Secure Image Over Cloud Using Visual Cryptography

Siva Pavani B[1], S.V.S. Santhi [2], Tarun Kumar D[3], Mounika D[4], Gopi D[5]

[1]Student, Dept. of CSE, Vignan's Lara Institute of Technology, Andhra Pradesh, Guntur, India
[2]Associate Professor, Dept. of CSE, Vignan's Lara Institute of Technology, Andhra Pradesh, Guntur, India.
[3]Student, Dept. of CSE, Vignan's Lara Institute of Technology, Andhra Pradesh, Guntur, India
[4]Student, Dept. of CSE, Vignan's Lara Institute of Technology, Andhra Pradesh, Guntur, India
[5]Student, Dept. of CSE, Vignan's Lara Institute of Technology, Andhra Pradesh, Guntur, India

---***---

Abstract - *With the rapid development of computer and communication technology, more and more confidential information is transmitted through the Internet. Therefore, safeguarding the confidential information from being suspected and decrypted has become critical research area. This paper proposes a new secret visual cryptography [1], scheme for color images based on XOR technique. The visual cryptography involves encryption and decryption. During the encryption process, initially, a chromatic image is decomposed into three monochromatic images in tones of Red, Green and Blue. Then, these three images are transformed into Shares using the XOR technique. During the decryption process, the XOR operation is performed on shares to retrieve the monochromatic images. Finally these monochromatic images are combined to reconstruct the original image. To verify the originality of the decrypted image, Structure Similarity Index Measure (SSIM) is used.*

***Key Words*: Cryptography, Visual Cryptography, XOR implementation; SSIM comparison.**

1. INTRODUCTION

There is instantaneous popularization of e-commerce and e-government at present. A lot of the multimedia information transmits and exchanges through network every day. Data such as digital image, video etc., are very easy to be intercepted illegally when they are transmitted in the network.

Cloud storage is considered an international transfer of data. It has different servers that are accessed over the internet. Hence many organizations prefer to store their data in the cloud. So, the data must be safe enough to preserve the sensitive information. To secure data over transmission and huge storage medium such as cloud, we propose the solution supported by visual cryptography.

Cryptography mainly involves Encryption and Decryption. Encryption is the process used for converting readable data into unreadable format by using different algorithms. The results of strategies are nothing but the encrypted information. The reverse of this process is termed as decryption.

Visual cryptography is a cryptographic technique which allows visual information like pictures, text, etc., to be encrypted in such a way that the decryption can be performed by human visual system.

Visual cryptography is a secret sharing method that uses human eyes to decrypt the secret. It has computation-free decoding process to decrypt the images. Generally visual cryptographic methods utilize the technique of secret sharing in which secret image is divided into shares and when k shares out of n stack together will reveal the secret image.

In real time, the cryptography is applied to secure sensitive information in Hospitals. Medical data of patients are very sensitive and required to be shield throughout the storage, particularly over the cloud, and through the transmission between 2 hospitals.

2. RELATED WORK

Thomas Monoth and Babu Anto P proposed [2], a new visual cryptography scheme Using Random Basis Column Pixel Expansion. In this method, initially during Encryption, the original secret image is encrypted into n number of shares in a recursive manner, which have dimensions identical to secret image. Then the shares are again encoded into n sub shares recursively. Further, while decrypting, the shares are recovered by stacking the sub shares. Finally the secret image is recovered by stacking the shares. Using this process the author improved the level of Security of the encrypted image.

Qiudong Sun et al. presented [3], a random scrambling algorithm based on bit-planes of image, to aim at the positions interchange of pixels and their gray values change at the same time. Initially, the gray image is decomposed into several bit-plane images. Then their pixel positions were shuffled by a random scrambling algorithm separately. Finally, the scrambled bit-plane images are merged according to their original levels on bit-planes and gained an encrypted image. The proposed algorithm has better efficiency and properties than the general random scrambling method (Arnold transform).

