International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.9, No.4 (2016), pp.425-434
http://dx.doi.org/10.14257/ijsip.2016.9.4.37

Secure Image Encryption based on a Cube

Sandeep Gurung, Preyansh Singh Matharoo, Mirnal Kanti Ghose

Department of Computer Science and Engineering,
Sikkim Manipal Institute of Technology, Majhitar, India 737134
gurung_sandeep@yahoo.co.in, preyanshmatharoo@gmail.com,
mrinal.ghose@smu.edu.in

Abstract

With the explosive growth of internet and the fast communication techniques available in recent years, the security and confidentiality of the sensitive data has become of supreme importance and concern. In order to protect this data from tampering and unauthorized access various methods for data hiding in cryptography and steganography have been developed and are in practice today. Steganography hides messages inside a carrier media. Cryptography, on the other hand obscures the content of the message. Visual cryptography, a Secret sharing Scheme, is a new technique which provides information security on digital information by distributing the secret information into many shares. The approach is simple unlike the complex, computationally intensive techniques used in traditional cryptography. Decryption can be performed by simply stacking the shares together and by interpreting it using the Human Visual System (HVS) without the involvement of any computational machines. An attempt has been made to extend the simple (2-2) secret sharing scheme based on Random Grids Visual Secret Sharing Scheme for authentication into a cuboid representation where each share represents a face of the cube. The representation also increases the carrying capacity of a system. Each face (share) of a cube is fragmented into a collection of randomly scrambled sub-blocks. The respective blocks are embedded into a carrier image to hide its existence by using a stenographic technique. The final information is revealed by overlapping the two shadows/shares containing the sub-blocks with the correct index.

***Keywords**: Authentication, Fragmentation, LSB Steganography, PSNR, Random Grids, Secrecy, Shares, Visual Secret Sharing.*

1. Introduction

With the rise of the internet, the need for information sharing and transfer has increased exponentially. This has given a lot of concern over information security. The threat of an intruder accessing the information has been a matter of apprehension not only for an individual but also for businesses and governments. Trust in digital data is characterized by three important service mechanisms namely confidentiality, authenticity and integrity. Confidentiality relates to the property that information is not made available or disclosed to unauthorized individuals, processes or entities. Authentication defines the corroboration that the source of data received is as claimed. Integrity deals with the property that data has not been altered or destroyed in an unauthorized manner. As the technology advances and the computation power of machines increases, it is only a matter of time before decrypting the information becomes simple. Thus, there is a need for an encryption setup which ensures the basic service mechanism, primarily confidentiality and authentication and is also cost effective.

Naor and Shamir [1] proposed a secret sharing scheme where a secret is distributed among ‘n’ parties and at least ‘k’ shares must be stacked to obtain the original message.

The secret will not be revealed if ‘k-1’ shares are stacked together. Visual cryptography is a powerful technique that implements the (k, n) secret sharing scheme on digital images. A binary image is taken and divided into two or more noisy pieces known as shares. These shares are printed on transparencies, piled together and interpreted by using the Human Visual System (HVS). No computer participation is required, thus demonstrating one of the distinguishing features of VC. However the visual secret sharing scheme has the following drawbacks:

a. A complex codebook is required to generate the cipher text.
b. Pixel expansion, resulting in increased size of the encrypted share.
c. Number of images that can be encrypted is one.

The random grid scheme proposed by Kafri and Keren [2] provided a solution to the problems of visual secret sharing by implementing a collection of two dimensional transparent and opaque pixels arranged randomly, which when superimposed reveals the secret to human visual system. Random grid eliminates the use of a complex code book since it does not need the basis of matrices to encode the shares. Pixel expansion is disallowed which is therefore a great advantage of using Random Grids.

Least Significant Bit replacement mechanism a category of Spatial Domain Steganography is simple and easy to implement. Transformation based stenographic techniques are more robust to attacks. It also provides a good basis for hiding the digital information without revealing the patterns of data embedded in it. Thus the existence of the noisy patterns can easily be hidden on a digital cover for its distribution.

The paper is organized in the following way: Chapter 2 gives a gist of related works, Chapter 3 describes the proposed methodology, Chapter 4 outlines the design of the proposal, Chapter 5 features the Experimental results and Chapter 6 gives the Limitations and Conclusion.

2. Related Work

2.1 Random Grids

Random grid, suggested by Kafri *et. al.* [2], consists of a transparency comprising of transparent and opaque pixels arranged randomly. The stacked transparencies reveal 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.

