTRODUCTION
Attaining data confidentiality and authentication is a must in today's world due to the increasing use of technology for the transmission and reception of sensitive information. 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.

Visual cryptography, as proposed by Moni Naor and Adi Shamir [7] in 1994, is a visual secret sharing (VSS) technique in which materials (pictures, text, etc.) are encrypted in a totally secure fashion and do not require any financial or technical assistance in the decryption process as the decryption is achieved merely by the Human Visual System (HVS). In this scheme the secret information is encrypted into a number of shares which themselves are a random collection of noise and do not give away any information individually. The secret information is revealed when the shares are stacked on top of each other as observed by the human visual system. Thus, no calculations or computations need to be performed. This technique is very desirable for situations where complex machines aren't available to obtain the required information. Moreover, this technique does not require any knowledge of cryptography and can be used by any person. In case of a (n, k) threshold cryptography scheme the secret is encrypted into n shares. When any combination of k shares is overlaid, the secret information is decrypted. Thus, even an expert having less than k number of shares will never be able to obtain the hidden information. For instance, in a (3, 2) threshold cryptography scheme the secret information is encrypted into 3 meaningless shares. Any 2 shares reveal the secret when stacked on top of each other.

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.

2. RANDOM CIRCULAR GRIDS
A random grid for a binary image is a two dimensional array of pixels. This scheme of encryption using random grids was proposed by Kafri and Keren [8] in 1987.The pixels can either be completely transparent (white) or completely opaque (black). This method is completely probabilistic. 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 white (transparent) pixels let through the light whereas the black (opaque) restrict it. Since in a random grid, the no of white pixels is approximately equal to the number of black pixels, its average light transmission is half. This scheme of encrypting the images is in a way similar to one-time pad techniques, which adds to its security. The decryption mechanism simply consists of stacking the transparencies on top of each other to reveal the hidden image. When the grids are superimposed, the correlated areas of the grids come together and reveal the secret information due to the difference in light transmission. The decoding is entirely done by the human visual system (HVS).

As compared to the traditional visual cryptography technique, this scheme does not use the basic matrices to encrypt the shares and so the problem of pixel expansion is completely eliminated. As a consequence the sizes of the original image as well as the encrypted shares are the same which reduces the overhead of transmission, communication and storage. 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, Tsao and Wei [3] 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. 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, Tzung-Her Chen, Kuang-Che Li [14] 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.

3. RECURSIVE IMAGE HIDING

The traditional visual cryptography scheme suffers from various drawbacks as discussed earlier. The most significant among these is the limitation of only being able to encrypt one image. The idea of recursive information hiding overcomes this limitation by allowing one to encrypt multiple images efficiently.

In this scheme [5], the images that are to be encrypted are taken in the increasing order of their sizes. First, the shares of the smallest image that is to be encrypted are generated. These randomly generated shares are then concatenated to generate the first share of the secret image. The second share of the secret image is obtained in such a manner that if the two shares are overlaid on top of each other, the original image can be obtained. The scheme proceeds by generating random shares of all the secret images that are to be hidden. As already pointed out, the images have to be taken in the increasing order of their sizes. The shares of the smallest image are hidden in the shares of the image which is next larger in size and the shares of this image are hidden within the shares of the next larger image. So, in this way the secret information is recursively hidden in the shares of the secret images. Therefore, the original (largest) image has got all the hidden information within its shares. The decryption process is simple. It is the exact reverse of the encryption process. We first need to extract the shares of the original image and from those shares we recursively extract the shares of the smaller images till we obtain the shares of the smallest hidden image.

This scheme extends the usability and capacity of the traditional visual cryptography scheme by allowing one to encrypt multiple images. However, it is also subject to a certain restriction. The size of the secret image that is to be hidden within the original image should be a multiple of 2 with respect to the original image's size. For instance, if the size of the original image is 6 × 6, then the size of the first secret image has to be 3 × 3 and the size of the second secret image will be 6 × 3.

4. PROPOSED METHOD

The following block diagrams give a brief idea regarding the methodology being adopted for the generation of shares, hiding multiple images in a recursive manner and then transforming it into circular grids.