Manimurugan.S and Ramajayam.N proposed [4], a new visual cryptography scheme to decrypt image with quality and no pixel expansion. In this method, initially during Encryption, the original secret image is encrypted into n number of shares by Visual cryptography based on optimization techniques with no pixel expansion. Then the shares are compressed by Modified RLE compression. After that, while decrypting, the shares again decompressed RLE process. It is a lossless algorithm. RLE is probably the easiest compression algorithm. Finally after finishing the decompression, shared images are stack together by “OR” operation. Based on this process we can improve the display quality of the recovered image as well as the security of the recovered image.

Quist-Aphetsi Kester proposed [5], an Image Encryption based on the RGB pixel Transposition and Shuffling Method. In this method to encrypt the image initially, import data from image and create an image graphics object by interpreting each element in a matrix. Secondly, extract the red, green and blue components and reshape these components into one-dimensional arrays. By using these three arrays form a column matrix and transpose the column matrix. Further reshape the transposed matrix into one-dimensional array. Then divide the resulted one-dimensional array into three vector parts, such as from first part to one third part of one-dimensional array, from one third part to two third part of one-dimensional array and from two third part to nth of one-dimensional array. Transform these three vectors into a matrix with same dimension of red or green or blue component of the original image. Finally, the data will be converted into image format to get the encrypted image. The inverse of the whole process will decrypt the encrypted image back into the original image.

Himani Mehra et al. proposed [6], a new visual cryptography scheme using steganography. Hiding the information by embedding secret data into safe medium is referred as steganography. Visual cryptography mainly involves encryption and decryption. Initially during Encryption, the original secret image is embedded into least significant bit (LSB) of the cover image using Steganography (resultant image is known as Steg-Image) and using genetic algorithm pixel values of Steg-Image are modified. Then the shares are generated for the Stego Image. During decryption, the shares are stacked to get the original image with hidden data. Then Inverse steganography is used to retrieve the original image.

3. PROPOSED WORK

The proposed methodology uses visual cryptography scheme. This methodology involves three phases. The first phase performs decomposition of original image into three primitive color channels. The second phase performs Encryption which involves generation of shares using XOR implementation and the third phase performs Decryption which involves reconstruction of shares using XOR operation.

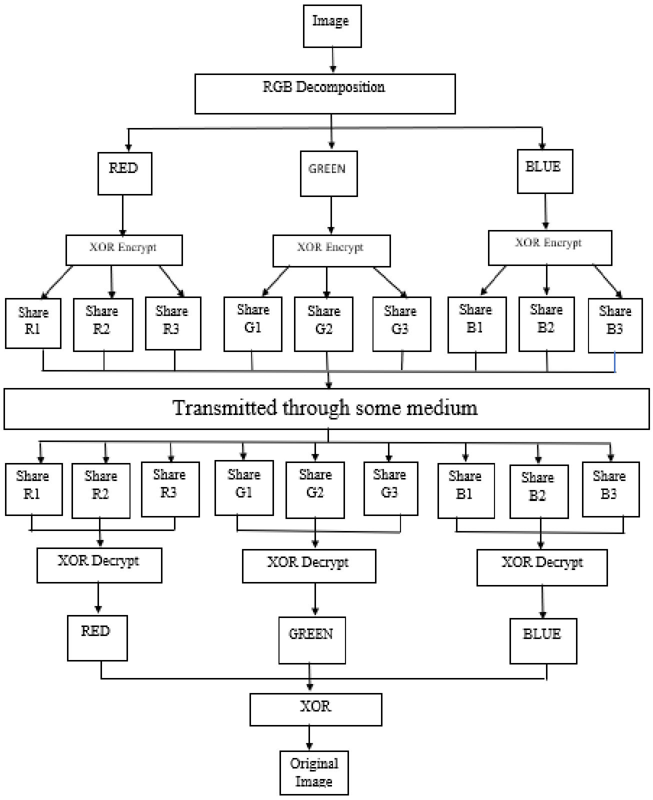

Figure 1: Architecture of XOR based visual cryptography scheme

Phase 1: RGB decomposition

In this phase the chromatic image is taken as input. Then from each pixel of the chromatic image the amount of red, green, blue colors are extracted. Then based on amount of the colors the chromatic image is divided into three monochromatic images namely red(R), green(G), blue(B).