For a certain pixel ‘r’ in a random grid R, the probability of r to be transparent is equal to that of it being opaque therefore: $P(r=0) = P(r=1) =1/2$; where 0 denotes opaque and 1 denotes transparent. Thus, the probability of light transmission of a random pixel ‘r’ in a random grid ‘R’ is equal to $T(R) = ½$.

There are three variations of the algorithm proposed by Kafri and Keren to accomplish the encryption of the image. The basic principle behind all three algorithms is that pixels of first share are generated randomly and pixels of second share are generated by taking original image as reference. The contrasts achieved by the three algorithms are ½, 1/5 and ¼. The approach that gives the highest contrast is given below. A sample output file is mentioned in Figure 1.

Algorithm 1

```
1: Generate R1 as random grid
1.1: for (each pixel R1 [i, j], 1≤i≤W and 1≤j≤H) do
1.1.1:    R1 [i, j] = random_pixel (0, 1).
2: for (each pixel B [i, j], 1≤i≤W and 1≤j≤H) do
2.1:      {if (B [i, j] =0) R2 [i, j] = R1 [i, j]
          else R2 [i, j] =1- R1 [i, j]
          }
3: output (R1, R2).
```

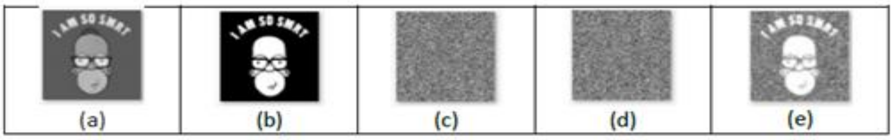


Figure 1: Implementation of Algorithm 1. (a) Input Image (345x345). (b)Threshold image. (c) First Share. (d) Second Share. (e) Reconstructed Image with PSNR 4.0804

2.2 Multiple Information Hiding

The concept of using a grid has a limitation that only a single secret can be encrypted. Chen [4-7] proposed a method to encrypt multiple secrets, wherein the secret images can be decrypted by stacking the two shares and then rotating one of the share while keeping the other share fixed at one position. This scheme has a limitation that a maximum of four secrets can be hidden because of the rectangular shape of random grids. One of the two shares produced can be rotated by 90°, 180° or 270° to decrypt the rest of the secrets. Since the angles of rotation are known, an attacker may try to decrypt the secrets by using Brute-force technique if he could get his hand on to both the shares. The idea would be significantly difficult if each of the grids is made as a collection of randomly scrambled sub grids before being represented as one of the shares.

The geometric configuration of the shares can also be exploited to increase the effectiveness of the data being concealed. The transition of circular to spherical grids [5], and the cubical representation [6] of the shares increase data security and the carrying capacity of the shadows.

2.3 Recursive Information Hiding

The most significant limitation of traditional VC is the ability to encrypt only one image at a time. In recursive image hiding technique [3], the images to be encrypted are taken in increasing order of their sizes. The shares of the smallest image are generated, which are then concatenated to generate the first share of the second image. Using the concatenated share and the secret image as a reference, the second share is generated. Thus, this mechanism helps us hide more secrets recursively but at the expense of increasing the size of the shares.

3. Proposed Methodology

In the proposed methodology, the traditional random grid is used to generate the shares. This would overcome 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 this scheme. The grids (shares) generated are broken down into a number of sub-blocks/fragments. Each block is associated with an index corresponding to its original image and the index in turn is embedded into the block using a steganography technique based on Least Significant Bits. The index values are then randomly arranged and then the corresponding blocks are arranged. Thus, the shares are now scrambled. This increases the complexity when trying to stack the shares. To hide the noisy shares/blocks generated a simple LSB based stenographic technique is used to carry the secret information to the intended recipients. The whole process is further applied to a maximum number of six images. They can be then arranged as a cube, each image making a face of the cube. Figure 2 shows how a cube can be spread into various different patterns.