Step 1: Generation of Random grids

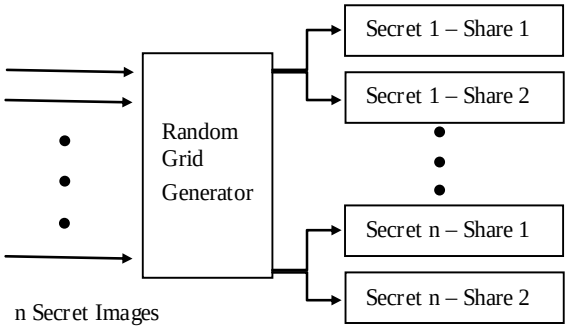


Figure 1: Generation of Random Grids

The Random Grid Generator in the above figure takes a secret image to be encrypted and generates the corresponding random grids for the same. Each secret image is taken as an input to the Random Grid Generator and the corresponding shares (i.e: two shares) are generated.

The algorithm that is used to generate the grids is given below.

Algorithm : Random_Grid_Generator

Input: A binary secret image M of size WxH
$M = \{ M(i,j) \mid M(i,j) = 0 \text{ or } 1,\ 1 \le i \le W,\ 1 \le j \le H\}$
Output: Two random grids R_1 and R_2 of size WxH

1. for (i and j, $1 \le i \le W$, $1 \le j \le H$)
   $R_1(i,j) = rnd\_val(0,1)$
2. for (i and j, $1 \le i \le W$, $1 \le j \le H$)
   if ($M(i,j) == 0$) // 0 represents a white pixel
   $R_2(i,j) = R_1(i,j)$
   else
   $R_2(i,j) = 1 - R_1(i,j)$
3. Output (R_1, R_2)

The function **rnd_val(0,1)** returns either a 0 or 1 randomly.

Step 2: Recursive Image hiding of secrets and Generation of Circular Grids

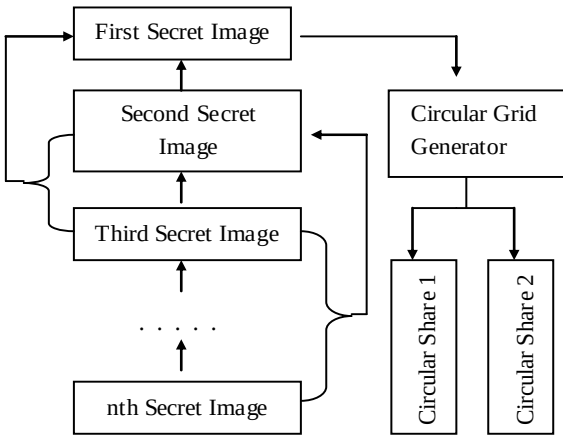


Figure 2: Steps followed to recursively hide shares and then generate circular share for last level of recursion [5].

This step is divided into two different processes.

The first process is to recursively hide the secrets. It consists of the following set of steps:

1. Take the first set pair of secrets to be encrypted.
2. Concatenate the same either horizontally or vertically. The resultant grid should be of the same size as that of the next secret to be hidden.
3. Generate the second share of the next image by the *Random_Grid_Generator* algorithm using the concatenated share as R_1.
4. Repeat steps 2-3 until all the secret images have been recursively hidden.
5. The last set of shares generated hold the information for all the previously generated images.

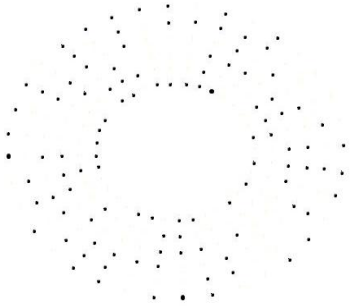
The second process is to generate the rectangular random shares to circular grids. It is done in the following manner.

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 reference circle 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.
4. Perform a mapping of the reference circle onto the filled circle. Whenever a black pixel is encountered in the reference circle, the corresponding sector is filled with white color.
5. This generates the circular random grid.

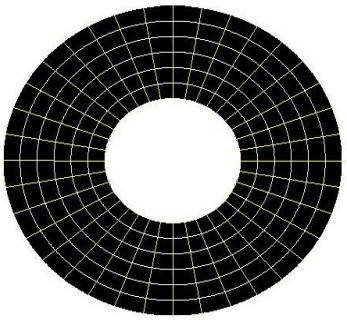
Once the circular grids have been generated, the secret can be revealed by simply stacking the two circular grids on each other for the correct angle of rotation (or orientation).

However, the circular shares currently will reveal only the topmost secret encrypted. In order to retrieve the next level of secrets, the reverse operation of the recursive image hiding is performed. The first share which contains both the previous level of shares concatenated within it is split to obtain the random grids constituting it.

a)



b)



c)

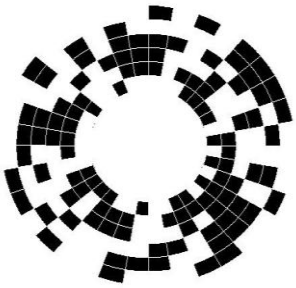


Figure 3: Generation of Circular Random Grid using the reference circle and the filled circle, a) Reference Circle, b) Filled Circle and c) Resultant Circular Grid

The rectangular grids are then again converted to circular grids using the same set of procedures and stacked to reveal the information. These steps are repeated until all the secrets have been revealed.