Algorithm:

Input: Image

Output: Individual RGB color components of Input Image.

Step 1: Extract amount of Red color from each pixel of the Input Image and consider the resultant image as R.

Step 2: Extract amount of Green color from each pixel of the Input Image and consider the resultant image as G.

Step 3: Extract amount of Blue color from each pixel of the Input Image and consider the resultant image as B.

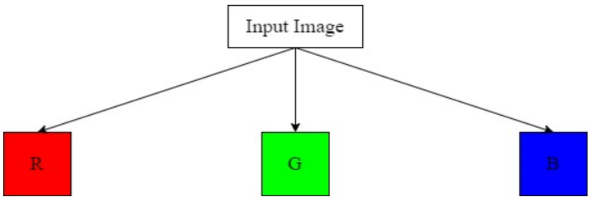

Figure 2: RGB decomposition

Phase 2: Encryption (Generation of shares)

The individual color components are converted into shares which are in unreadable format. These shares will be the encrypted data.

Algorithm:

Input: Individual RGB color components.

Output: The generated shares which are in unreadable format.

Step 1: Extracting the pixel values of each color component and generate basic matrix for each color component.

Step 2: Generate two random matrices for each individual color component.

Step 3: Assign first random matrix to share2 and second random matrix to share3 of the respective color component.

$\text{Share2\_R} = K_{R1}$ $\text{Share2\_G} = K_{G1}$ $\text{Share2\_B} = K_{B1}$

$\text{Share3\_R} = K_{R2}$ $\text{Share3\_G} = K_{G2}$ $\text{Share3\_B} = K_{B2}$

Step 4: Perform XOR operation between respective color component and its first random matrix and again perform XOR operation between resultant matrix and perspective color component second random matrix. Now consider the resultant matrix as share 1.

$$\text{Share1\_R} = \text{Basic\_ R} \wedge K_{R1} \wedge K_{R2}$$

$$\text{Share1\_G} = \text{Basic\_ G} \wedge K_{G1} \wedge K_{G2}$$

$$\text{Share1\_B} = \text{Basic\_ B} \wedge K_{B1} \wedge K_{B2}$$

Step 5: Repeat above step 4 until each color component generates shares

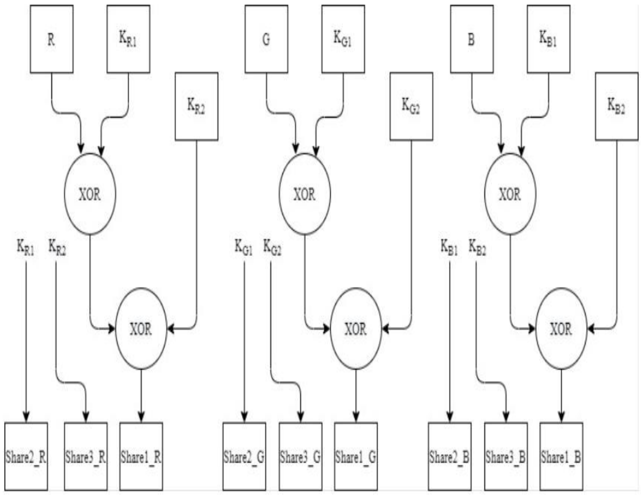

Figure 3: Generation of Shares

Phase 3: Decryption (Reconstruction of shares)

To reveal the encrypted image decryption has to be performed. The generated shares undergo the following steps to reveal the secret image.

Algorithm:

Input: The Encrypted Shares.

Output: Original Secret Image

Step 1: Extracting the pixel values of the each and every share generated by the encryption phase.

