A Novel Image Transmission Technique via MIS using an Advanced AES Algorithm with Chaotic Map for Enhanced Security

Athira Leeladharan[1] A. S. Vibith[2]
[1]P. G Student [2]Assistant Professor
[1,2]Department of Computer Science and Engineering
[1,2]Kingston Engineering College, Vellore, India

Abstract— There are several image transmission techniques implemented in the recent world. But there are many compromises in them. Steganography and cryptography are the two main areas of secure data and multimedia transmissions. Here, a secure image transmission technique is introduced using the concept of Mosaic Image Steganography. In this technique we have two images, one being the secret image and the other being the target image. On the sender side the secret image is converted into a mosaic image. The mosaic image generated looks exactly like the pre-selected target image. This image is used as a camouflage of the secret image. It is generated by dividing the secret image and target image into fragments where each fragment of a secret image is called tile image and each fragment of a target image is called target block. Then we transform the color characteristics of the tile to those of the corresponding target block. Next, we embed the recovery information which is a bit steam into the created mosaic image using an improved LSB substitution technique with integer transformation. Before performing this step, we encrypt the recovery information with a secret key. The receiver uses the same key for decryption. To enhance security we encrypt the recovery information with an advanced AES algorithm using chaotic maps. The receiver first extracts the recovery information from the mosaic image using this key and then recovers the secret image using the recovery information.

Key words: LSB, Mosaic images, encryption, AES, chaotic maps

I. Introduction

Recent advances in Internet have made the multimedia communication more convenient and easy. However, the prevalence of these technologies has led to serious security concerns and handling needs. These issues have driven the research community to invent multimedia hiding techniques. In the recent world, many techniques have been developed for the secure transmission of multimedia data. But the common problem found in these techniques is that, they use data hiding and encryption to securely transmit information. These methods generate meaningless files that attract the attackers. Hence they find all the possible ways to decrypt the hidden information. Thus we implement a technique which can resolve the drawback mentioned above in the existing systems. Information hiding techniques have been developed widely both in academia and industry, which can embed a secret piece of text into another media like image, audio or video. This technique was known as Steganography. With the rise in the field of communication, people not only used texts but also images, audios and videos for effective communication. This introduced many Steganography techniques like image Steganography, which deals with hiding a secret image into another image, audio Steganography dealing with hiding a secret audio file into another audio and video Steganography which hides a video clip into another video. Steganography differs from cryptography in the sense that the cryptography [3] focuses on keeping the contents of a message secret whereas Steganography focuses on keeping the message secret. Once the presence of hidden information is identified, then the purpose of Steganography is partial. In this paper, we implement an improved version of Steganography known as the mosaic image Steganography.

II. Objective

The above mentioned security issues are overcome using a new technique known as Mosaic Image Steganography [6], [8]. The existing Steganography technique is improved by integrating a mosaic image concept into it. To implement the technique, we use two images as inputs namely, the secret image and the target image. The target image is arbitrarily selected without using a database. The secret image is completely converted to a so-called mosaic image by applying certain transformation and rotation functions. The mosaic image thus created and the target image looks exactly similar to each other. Thus the attacker will not have any confusion over such mosaic images. We also embed the recovery informations into the created mosaic image. In this way, we solve the drawback of the existing system. In order to enhance security, we encrypt the recovery informations using an advanced AES algorithm using a chaotic map.

III. Proposed System

The proposed system consists of 2 phases:

1) Mosaic Image Creation Phase
2) Encryption phase

A. *Mosaic Image Creation Phase:*

In this phase, we create a mosaic image out of two images one being the secret image and other the target image.

