Meliorated Multi Layered Key Less Mechanism in Visual Cryptography

Kalyan Das, Sayantan Samajpati, Abhirup Das, Samir Kumar Bandyopadhyay

Abstract: *Visual Cryptography algorithm primarily ensures lossless recovery of the secret image, by breaking the secret message into multiple shares before sending through a channel, which increases the bandwidth requirement of the channel due to increase in the size. The proposed algorithm deals with this problem by using two exclusive locks on the image to be shared which are applied once on the sender side and once on the receiver side. Thereafter sender and receiver open's their individual locks to finally retrieve the secret image at the receiver end.*

Keywords: *Invariant image size, key less secret sharing, reversible (loss less) data hiding, secret sharing*

I. INTRODUCTION

The information to be shared is a valuable asset to every individual and organization. Due to rapid increase in technology usage and sharing of data, companies must ensure that data security and privacy remains a priority. The paper discusses about double lock method to ensure security while sharing data between parties without sharing of any key.

Data hiding can be defined as a process to hide data (representing some information) in such a form which is unreadable or meaningless to any party other than the intended receiver to whom the data was to be sent. Nowadays, during authentication, there is a requirement of shared public key between the sender and the receiver which occurs once at the very beginning of the exchange of data. However, this requires the involvement of a trusted third party to generate and distribute the shared key. Whereas in our proposed algorithm there is no requirement of any public key to be shared. Both the parties maintain their own private key which is used for encryption, thus adding two extra levels of security and hence no key sharing is required. In the said algorithm the PSNR has been exposed to be at least 60 and there is no data loss.

[1] In 1995, Naor and Shamir were the first to introduce a new cryptography scheme where the cypher text is decoded by the human visual system.

The idea was to break the secret image into multiple shares where any single share wouldn't disclose the entire message but k out of n (k<=n) shares may be enough to recover the secret. However, (k-1) shares will give no information about the secret image.

[2][11] In the stated algorithm it requires multiple shares with dimensions identical to the original image to be generated for sharing of the data which therefore increases the channel bandwidth.

[3][4][5][6][7] In the stated respected papers due to pixel expansion or breaking into shares the volume to be sent increases. Here we have solved by encrypting the image twice thereby not requiring k out of n shares scheme.

[12] In some visual cryptography schemes, prior to sharing an image either noise was added to the image or after encrypting the image in meaningless image was then embedded in a meaningful cover image before sharing the image. This requires the knowledge of where each pixel is embedded to be known at the time of decoding. Also it increases the overall payload of the secret as it's impossible to keep the cover image meaningful if the secret and cover images are of the same dimensions without having considerable amount of distortions in the cover.

[8][9][10] Some visual cryptography scheme also suffers from increase in the volume to be shared over a channel due to breaking the image and embedding the secret and breaking it into multiple shares.

[13] The stated algorithm uses random permutation to generate n shares for their k out of n share scheme. The idea of sharing meaningless shares, although one of the most trivial, but used plenty in visual cryptography schemes.

[14][15] Another form of visual cryptography takes into aspect a key sharing scheme where a secret key is sent to the receiver through a secret channel prior to the exchange of data. However, in this proposed algorithm we have gotten rid of it using a new form of secret sharing in which the two parties share the same image three times between them instead of traditional methods which requires only once for the secret data and one for the secret key In another form of key based secret sharing requires generation of two keys (viz. private, public) where the sender encrypts the data using private key and the receiver decrypts the data using the public key shared by the sender and the private key of the receiver. Moreover, since these individual shares are illogical containing certain parts of the message within them using the visual cryptography scheme.

Revised Manuscript Received on May 25, 2020.
* Correspondence Author

Kalyan Das*, Assistant Professor, Department of Information Technology, St. Thomas' College of Engineering and Technology, Kolkata, India.

Sayantan Samajpati, Student, Department of Information Technology, St. Thomas' College of Engineering and Technology, Kolkata, India.

Abhirup Das, Student, Department of Information Technology, St. Thomas' College of Engineering and Technology, Kolkata, India.

Prof. Samir Kumar Bandyopadhyay, Professor, Department of Computer Science & Engineering, University of Calcutta, India.

Retrieval Number: E9303069520/2020©BEIESP
DOI: 10.35940/ijeat.E9303.069520
Journal Website: www.ijsce.org

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication
© Copyright: All rights reserved.