Step 2: All shares are combined together using XOR operations to retrieve the color components of the secret image individually.

$$S_R = \text{Share1\_R} \wedge \text{Share2\_R} \wedge \text{Share3\_R}$$

$$S_G = \text{Share1\_G} \wedge \text{Share2\_G} \wedge \text{Share3\_G}$$

S_B = Share1_B ^ Share2_B ^ Share3_B

Step 3: All individual color components combined together using XOR operations to retrieve the secret image.

Result Image = S_R ^ S_G ^ S_B

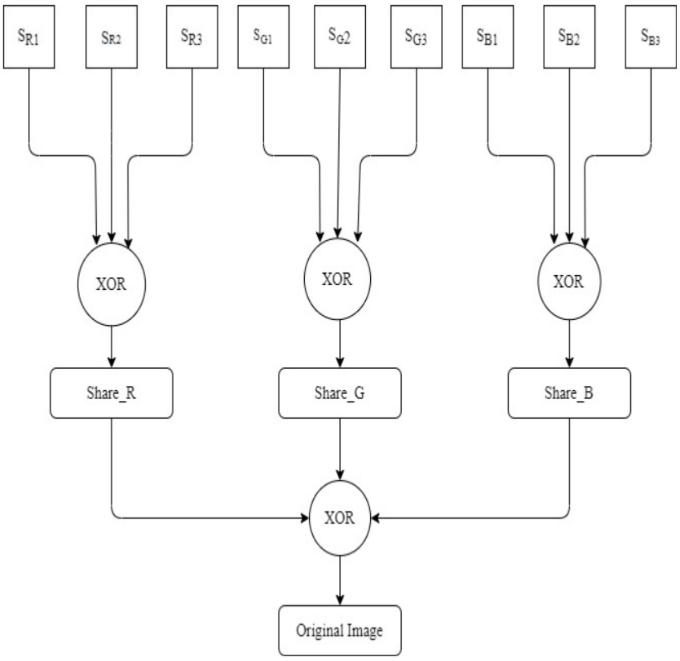

Figure 4: Reconstruction of Shares

4. RESULTS

Initially, the input taken is an image as represented in Figure 5.

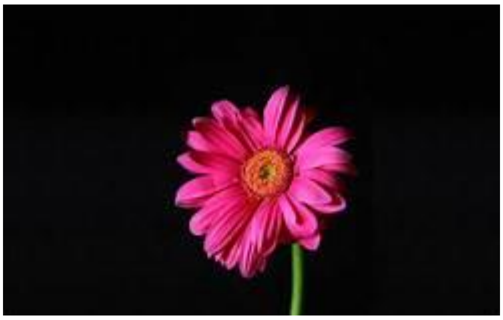

Figure 5: Input Image

Generated RGB components:

The input image is decomposed into three primitive color monotones namely Red(R), Green (G) and Blue (B) as shown in figure 5.1, figure 5.2 and figure 5.3 respectively.