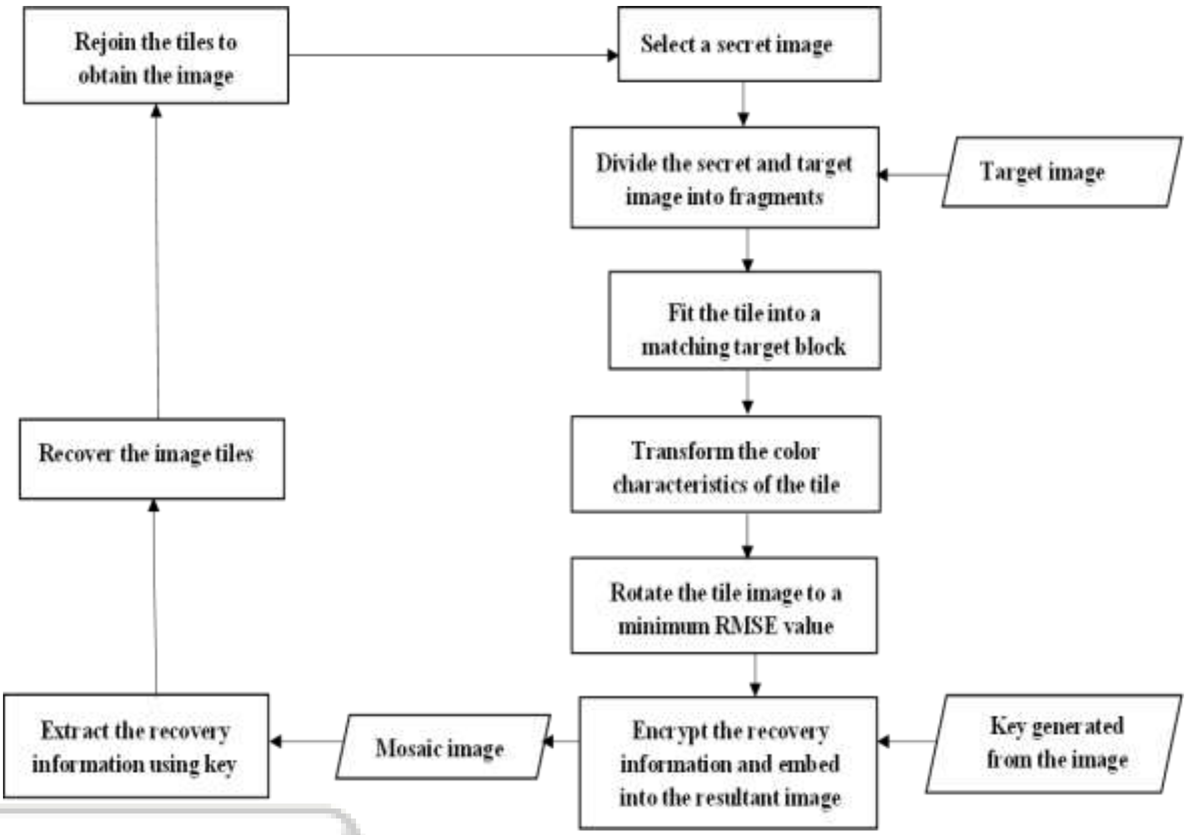

Rejoin the tiles to obtain the image
Select a secret image
Divide the secret and target image into fragments
Target image
Fit the tile into a matching target block
Recover the image tiles
Transform the color characteristics of the tile
Rotate the tile image to a minimum RMSE value
Extract the recovery information using key
Mosaic image
Encrypt the recovery information and embed into the resultant image
Key generated from the image

Fig. 1: Flow diagram of the proposed system

The mosaic image creation is divided into 5 stages:

– Transforming colours between Blocks

In order to transform the colour of the secret image to that of the target image, we divide both the image into blocks. The secret image is divided into several blocks where each block is known as tile image. Similarly the target image is also divided into fragments where each fragment is called target block. Each tile image consisting n pixels P_tile= {p_(1), 〖p〗 _(2),p_3 , …… , p_n } and each target block consists of n pixels P_target = {p_1^' , p_2^' , p_3^' , …… , p_n^'} where each pixel of the tile image is represented as p_(i)(r_i,g_i,b_i) and each pixel of the target block is represented as p_i^' (r_i^',g_i^',b_i^'). We then calculate the mean and standard deviation of the pixels using 2 formulae:

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i \qquad \mu_c' = \frac{1}{n}\sum_{i=1}^{n} c_i' \qquad (1)$$

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i-\mu_c)^2} \qquad \sigma_c' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i'-\mu_c')^2} \qquad (2)$$