5. RESULTS

Considering the following 3 images to be encrypted:

Table 1. The set of secrets to be encrypted and their dimensions

Secret Image	Image Dimensions
	Secret Image 1 : 'SMIT' Dimension: 6 × 36 pixels
	Secret Image 2 : 'AND' Dimension: 12 × 36 pixels
	Secret Image 3 : 'SMIMS' Dimension: 24 × 36 pixels

Initially, the random grids are generated for 'SMIT', which are then concatenated to form R_1 for the next image 'AND'. The resultant grid obtained by concatenation is found to be of the same size as that of the next level of secret (12x36 in this case for 'AND'). R_2 is then generated using the *Random_Grid_Generator* algorithm. Again these R_1 and R_2 are concatenated to form the R_1 for the image 'SMIMS' and R_2 is similarly generated. After this, the circular grids are generated.

The circular shares generated for the largest image 'SMIMS' are as shown in Figure 4-5. The secret is revealed by stacking the shares on top of each other as shown in Figure 6.

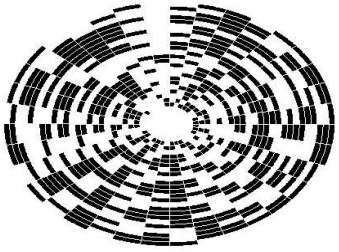


Figure 4: Circular Share 1 for 'SMIMS'

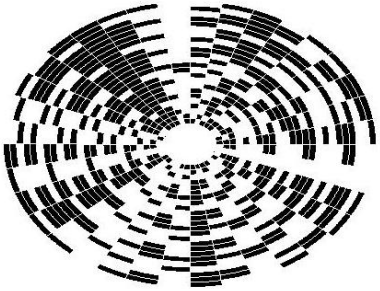


Figure 5: Circular Share 2 for 'SMIMS'

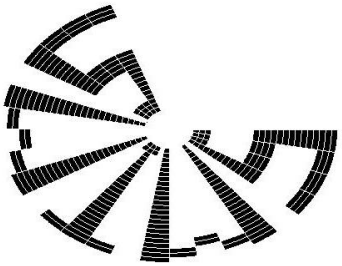


Figure 6: Decrypted secret 1 – 'SMIMS'

Now share 1 of this secret will result in the following set of shares for the next level of secret 'AND' as shown in Figure 7-9.

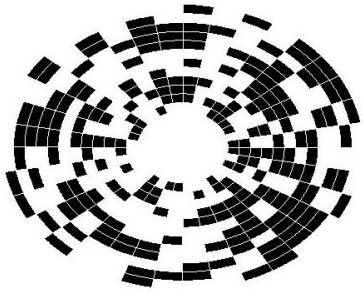


Figure 7: Circular Share 1 for 'AND'

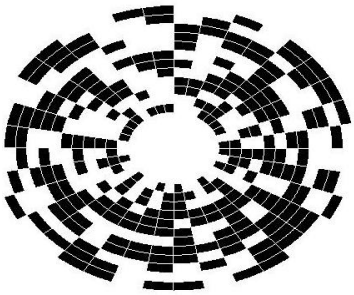


Figure 8: Circular Share 2 for 'AND'

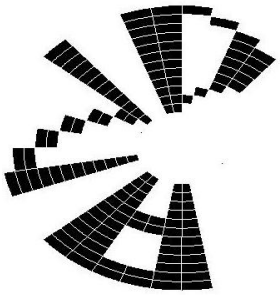


Figure 9: Decrypted Secret 2 - 'AND'

Similarly, the last level of secrets is revealed as shown in Figure 10-12.

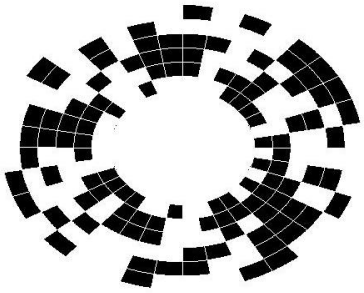


Figure 10: Circular Share 1 for 'SMIT'

In case of recursive image hiding, the efficiency [8] of the information encrypted is near 100%, as almost all the bits available are used to recursively encrypt the information. Moreover, encrypting only one secret in two shares using the random grids approach gives the highest contrast value of 0.5 [15]. Although this means that the capacity of the circular grids is not fully utilized, but if more secrets are encrypted into the same, the contrast value decreases. Above a certain number of secrets, the contrast value decreases to a much lower value, making it difficult for the image to be revealed by the Human Visual System.