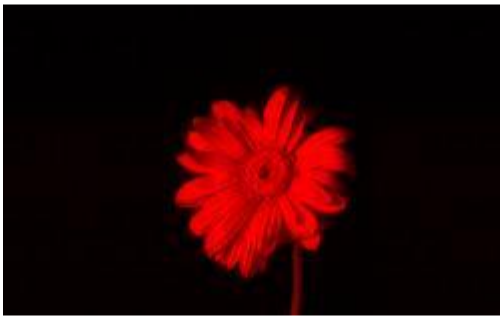

Figure 5.1: Red Component

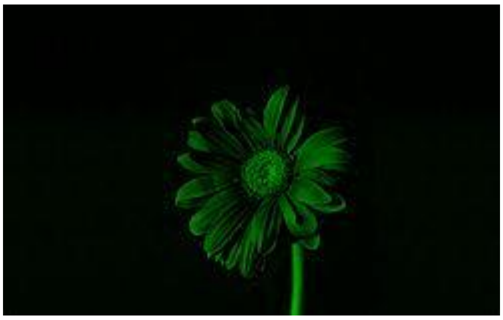

Figure 5.2: Green Component

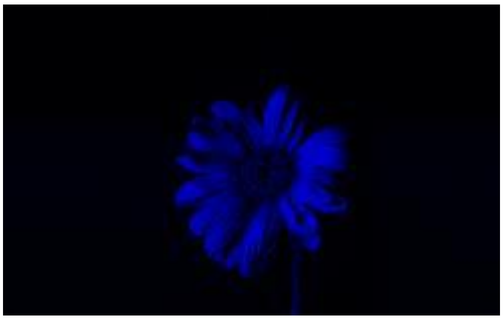

Figure 5.3: Blue Component

***Generated* Shares :**

After decomposition, three shares are generated for each color component as represented in figure 6.1 to figure 6.9.

Figure 6.1 : XOR_Share1_1

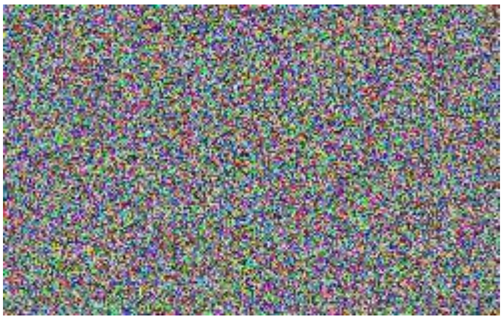

Figure 6.2 : XOR_Share1_2

Figure 6.3 : XOR_Share1_3

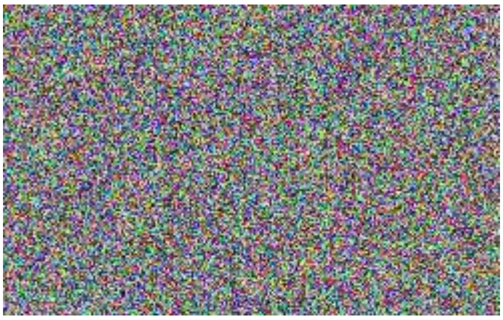

Figure 6.4 : XOR_Share2_1

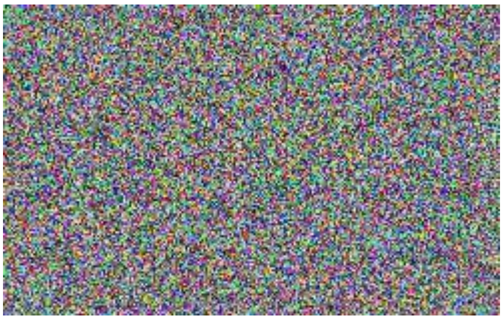

Figure 6.5 : XOR_Share2_2

Figure 6.6 : XOR_Share2_3

Figure 6.7 : XOR_Share3_1

Figure 6.8 : XOR_Share3_2

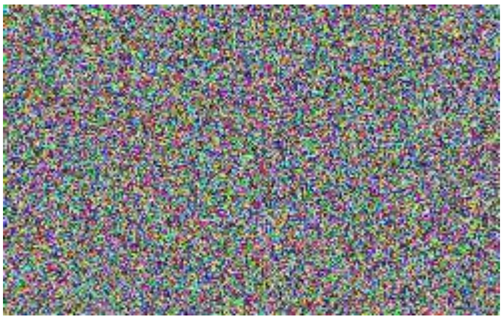

Figure 6.9 : XOR_Share3_3

***Reconstruction* Of Shares** :

After performing decryption operation the individual color components are retrived back as represented in figure 7.1 , figure 7.2, figure 7.3.