II. PROPOSED METHOD

The proposed method requires the image to be sent twice between the sender and receiver, since both the parties involved initially lock the image using mutually exclusive pixel operations and then turn by turn de-crypt their encryption during the description phase to get back the initial image.

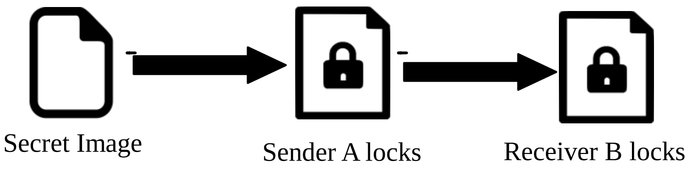

Fig. 1. Encryption Steps

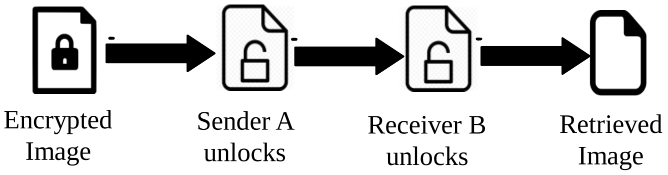

Fig. 2. Decryption Steps

We have used simple matrix layer operations and circular pixel rotations as our mutually exclusive pixel operations to illustrate the above-mentioned method. The below figure represents the 'layers of a matrix'.

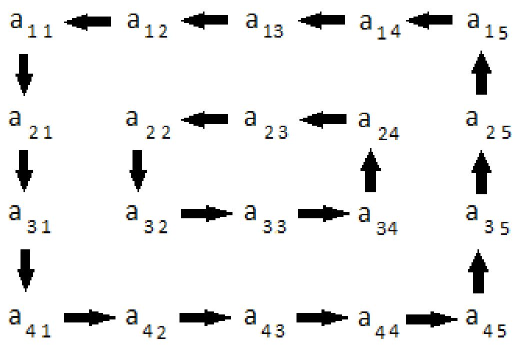

Fig. 3. Matrix layer rotation

For a 4 * 4 matrix we have 2 layers and for each element of the outer layer we have (12 – 1) positions to place that element. Similarly, for the inner layer, each position can be placed in (4 – 1) different places.

The method was tasted on Lena and PSNR of the final image is above 60db. This method is proposed for tackling increase of the total size of the shares when sharing a secret image.

III. MATH

The proposed method uses simple reversible matrix operations for generating the encryption of the secret image there by the share size is same as the secret image.

For an image of size R x C:

K = Ri x Ci – (Ri – 2) x (Ci – 2) gives us the number of pixels in the outermost layer. Similarly, for each pixel, the decimal value can be represented by 8 bits in binary on which circular rotation may be applied for a given offset.

The matrix layer rotation can be performed by the following pseudo code

The brute force to break the encryption will therefore require to try Pl = Σ {Ri x Ci - (Ri – 2) x (Ci - 2)} possibilities to break only the layer rotation. And for each such pixel B encrypts by rotating the binary bits of the binary representation of each pixel, i.e.; Pb = 8 * (min (R, C) / 2). Therefore after both A's and B's encryption total possibilities to check is Pl x Pb.. The larger the image, more securely will the image be encrypted.

The above implementation can be made more robust if randomness is introduced when setting the offset for both rotations in layers and circular shifts in binary bits. Even the direction of rotation can be randomized resulting in a more complex encryption.

A. Steps for Encryption

Here the proposed method of using two exclusive encryption algorithms is implemented using the simple matrix layer rotation and rotation of the bits of binary representations of the pixels of the image.

Step 1: A generates an offset by which every layer of the image matrix needs to get rotated in the clockwise direction. The layers of the image matrix can be found by simply subtracting all the pixels inside a given row and column. In other words, the difference between the area of the original matrix and the area of the matrix with one less row and column give the number of pixels in a given layer. These pixels can be accesses using the following formula:

Ri x Ci – (Ri+1 – 2) * (Ci+1 – 2)

Here (R x C) is the matrix size where R is the number of rows and C is the number of columns

A rotates all the pixels in the given layer by the set offset value and send the rotated image to B.

Step 2: B receives the image and sets the pixel offset by which the binary representation of each pixel in a given layer is to be rotated in the clockwise direction. The final image after rotating all the pixels is sent back to A thereby putting an extra level of security on top of what A already provided.