Where c_i and c_i^' denote the color channel values of pixels p_i and p_i^' respectively with c = r, g or b. The new pixel value p_i^" (r_i^",g_i^",b_i^") is calculated using a formula:

$$c_i'' = q_c(c_i - \mu_c) + \mu_c' \qquad (3)$$

Here $q_c = \sigma_c'/\sigma_c$ is known as the standard deviation quotient. It is seen that the new mean and standard deviation of the resulting tile image is same as that of the target block. The original color values of the pixels are calculated by performing the reverse operation:

$$c_i = 1/q_c(c_i'' - \mu_c') + \mu_c \qquad (4)$$

– Selecting a matching target block to fit the tile image

In order to perform color transformation between blocks, we need to choose an appropriate target block for a particular tile. We use the standard deviation of the three channels for this purpose so as to select the most similar target block for the tile image. We sort the tile images to form a set 〖Tile={tile〗 _1, 〖tile〗 _2, 〖tile〗 _3, 〖tile〗 _4… 〖tile〗 _n} and the target block to form a set Target = { 〖target〗 _1, 〖target〗 _2, 〖target〗 _3,….. 〖target〗 _n} in the increasing order of the average values of standard deviations of the three colour channels. Finally, we take the first tile image of the set Tile i.e., 〖tile〗 _1 and the first target block in the set Target i.e., 〖target〗 _1, as a pair for the colour transformation, the second tile image and the second target block as a pair and so on.

– Rotating the blocks to fit better with minimum RMSE

This step is performed on the new block obtained after the colour transformations to avoid any further distortions that have occurred even after the transformation. The step is conducted by rotating the resulting tile image into any of the four angles$0^\circ, 90^\circ, 180^\circ$or 270° which gives a minimum root mean square error (RMSE) value.

– Handling overflows and underflows

After performing the color transformations on the pixels, some of the pixels may have a value above 255 termed as overflow whereas some pixels may have a value below 0 termed as underflow. We first convert the pixels above 255 to 255 and the pixels below 0 to 0. We then calculate the residual values by taking the difference between the original values of the pixels and the converted values. These values are later used for the recovery of the image. To determine the number of bits needed to represent the residual values we use a different approach. Using two formulae we calculate the smallest possible value in the tile image that is larger than 255, and the largest possible value that is smaller than 0.

$$c_S = \left\lceil \left(\frac{1}{q_c}\right)(255 - \mu_c') + \mu_c \right\rceil \qquad (5)$$

$$c_L = \left[\left(\frac{1}{q_c}\right)(0-\mu_c') + \mu_c\right] \qquad (6)$$

Next, the residual values are calculated as follows:

$|c_i - c_S|$ for an underflow value of c_i
$|c_L - c_i|$ for an overflow value of c_i

Thus all the possible values of residuals will have a range of 0 to 255. Hence we require 8 bits to represent them.

– Embedding the recovery information

In order to recover the image from the created mosaic image, the receiver requires the image recovery information. Thus we embed the recovery information also into the mosaic image so as to recover it during decryption. LSB technique [1], [10] was the primitive technique used for data hiding. Here, we improve the LSB technique, by applying a simple transformation on the pixels before embedding them. Specifically, let P (x, y) be a pixel pair which is transformed into P' (x', y') using the formulae:

$$x'=2x-y, \qquad y'=2y-x \qquad (7)$$

$$x=\left[\frac{2}{3}x' + \frac{1}{3}y'\right], \quad y= x=\left[\frac{1}{3}x' + \frac{2}{3}y'\right] \qquad (8)$$

This technique yields high data hiding capacity compared to the normal LSB technique and the complexity is low.

The information hidden into the mosaic image for later recovery of the secret image includes:

- The index of the target block
- The optimal rotation angle of the tile image
- The means and standard deviation quotient of tile and target block
- The residual values

These information are integrated to form a stream of bits:
M=$t_1 t_2 \ldots\ldots t_m r_1 r_2 m_1 m_2 \ldots\ldots m_{48} q_1 q_2 \ldots\ldots q_{21} d_1 d_2 \ldots\ldots d_k$

Here, m bits $t_1 t_2 \ldots\ldots t_m$ represents the index of the target block, 2 bits $r_1 r_2$ represents the optimal rotation angle of tile image, 48 bits $m_1 m_2 \ldots\ldots m_{48}$ represents the mean of tile and target block in which the mean of n pixels in one color value uses 8 bits. 21 bits $q_1 q_2 \ldots\ldots q_{21}$ represents standard deviation quotient in which the value in a single color channel uses 7 bits. $d_1 d_2 \ldots\ldots d_k$ represents the residual values of the pixels

1) Algorithm 1 Mosaic Image Creation

Input: Image in which data is hidden (cover image) and target image.