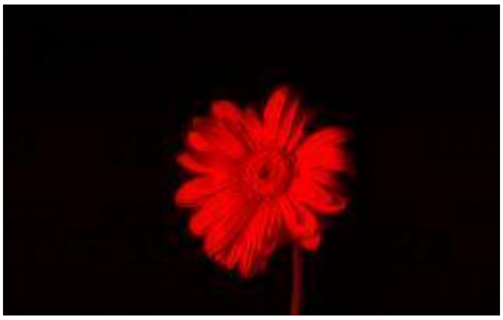

Figure 7.1 : Outpu1_XOR1

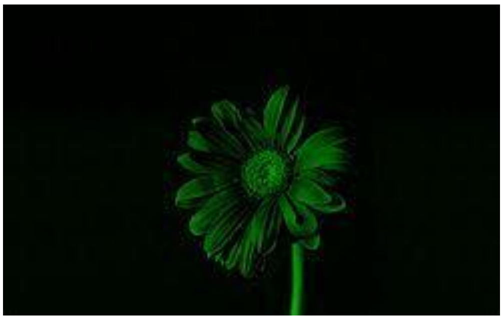

Figure 7.2 : Output_XOR2

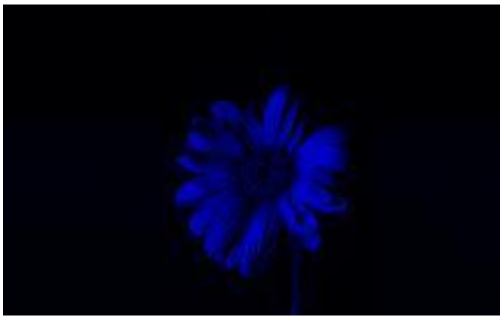

Figure 7.3 : Outpu1_XOR3

Combine Obtained Color Components:

After obtaining individual color components and combining them using XOR operation, figure 8 shows the Original ecrypted image.

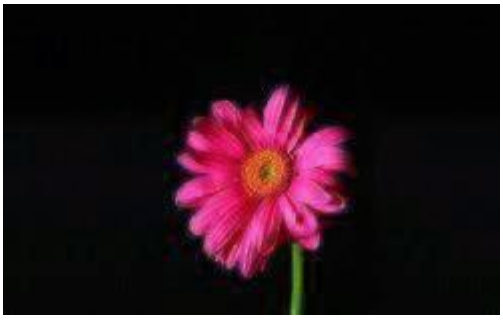

Figure 8 : Decrypted Image

SSIM (Structure Similarity Index Measure) :

The **structural similarity index measure** (**SSIM**) is a method for predicting the perceived quality of digital television and cinematic pictures, as well as other kinds of digital images and videos. SSIM is used for measuring the similarity between two images. The SSIM index is full reference metric in other words, the measurement or prediction of image quality is based on an initial uncompressed or distortion-free image as reference.

The value of SSIM is typically in the range **[0, 1]**. The value 1 indicates the highest quality and occurs when the result image and reference image are equivalent. Smaller values correspond to poorer quality. For some combinations of inputs and name-value pair arguments, SSIM can be negative.

Table 1: Accuracy of Decrypted Images

S.NO	**Input Image**	**Output Image**	**SSIM**
1			0.9752
2			0.8694
3			0.8975

4			0.8952
5			0.9899
6			0.9331

Result analysis

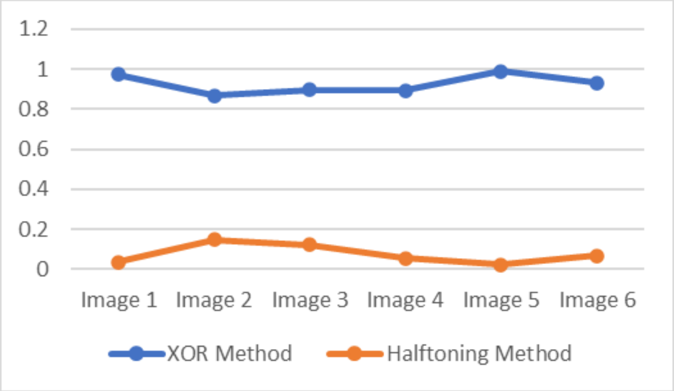

Figure 9: SSIM for XOR method and Halftoning method

The above 'figure 9' shows the comparison between SSIM values obtained for checking the quality of decrypted images after using existed method i.e. visual cryptography using halftoning method [7], and proposed method i.e. visual cryptography based on XOR implementation.