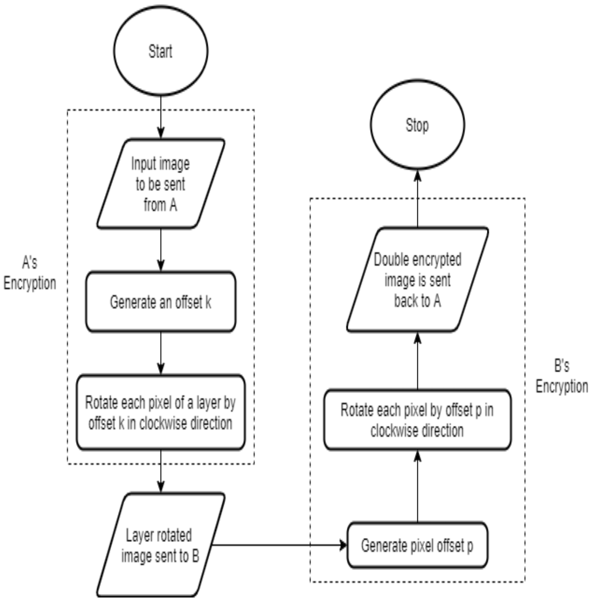
Start
Input image to be sent from A
Generate an offset k
Rotate each pixel of a layer by offset k in clockwise direction
A's Encryption
Layer rotated image sent to B
Generate pixel offset p
Rotate each pixel by offset p in clockwise direction
Double encrypted image is sent back to A
B's Encryption
Stop

Fig. 4. Flowchart of encryption

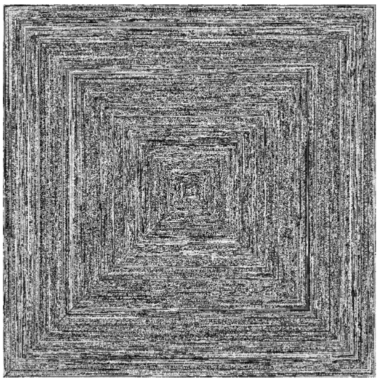

Fig. 5. Lena Image after encryption

B. Steps for Decryption

This proposed method does not require the presence of any secret channel or any form of shared keys. Therefore, the entire secret image can be losslessly recovered or retrieved from just the two shares of the secret image. The steps involving the retrieval of the image are as follows:

Step 1: Now A receives the image with the rotated pixels. Now it re-rotates the layers in the anticlockwise direction by the same set offset in Step 1 thereby unlocking the encryption of the image initially set by A but keeps the rotated pixels as done by B untouched. Now this re-rotated image is sent back to B.

Step 2: B receives the re-rotated layers of the image (after A unlocked its own encryption) and itself undoes the rotation in the binary representation of the pixels in a given layer by the initially set offset in Step 3 thereby unlocking all the locks set on the secret throughout the previous steps of the proposed algorithm, hence retrieving the original secret image meant to be sent by A.

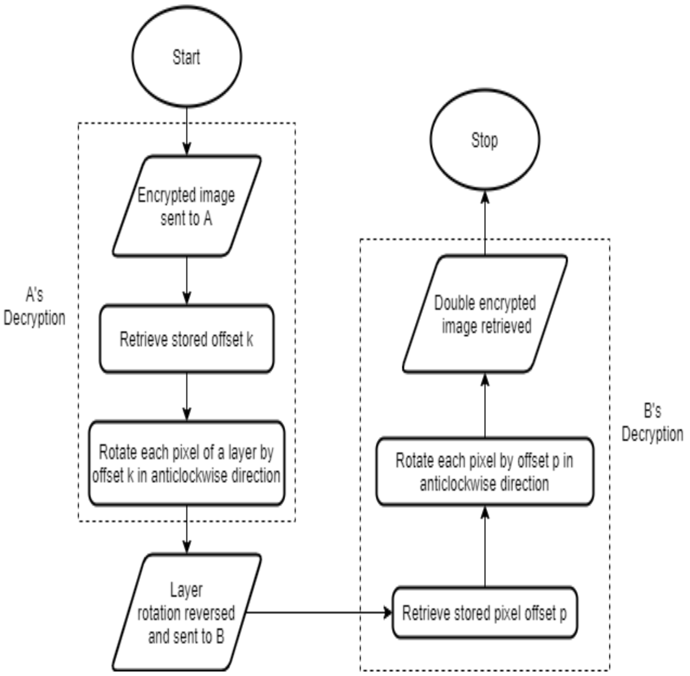
Start
Encrypted image sent to A
Retrieve stored offset k
Rotate each pixel of a layer by offset k in anticlockwise direction
A's Decryption
Layer rotation reversed and sent to B
Retrieve stored pixel offset p
Rotate each pixel by offset p in anticlockwise direction
Double encrypted image retrieved
B's Decryption
Stop