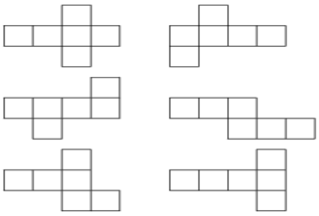


Figure 2. Patterns in which a Cube can be Arranged

4. Design Strategy

Under this section the overall stratagem of approaching the solution is reviewed. To implement the basic secret sharing scheme the gray scale image is converted to a binary image using the concept of thresholding. The produced binary image is then fed to a (2 ,2) random grid generator which produces the two shares. These grids are noisy images, which are fed to the (n x n) block generator. The block generator produces ‘m’ number blocks. As an example it can be seen that a 3 x 3 (n=3) size block can generate 32 (m=32) fragments on a secret image of size 288 by 288. Padding can be done accordingly by looking at the block size for each partition. Each block is associated with an index, based on its corresponding original share. The share is fed to a randomizer where the array of index is then randomly scrambled. Based on the new randomized array, the blocks corresponding to their index are arranged. Thus, the blocks are arranged in a random order and only the sequence of correctly placed blocks can reveal the exact information.

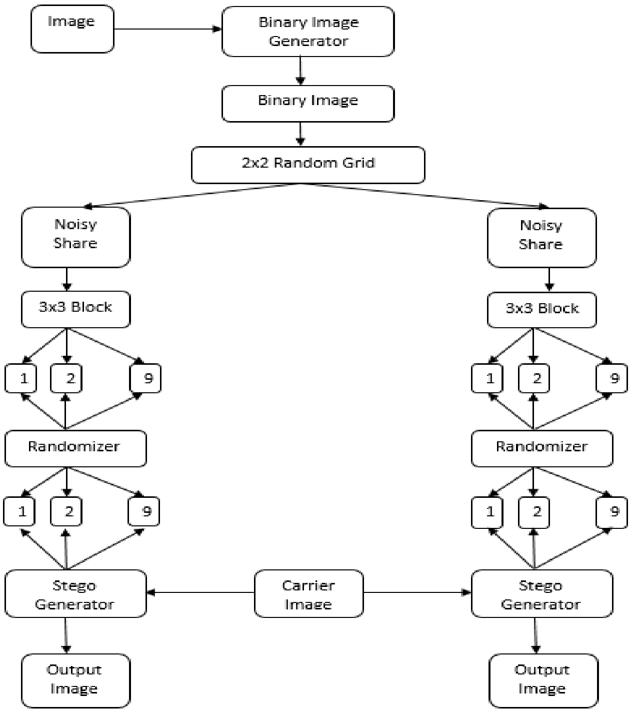


Figure 3. Basic Block Diagram of the Design Strategy

However, the fragments of the noisy share cannot be distributed as it would indicate the presence of some secret information. Therefore, the idea is to embed the fragments into a carrier image using simple Least Significant Bit steganography. Figure 3 shows the block diagram of the design strategy. Figure 4 shows how a noisy share is divided into 9 equal smaller shares.

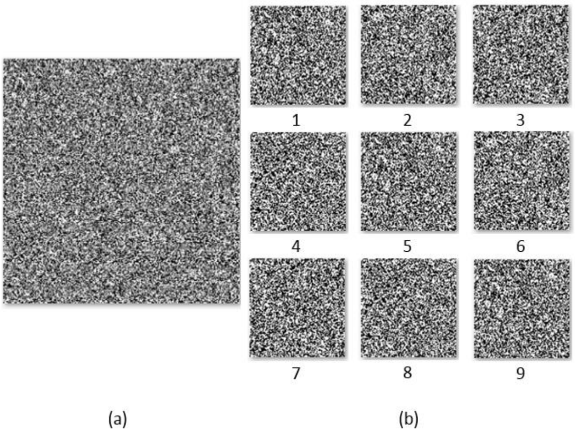


Figure 4. Breaking Shares into Blocks. (a) First Noisy Share (345x345). (b) First Share Divided into 9 blocks with Corresponding Index Values (115x115)

Randomization and arrangement of the fragments is explained in Figure 5. A random array is generated and each elements acts as the reference index for the share. The blocks are now arranged randomly. The index number associated with each block is embedded in the same block by using a steganography technique based on simple Least Significant Bits.