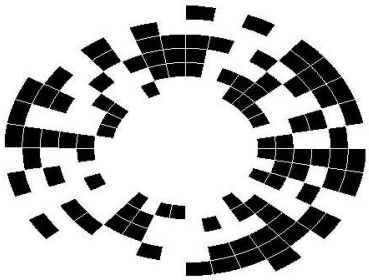


Figure 11: Circular Share 2 for 'SMIT'

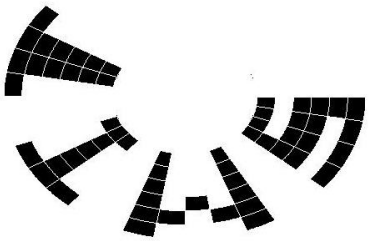


Figure 12: Decrypted Secret 3 - 'SMIT'

6. CONCLUSION

This paper has successfully been able to suggest the following ideas for a given set of secrets (keeping in view the constraint on the dimension chosen for the images):

1. Generation of random grids and recursively hiding information of the next level of secrets into the previous level shares. The shares in isolation leak no information regarding the secret for that particular level.

2. Generation of circular random grids which correspond to the rectangular grids generated. These circular grids successfully reveal the secret hidden within them for the correct angle of stacking.

3. The share at the highest level contains information of the shares hidden at previous levels. We can successfully split the share to give the two shares of images which on superposition reveal the secret of that level.
4. Thus, both confidentiality and authentication can be achieved by this method of encryption.

However, this paper only suggests ideas for the encryption of black and white images and not colored ones. Another limitation is that within one pair of the circular grids, only a single secret is encrypted.

7. FUTURE SCOPE

The project can be extended further to incorporate the following:

1. Encryption of gray scale and colored images rather than just binary images.

2. Hiding of multiple secrets within the same share, so that multiple secrets are revealed on rotating the circular shares. This way multiple secrets are hidden not only recursively, but at each level, numerous secrets can be encrypted as well.

8. ACKNOWLEDGMENTS

The corresponding author deeply acknowledges the guidance and inspiration by his Ph.D. guide Prof. (Dr.) M K Ghose, Head, Computer Science and Engineering Department, SMIT, Sikkim, India. The author also deeply acknowledges the contribution of Nishant Mintri and Pooja Agarwal, B.Tech students of Computer Science and Engineering Department, SMIT, Sikkim, for their contribution towards the work.

9. REFERENCES

[1] Shamir, "How to share a secret", Communications of the ACM, Vol. 22, pp. 612-613, 1979.

[2] Hsien-Chu Wu, Chin–Chen Chang, "Sharing visual multi- secrets using circle shares", Computer Standards and Interfaces 28 (2005) 123-135.

[3] 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.

[4] 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).

[5] 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).

[6] L.H Chen, C.C. Wu, "A study on Visual Cryptography", Master thesis, Institute of Computer and Information Science, National Chiao, Tung University, Taiwan, R.O.C, 1998.

[7] M. Naor, A. Shamir, Proceedings of advances in cryptology: Eurocrypt94, Lecture Notes in Computer Science, vol. 950, (1995).

[8] Meenakshi Gnanaguruparan , Subhash Kak , "Recursive Hiding Of Secrets In Visual Cryptography" in Cryptologia, Volume XXVI ,Issue 1(2002).

[9] O. Kafri, E. Keren, "Encryption of pictures and shapes by Random Grids", Optics Letters 12 (1987).

[10] S.J. Shyu, "Image Encryption by Random Grids", Pattern Recognition 40(2007) 1014-1031.

[11] S.J. Shyu, "Image encryption by multiple random grids", Pattern Recognition 42(7)(2009) 1582-1596.

[12] T.H Chen, K.H Tsao, "Image encryption by (n,n) random grids" in Proceedings of the 18th Information Security Conference, Taiwan, 2008.

[13] T.H Chen, C.C. Wu, "Visual secret sharing by random grids revisited", Pattern Recognition 42(2009) 2203-2217.

[14] 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).

[15] Tzung-Her Chen, Kuang-Che Li, "Multi-image encryption by circular random grids", Information Sciences, Vol.189, (April 2012).

[16] W.P. Fang, J.C Lin, "Visual Cryptography with extra ability of hiding confidential data", Journal of Electronic Imaging 15(2) (2006).