Fig. 6. Flowchart of decryption

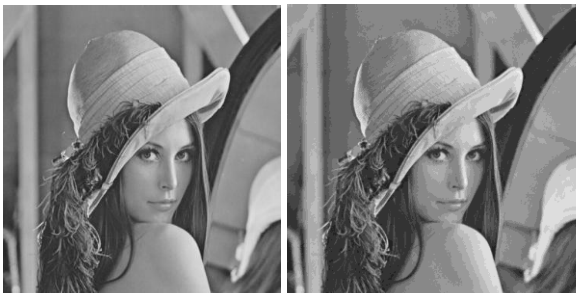

Fig. 7. Lena image: (a) original image, (b) after extraction (PSNR = 76.75 dB)

IV. RESULT ANALYSIS

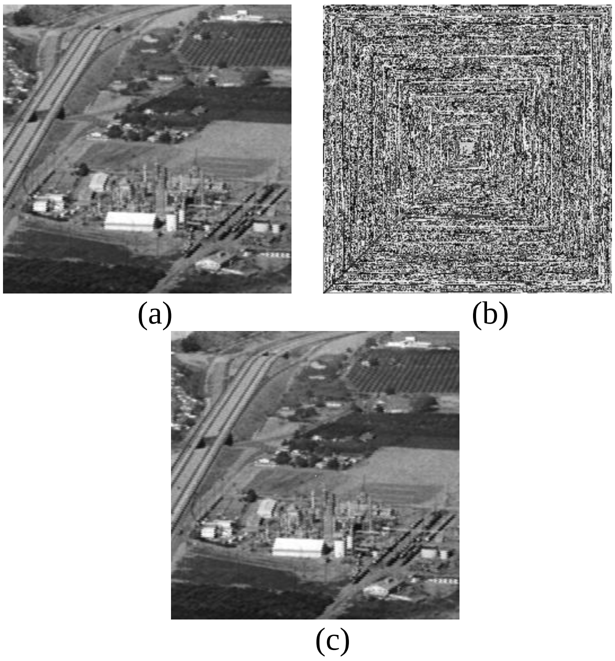

Fig. 8. Aerial image: (a) original image, (b) after encryption, and (c) after extraction (PSNR = 75.76dB)

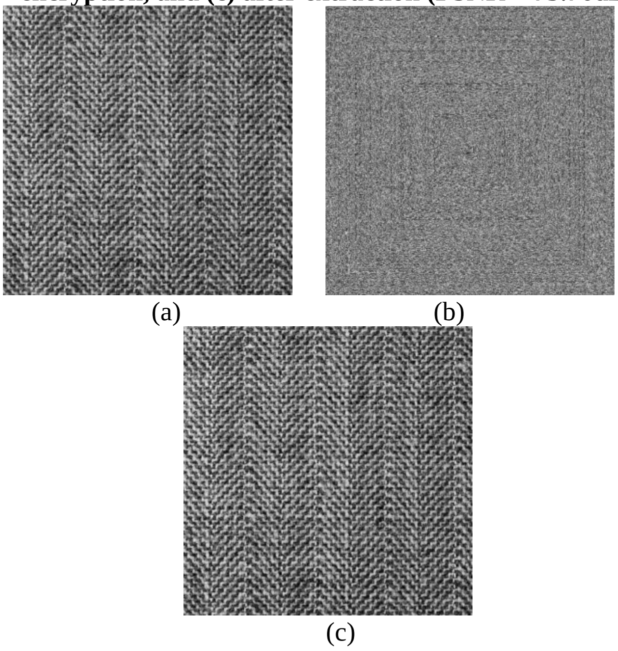

Fig. 9. Carpet image (texture): (a) original image, (b) after encryption, and (c) after extraction (PSNR = 94.35dB)

Retrieval Number: E9303069520/2020©BEIESP
DOI: 10.35940/ijeat.E9303.069520
Journal Website: www.ijsce.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication
© Copyright: All rights reserved.