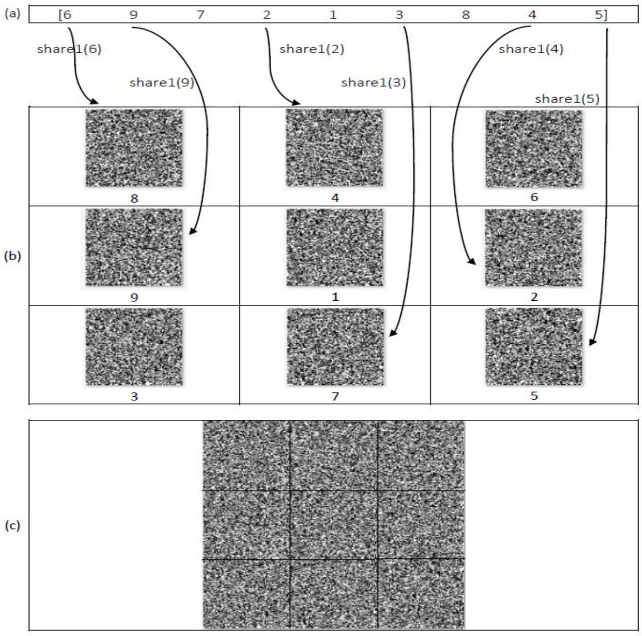


Figure 5. Randomizing the Blocks. (a) Array with Randomized Index Values. (b) Randomized Arrangement of the Blocks Based on the Index with Reference to Share1. (c) Compilation of the Randomly Arranged 9 Blocks Into a Complete Share (345x345)

After generating the noisy fragments, they can be embedded using the LSB steganography for images. The fragments are a binary image consisting of pixel values of either 0 or 1. These values are embedded in the least significant bit of the carrier image. Figure 6 shows a fragment, a carrier image and a resultant stego image. The index number of each block can also be stored in the same block using simple substitution techniques.

The shares can be extended by creating K^2 number of blocks (K=2,3,4…. n) to achieve more complexity while decrypting.

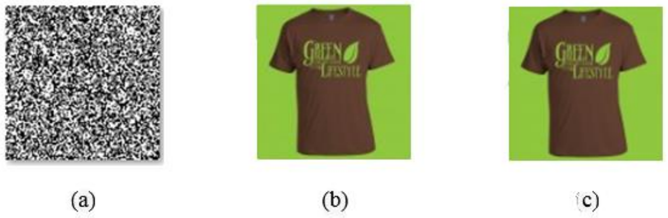


Figure 6. Input and Output of Stego Generator. (a) Input Image (115x115); (b) Carrier Image (115x115); (c) Stego Image (115x115)

5. Experiment and Results

5.1 PSNR Comparison

Fidelity refers to the amount of distortion produced in the original cover image due to embedding. The effects of embedding can be evaluated in terms of Peak-Signal-to-Noise Ratio (PSNR). This section evaluates the PSNR value of the input image and the secret that is revealed at the end using the formula:

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

Where “I” is a noise free image of size (m x n) and K is the noisy share. The PSNR is defined as:

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

Where MAX=255 when pixels are represented using 8-bit representation. For binary images MAX=1. Higher the PSNR value better is the fidelity and hence, lower distortion of the stego image.

5.2 Experiment

An example of the proposed system is shown in Figure 7. An input image is taken and from which two shares are generated. The first share is then scrambled using the randomizer.

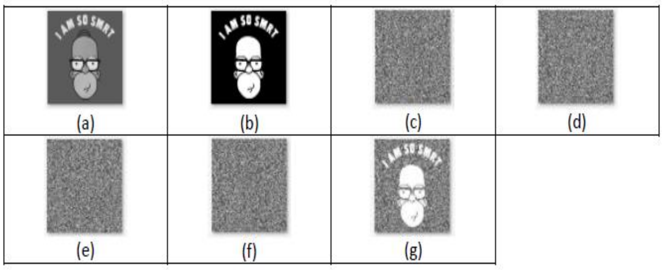


Figure 7. Implementation for an Image. (a) Input Image of 350 by 350 Pixels. (b) Threshold Image (Binary Image). (c) First Share. (d) Second Share. (e) Scrambled First Share. (f) Unscrambled First Share. (g) Result Obtained by Stacking (d) and (f) with PSNR 4.0812

A comparative study was done for images of various sizes. Table 1 shows a comparison of the PSNR in ascending order of the image size. A supporting graphical representation of the same is shown in Figure 8. The tabular data interprets the ideal dimensions of the image size with an acceptable PSNR value.

Table 1: Comparison of PSNR values with increasing image size.