The lower orange color line in the above graph represents the SSIM values obtained for the 6 different input images and these values range from 0 to 0.25 approximately. The similarity between input and result image is approximately <= 25% only in case of visual cryptography using halftoning method.

The upper blue color line in the above graph represents SSIM values obtained for the same images which are used for existed method and the values range from 0.75 to 0.98 approximately. The similarity between input and result image is approximately 75% to 98% in case of proposed method visual cryptography based on XOR implementation.

5. CONCLUSIONS

In this paper we proposed an image encryption method based on RGB decomposition and XOR operation. The basic idea involves providing image quality without pixel expansion and security. The process involves decomposition of the image into RGB components and performing XOR based encryption to generate encrypted shares. From the SSIM values of decrypted images it is clearly shown that the decrypted image is approximately same as original image. Future work will be focused on the implementation of this algorithm for videos.

6. REFERENCES

[1] Moni Naor and Adi Shamir, "Visual Cryptography", In proceedings of Advances in Cryptology Eurocrypt 1994.

[2] Thomas Monoth and Babu Anto P, "Recursive Visual Cryptography Using Random Basis Column Pixel Expansion", 10th International Conference on Information Technology (ICIT 2007), 18 December 2007.

[3] Qiudong Sun, Wenying Yan, Jiangwei Huang, Wexin Ma, "Image Encryption Based on Bit-plane Decomposition and Random Scrambling ", 22 April 2012.

[4] Manimurugan.S and Ramajayam.N, "Visual Cryptography Based on Modified RLE Compression without Pixel Expansion ", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 3, September 2012.

[5] Quist-Aphetsi Kester, "Image Encryption based on the RGB PIXEL Transposition and Shuffling", I.J. Computer Network and Information Security, 2013, 7, 43-50, June 2013.

[6] Himani Mehra, Mr. Tarun kumar Sahu, Miss Garima Tiwari, "Steganography using Genetic Algorithm along with Visual Cryptography for Wireless Network Application", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 2, February 2016.

[7] Sneha Lokhande, Vishakha Autade, Soham Nale, VaradSupekar, A.A.Barbind , "Secure Medical data over cloud using visual cryptography ", MAT journals 2020.

BIOGRAPHIES

B. Siva pavani persuing final year B.Tech in the stream of Computer Science and Engineering at Vignan's Lara Institute of Technology and Science(VLITS), Vadlamudi, Guntur, Andhra Pradesh, India.

S.V.S. Santhi is an Associate Professor in Department of Computer Science and Engineering at Vignan's Lara Institute of Technology and Science (VLITS), Vadlamudi, Guntur, Andhra Pradesh, India. She received her Master's in Information Technology from Andhra University, Visakhapatnam in 2008 and PhD in Information Technology from GITAM University, Visakhapatnam, Andhra Pradesh, India in 2018. Her current research interests are data mining, graph mining and networking.

D. Tarun Kumar persuing final year B.Tech in the stream of Computer Science and Engineering at Vignan's Lara Institute of Technology and Science(VLITS), Vadlamudi, Guntur, Andhra Pradesh, India.

D. Mounika persuing final year B.Tech in the stream of Computer Science and Engineering at Vignan's Lara Institute of Technology and Science(VLITS), Vadlamudi, Guntur, Andhra Pradesh, India.

D. Gopi persuing final year B.Tech in the stream of Computer Science and Engineering at Vignan's Lara Institute of Technology and Science(VLITS), Vadlamudi, Guntur, Andhra Pradesh, India.