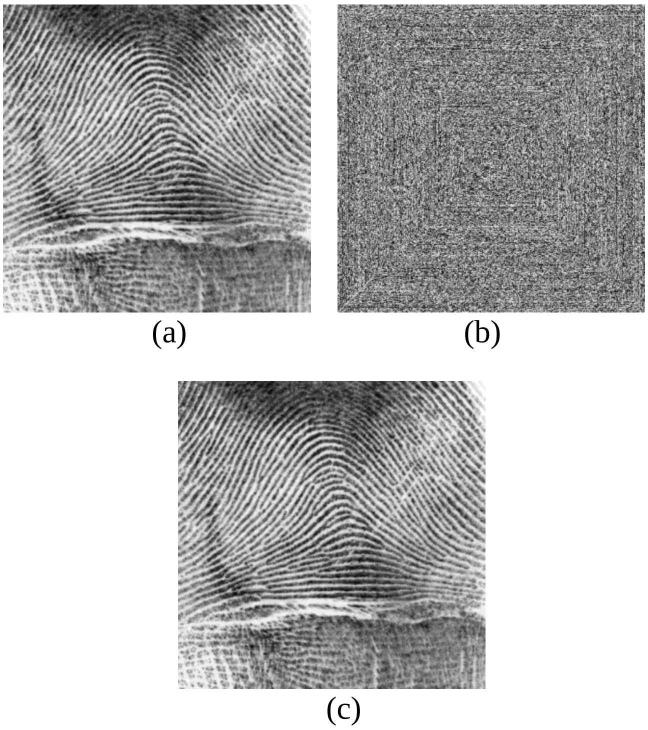

Fig. 10. Fingerprint image: (a) original image, (b) after encryption, and (c) after extraction (PSNR = 69.13dB)

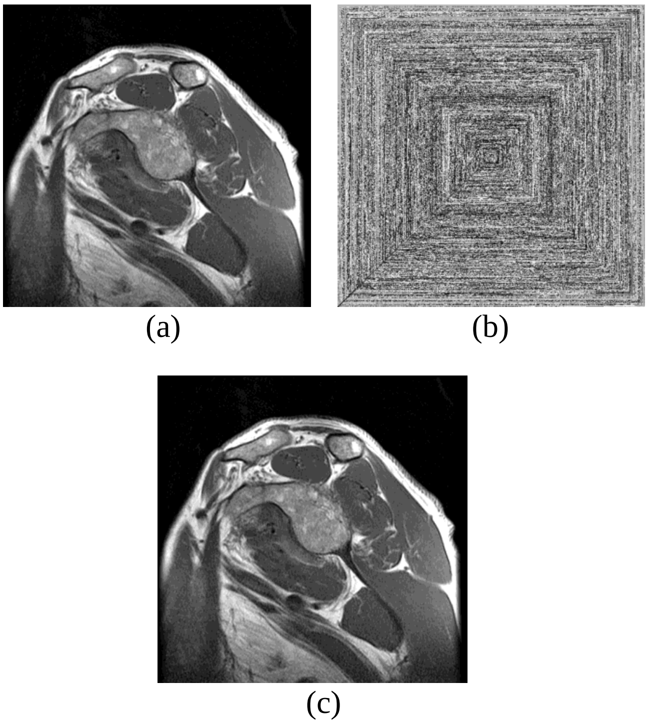

Fig. 11. MR image (medical): (a) original image, (b) after encryption, and (c) after extraction (PSNR = 87.01dB)

The double lock encryption and decryption algorithm has been applied on various images, including some classic used images, medical images, texture images, fingerprint images and vehicle images. The following tables shows the experimental results obtained by applying the proposed algorithm on certain images:

Table 1 Experimental Results For Some Classic Used Images

Images (512x512)	PSNR of retrieved image (dB)
Lena	76.75
Bridge	67.29
Cameraman	73.09
Clown	76.01
Couple	67.79
Crowd	75.19
Girl face	71.17
Man	96.29
Zelda	67.83

Table 2 Experimental Results For Six Texture Images

Images (1024x1024)	PSNR of retrieved image (dB)
Carpet	94.35
Blobs	63.58
Brick wall	100
Texture 1	86.05
Texture 2	87.13