Output: Mosaic image

Steps:

1) Step 1: Divide the secret image into tile images and target image into target blocks.
2) Step 2: Calculate the mean and standard deviation of the tile image and the target block.
3) Step 3: Choose an appropriate target block for a particular tile image using the average of the standard deviation of the three colour channels.
4) Step 4: Transform the colour characteristics of the tile image with respect to the target block chosen for it.
5) Step 5: Rotate the tile image to an angle with minimum RMSE value.
6) Step 6: Calculate the residual values of the pixels with underflow and overflow.
7) Step 7: Generate a stream of bits that contain the recovery informations.
8) Step 8: Encrypt the recovery information using a secure key.
9) Step 9: Embed the recovery information into the generated mosaic image.

B. Encryption

In the proposed scheme, in order to enhance security we use an advanced form of AES algorithm. The existing AES technique is advanced by combining it with a chaotic map [2]. The technique was introduced by Ali Abdulgader, Mahamod Ismail, Nasharuddin Zainal, Tarik Idbeaa. Chaotic maps have gained extensive consideration from cryptography scholars who wish to develop new schemes for encryption. Chaotic encryption schemes are mainly developed using properties of chaos, including deterministic dynamics, random behavior, and nonlinear transform. These features allow chaos-based encryption to perform better confusion and diffusion in the encryption system.

Here we use a type of chaotic map called Arnold Cat Map, which can be expressed in matrix form:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix}$$

The encryption algorithm used here is a block cipher together with a chaotic system with the conventional encryption algorithms, such as AES [9], in CBC mode. This technique is implemented to increase the efficiency of the data encryption by making additional modifications to the existing AES algorithm [3]. These modifications focus on the reduction of the encryption and decryption time. The technique is used to encrypt the recovery information hidden in the mosaic image. These modifications are as follows:

- We implement some circular shift on the S-box based on the round keys in order to overcome the drawbacks of the fixed S-box and high calculation in the AES and improve key security.
- We replace the MixColumn step with the chaotic system to reduce the computation amount in the AES algorithm. The MixColumn stage which diffuses the data in the AES algorithm uses large calculations that slow down the AES algorithm. The remaining two stages are unchanged within the AES.

The proposed algorithm uses the principle of the shift register technique. During the encryption, the values in the AES S-box circularly right shift using a shift amount, which is based on the round secret key. The key is produced by the key schedule algorithm in the AES algorithm. Assuming the round key in ith round and the original AES S-box will be circularly shifted using the shift amount computed by the equation shown below, and then the new AES S-box now depends on the round key.

$$sh = \left(\sum_{m=1}^{m=16} round_{key_i}(m)\right) \bmod 16$$

In the permutation process, the positions of the element of the state array after the shift row stage are scrambled using an Arnold Cat Map. The general structure of the proposed algorithm is shown in Fig.4. The complete description of each step of the proposed method for encryption and decryption is as follows:

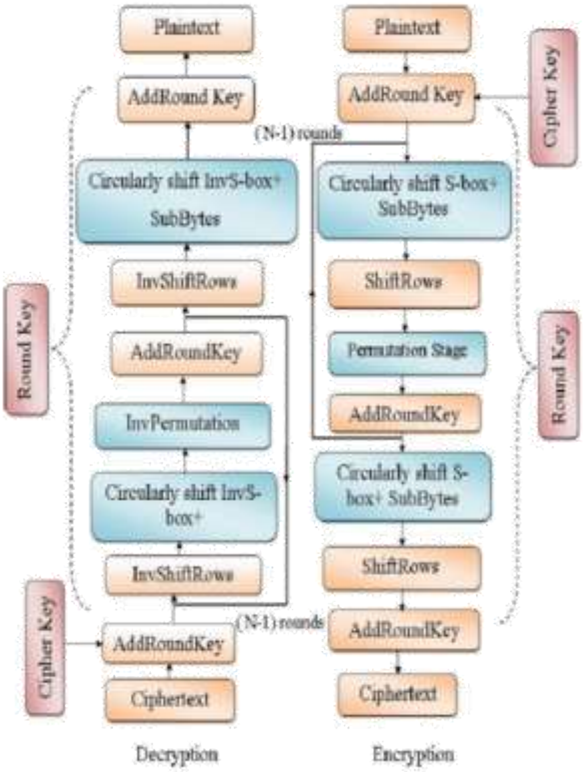
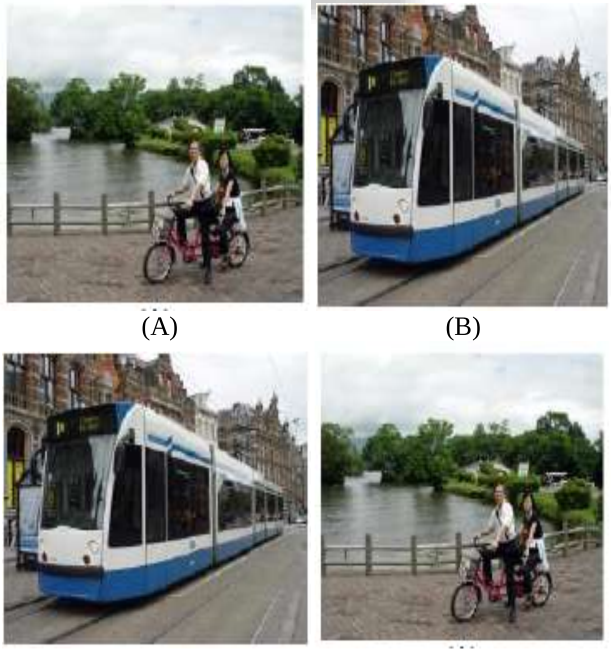