Image Size	PSNR
30x30	3.8697
60x60	3.9786
240x240	4.095
345x345	4.0804
360x360	4.0769
480x480	4.0768
500x500	4.0802
600x600	4.0732
720x720	4.0864
900x900	4.0928

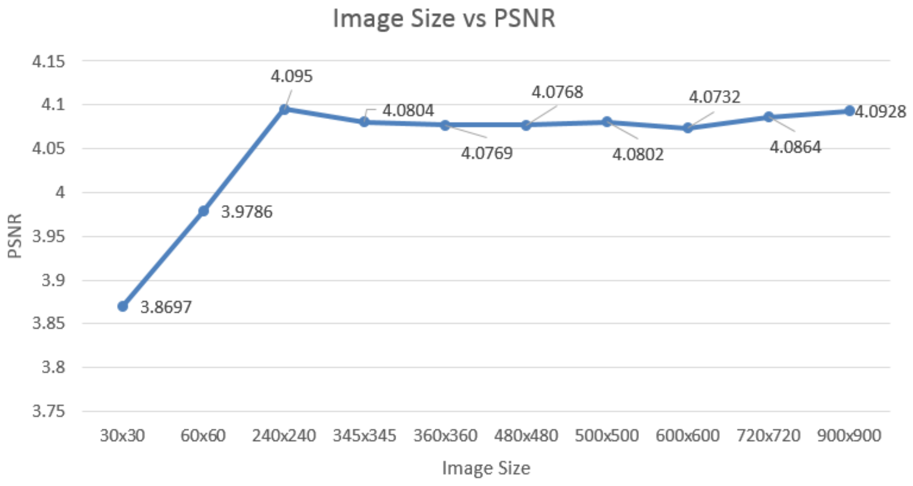
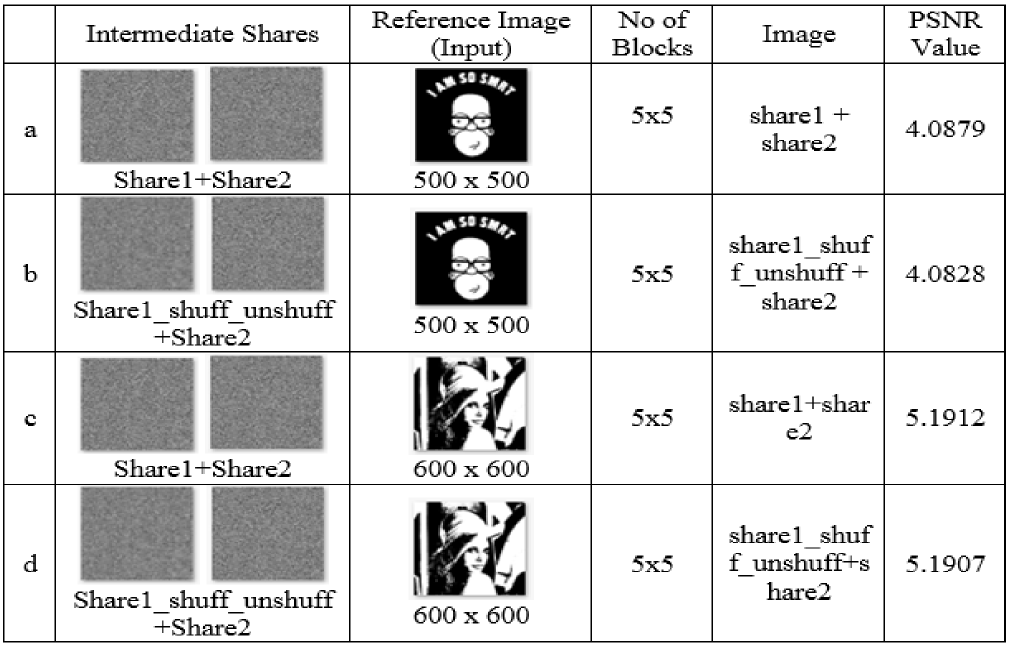


Figure 8. Image Size v/s PSNR.

Further experiment was performed on two images of size 500x500 and 600x600 and both were broken down into 25 blocks. Figure 9 shows the PSNR comparison of the two images respectively. As seen the PSNR value decreases on assembling the scrambled fragments making the cipher difficult to interpret.

6. Conclusion and Future Scope

Pixel expansion, use of a codebook for reference and the carrying capacity are the important attributes of any visual cryptography schemes. Some schemes present methods which do not work with printed transparencies and they rely on computation in order to recover the secret. But apparently it is preferred that the scheme works properly with printed transparencies. If an application requires digital recovery of the secrets, then perfect recovery can be made my using XOR operation.