Table 3 Experimental Results For Three Fingerprint Images

Images	PSNR of retrieved image (dB)
Fingerprint 1	80.73
Fingerprint 2	69.13
Fingerprint 3	74.66

Table 4 Experimental Results For Five Medical Images

Images (256x256)	PSNR of retrieved image (dB)
Brain	72.71
Heart	75.46
Muscle	78.23
X-ray	75.76
MR	87.01

Table 5 Experimental Results For Eight Aerial Images

Images (256x256)	PSNR of retrieved image (dB)
Aerial 1	74.15
Aerial 2	78.23
Aerial 3	75.76
Aerial 4	75.08
Aerial 5	90.27
Aerial 6	74.72
Aerial 7	74.72
Aerial 8	73.62

V. CONCLUSION

This proposed algorithm unlike the previous algorithms doesn't require sharing of any keys and the shares over any public channel of the same volume as the message. To any middle man without proper access to the state of the algorithm the shared media over the channel will make no sense to the eye.

The PSNR value as tested over multiple images have been noticed to be at least 60dB. The complexity of the proposed algorithm is directly dependent on the size of the secret image to be shared. So, the bigger the size of the image or the more the number of channels in the secret image the brute force for breaking the encryption scheme will be higher thereby more securely hiding the secret from any unwanted individual(s).

The double lock method used ensures authentication of the secret image without passing any public key. This method can even securely share colored secret image (with even higher degree of encryption).

REFERENCES

1. Naor, M., & Shamir, A. (1995). Visual cryptography. Lecture Notes in Computer Science, 1–12.
2. Shankar, K., & Eswaran, P. (2017). RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Communications, 14(2), 118–130.
3. Jin, D. (2005). Progressive color visual cryptography. Journal of Electronic Imaging, 14(3), 033019.
4. Blundo, C., & De Santis, A. (1998). Visual cryptography schemes with perfect reconstruction of black pixels. Computers & Graphics, 22(4), 449–455.
5. Monoth, T., & Babu, A. P. (2007). Recursive Visual Cryptography Using Random Basis Column Pixel Expansion. 10th International Conference on Information Technology (ICIT 2007).
6. Weir, J., & Yan, W. (2009). Sharing multiple secrets using visual cryptography. 2009 IEEE International Symposium on Circuits and Systems.
7. Shanmugasundari, T., Subban, R., Shanmugamoorthy, S., & Manogari, S. (2017). Research on Visual Cryptography Methods. 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC).
8. Young-Chang Hou, Shih-Chieh Wei, & Chia-Yin Lin. (2014). Random-Grid-Based Visual Cryptography Schemes. IEEE Transactions on Circuits and Systems for Video Technology, 24(5), 733–744.
9. Zhi Zhou, Arce, G. R., & Di Crescenzo, G. (2006). Halftone visual cryptography. IEEE Transactions on Image Processing, 15(8), 2441–2453.
10. Hou, Y.-C. (2003). Visual cryptography for color images. Pattern Recognition, 36(7), 1619–1629.
11. Monoth, T., & Babu, A. P. (2007). Recursive Visual Cryptography Using Random Basis Column Pixel Expansion. 10th International Conference on Information Technology (ICIT 2007).
12. Lee, K.-H., & Chiu, P.-L. (2012). An Extended Visual Cryptography Algorithm for General Access Structures. IEEE Transactions on Information Forensics and Security, 7(1), 219–229.
13. Lin, C.-C., & Tsai, W.-H. (2003). Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, 24(1-3), 349–358.
14. Chang, C. C. and Yu. T. X., Sharing a Secret Gray Image in Multiple Images, in the Proceedings of International Symposium on Cyber Worlds: Theories and Practice, Tokyo, Japan, Nov. 2002, pp.230-237.
15. Youmaran, R., Adler, A., & Miri, A. (n.d.). An Improved Visual Cryptography Scheme for Secret Hiding. 23rd Biennial Symposium on Communications, 2006.

AUTHORS PROFILE

Kalyan Das, Assistant Professor of Information Technology St. Thomas' College of Engineering and Technology

Sayantan Samajpati student of St. Thomas' College of Engineering and Technology, Information Technology 4th year.

Abhirup Das student of St. Thomas' College of Engineering and Technology, Information Technology 4th year.

Prof. Samir Kumar Bandyopadhyay, Professor of Computer Science & Engineering, University of Calcutta.