Fig. 2: General structure of the modified AES algorithm

IV. Results and Observations

The proposed system is tested with many images. The secret image and target image is considered to be of the same size. An example of the experimental results is shown in Figure 3. The created mosaic image which is created using figure 3(A) as the secret image and figure 3(B) as the target image is shown in figure 3(C). The recovered image using the correct RMSE value is shown in 3(D).


(A) (B)

(C) (D)

Fig. 3: Experimental results of the proposed method (A) Secret image (B) Target image (C) Mosaic image created with tile image size 8x8 (D) Recovered cover image using a correct key with RMSE=0.948

The tile image size is 8x8. We can see that the figures 3(C) and 3(B) are similar to each other. Similarly the figure 3(D) looks nearly identical to the original secret image shown in figure 3(A) with RMSE = 0.948 with respect to the secret image. Moreover, in figure 4, we see that a wrong key is used to recover the image. Thus we obtain a noise image.

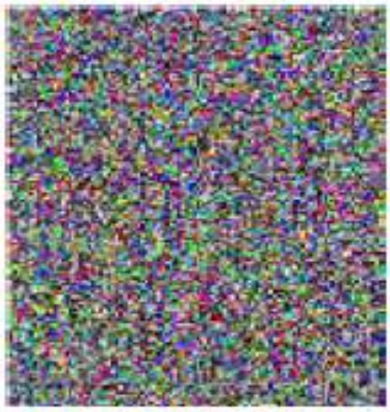


Fig. 4: Recovered secret image using a wrong key

An input-output model in tabular form is provided in the table below, for easy comparison of input, output and process.

INPUT	PROCESS	OUTPUT
SECRET IMAGE	USER INPUT	ACCEPT INPUT DATA
TARGET IMAGE	ARBITRARILY SELECTED	ACCEPT AS INPUT
SECRET IMAGE AND TARGET IMAGE	MAT2CELL	BLOCK OF TILE AND TARGET BLOCKS
TILE IMAGE AND TARGET BLOCK	TRANSFORMATION AND ROTATION	MOSAIC IMAGE
SECURE KEY	ENCRYPTION	MOSAIC IMAGE WITH RECOVERY INFORMATION
MOSAIC IMAGE	DECRYPTION	RECOVERY INFORMATION
RECOVERY INFORMATION	DECRYPTION	SECRET IMAGE

Table 1: Input-Output Process Table

We now compare the existing Steganography technique with the proposed system. Figure 5 shows the result of this comparison. As we can see, the Mosaic Image Steganography technique has less image distortions compared to the normal Steganography technique. Thus the accuracy of the proposed system is more than the existing system.