	Intermediate Shares	Reference Image (Input)	No of Blocks	Image	PSNR Value
a	Share1+Share2	500 x 500	5x5	share1 + share2	4.0879
b	Share1_shuff_unshuff +Share2	500 x 500	5x5	share1_shuff_unshuff + share2	4.0828
c	Share1+Share2	600 x 600	5x5	share1+share2	5.1912
d	Share1_shuff_unshuff +Share2	600 x 600	5x5	share1_shuff_unshuff+share2	5.1907

Figure 9. Comparison of PSNR. (a) Result of Stacking Share1 and Share2 Produces PSNR of 4.0879. (b) Result of Stacking Share1 (After Shuffling, Un-shuffling) and Share2 Produces PSNR of 4.0828. (c) Result of Stacking Share1 and Share2 Produces PSNR of 5.1912. (d) Result of Stacking Share1 (After Shuffling, Un-Shuffling) and Share2 Produces PSNR of 5.1907

The proposed method aims at increasing the complexity of shares of the secret generated which is achieved by dividing the shares into sub-blocks/fragments and randomly shuffling them. The Human Visual System (HVS) can decode the correct information if the fragments are aligned properly in both the shares.

The following are the merits of the proposed methodology.

i. The image is divided into blocks which are randomly arranged. This makes it difficult to obtain the secret by stacking the shares.

ii. As the number of blocks increases, the complexity of decrypting the secret increases.

iii. Since the images are arranged as a cube and the decryption is done by HVS, the number of combinations of arranging the noisy blocks in their respective image increases, hence increasing the overall complexity of the system.

iv. Digital recovery can be used to decrypt the images since the true indices are embedded into the blocks.

v. The intruder does not have any idea if the share is scrambled or un-scrambled, neither is he aware of true hidden index.

Acknowledgments

The corresponding author deeply acknowledges the guidance and inspiration by his Ph.D. guide Prof. (Dr.) M K Ghose, Dean Academics, Sikkim Manipal Institute of Technology, Sikkim, India. The author also deeply appreciates the contribution of Mr Kaushik Bandyopadhyay and Mr Rituraj Thakur, Final Year B. Tech Computer Science and Engineering students for their contribution towards the work.

References

[1] M. Naor and A. Shamir, Visual cryptography in, ‘‘Advances in Cryptology Eurocrypt ’94’’, (A. De Santis, Ed.), Lecture Notes in Computer Science, Springer-Verlag, Berlin, vol. 950, pp. 1 -12, **(1995)**.

[2] O Kafri and E. Keren, “Encryption of pictures and shapes by Random Grids.” Optics, Letters, **(1987)**, pp. 377–379.

[3] S. Gurung, G. Ojha and M. K. Ghose, “Multiple Image Encryption using Random Circular Grids and Recursive Image Hiding”, International Journal of Computer Applications, vol. 86, no. 10, **(2014)**.

[4] T.-H. Chen, K.-H. Tsao and K.-C. Wei, “Multiple-Image Encryption by Rotating Random Grids‖”, IEEE Computer Society Magazine, **(2010)**.

[5] M. K Ghose, S. Gurung and A. Aggarwal, “Multiple Information Hiding using Spherical Random Grids”, Procedia Journal, **(2015)**.

[6] S. Gurung, K. P. Choudhury, A. P. and K. Panghaal, “Multiple Information Hiding using Cubical Approach on Random Grids”, International Journal of Computer Networks and Information Security **(2015).**

[7] T.H. Chen, K.H. Tsao and K.C. Wei, “Multiple-image encryption by rotating random grids”, Proceedings of the 8th International Conference on Intelligent System Design and Applications, **(2008)**.

Authors

Sandeep Gurung received M.Tech degree in Computer Science and Engineering from Sikkim Manipal Institute of Technology, India. He is currently working as Assistant Professor in the Department of Computer Science and Engineering, Sikkim Manipal Institute of Technology, Sikkim. His research interests include Cryptography, Distributed System and Soft Computing.

Preyansh Singh Matharoo is pursuing Bachelor’s degree in Computer Science Engineering from Sikkim Manipal Institute of Technology and is currently interning at Wells Fargo India Solutions. His research interest lies are Cryptography and Machine Learning.

Mrinal Kanti Ghose is currently working as Dean (Academics) & Professor in Computer Science & Engineering Department, Sikkim Manipal Institute of Technology, Majhitar, Sikkim, India. He is a formerly retired Senior Scientist from Vikram Sarabhai Space Centre & RRSSC (E), ISRO.