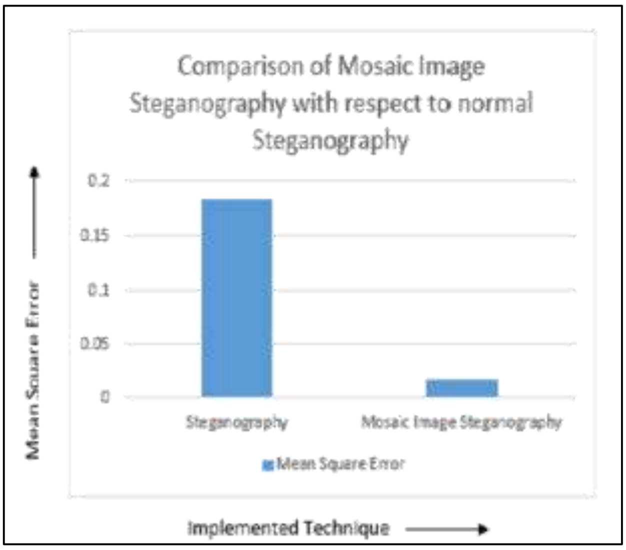


Fig. 5: Comparison of the Mosaic Image Steganography technique with respect to the existing Steganography technique.

V. SECURITY CONSIDERATIONS

In order to increase security, we encrypt the recovery information using an advanced form of AES algorithm together with chaotic key. The accuracy of chaotic maps makes the system for secure from many types of attacks. Only the receiver who knows the key can retrieve the recovery information. Once he extracts the recovery information, he can retrieve the secret image. On the other hand an attacker can try all the feasible permutations to get back the secret image. But, from the trial and error methods, the number of possible permutations was found to be n! , hence the probability for an eavesdropper to find the correct permutation is p=1/n!. This is a very small value. Hence breaking the system in this manner is practically impossible.

Next we have an attacker who guesses the permutation correctly. Without knowing the correct parameters, he/she cannot recover the secret image correctly. It can be still be considered that in extreme cases, he/she will observe the content of the mosaic image with a correct permutation, and try to recover the secret image. To increase the security of the proposed method against this type of attack, one possible way to is to use the key to randomize the important part of a secret image, such as the positions of the pixels in the secret image, before transforming the secret image into a mosaic image by the proposed method. Consequently, only authorized users with the key can know the correct secret image while an attacker cannot.

VI. CONCLUSION

The proposed system is found to remove the drawbacks of the existing systems discussed before. We select a secret image to be transmitted to the receiver. We then divide the image into small fragments and embedded into a pre-selected target image. No image databases are used in this technique for the selection of target images. The resultant image is known as mosaic image. The image recovery information is also embedded in the mosaic image after encrypting it using a key. The security is further enhanced by encrypting the recovery information using an advanced AES algorithm with chaotic key. The mosaic image is recovered using the recovery information. From the mosaic image the secret image is obtained by performing the reverse operations.

ACKNOWLEDGEMENT

We would like to thank all the reviewers for many useful comments and feedbacks that improve the paper presentation.

REFERENCES

[1] Chia-Chen Lin, Yi-Hui Chen and Chin-Chen Chang,“LSB-Based High-Capacity Data Embedding Scheme For Digital Images”, International Journal of Innovative Computing, Vol.5, November 2009.

[2] Ali Abdulgader, Mahamod Ismail, Nasharuddin Zainal and Tarik Idbeaa, “Enhancement Of AES Algorithm Based On Chaotic Maps And Shift Operation For Image Encryption”, Journal of Theoretical and Applied Information Technology, Vol.71 No.1, January 2015.

[3] William Stallings, “Overview in Cryptography and Network Security”, 5th edition, Pearson Education, Inc, 2006, ISBN 10: 0-13-609704-9

[4] Ya-Lin Lee and Wen-Hsiang Tsai, “A New Secure Image Transmission Technique via Secret-fragment-visible Mosaic Images by Nearly-reversible Color Transformations”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 24, No. 4, April 2014.

[5] Soumi C.G, Joona George and Janahanlal Stephen, "Genetic Algorithm based Mosaic Image Steganography for Enhanced Security", ACEEE Int. J. on Signal and Image Processing, Vol. 5, No.1, January 2014.

[6] I-Jen Lai and Wen-Hsiang Tsai,”Secret-Fragment-Visible Mosaic Image–ANew Computer Art andIts Application to Information Hiding”, IEEE Transactions on Information Forensics and Security, Vol. 6, No. 3, September 2011.

[7] N.S. Soleimani Zakeri and M.A. Balafar, “A Review on Data Hiding upon Digital Images”, International Journal on Technical and Physical Problems of Engineering.

[8] Chi-Kwong, Chsn and L.M Cheng, “Hiding Data in Images by Simple LSB Substitution “, Pattern Recognition, August 2013.

[9] Ritu Pahal and Vikaskumar, “Efficient Implementation of AES”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, July 2013.