Proposing Innovative method of Steganography with Gray Scale LSB Image with Encryption

Shalini Sharma[#1], Dr. Neeraj Bhargava[*2] & Dr. Amit Chaturvedi[*3]

*M.Tech (CS) Student, MDS Univ, Ajmer[#1], Prof., CS Dept, MDS Univ, Ajmer[*2]*
*& Engineering College, Ajmer[*3]*
*shalinisharma@gmail.com[#1], drneerajbhargava@yahoo.co.in[*2],amit0581@gmail.com[*3]*

Abstract: *Innovative Secret communication methodis always a requirement for the all, including organizations, government representatives, or army. Steganography and Cryptography are the two major techniques used for secret communication. There are numerous applications of these techniques are designed and used for secret communication. In this paper, we are proposing in innovative method of applying steganography to hide a secret text message under a gray scale LSB Image and to more secure the message AES encryption is applied on it. The gray scale image will be separated first from the eight bit planes and then LSB (Least Significant Bit) bit plane will obtained. The text message will then be hided under this LSB bit plane cover image. The AES encryption algorithm will be considered most complex and secure among other encryption algorithms if its category. So, AES encryption will also be used here for making the method more strong to breach the security of the communication message.*

Keywords: **LSB image, bit plane, encryption, Steganography, Steganalysis, secret message, key.**

1. INTRODUCTION

Steganography is not a new concept it is in practice from last more than hundred years. Using technology new applications of steganography are designed for providing various methods of secure communications over internet or shared medium of communication. Using steganography only sender and the intended recipient can get the secret message. In the steganography, the secret message will be hided under a cover. The cover may be a text, image, audio, or video file. The cover of the secret message is also a meaningful object and the selection of the cover is also a strategic issue. So, if any how the final object is get leaked or an unauthorized person get the final object, it should not have doubt that there is any secret message under this image cover.

There are different types of steganography in practice like Text Steganography, Audio Steganography, Image Steganography, etc. Image Steganography is a modern way of hiding information in a way that the unauthorized persons may not access or identify the secret message. Data to be hided under the image cover may be a text message or another image. Image Steganography may be very much useful or helpful to individual, organizations, or government in a number of ways such as hiding the secret data, data authentication, ensuring authenticated data availability for academic usage, monitoring of data privacy, labeling electronic data or contents, copyright protection, ownership identification, providing confidentiality and integrity enhancement control of electronic data privacy, etc. The important constructs of steganography are: (1) Cover file, (2) Stego Medium, (3) Secret Message, and (4) Steganalysis.

Steganography may be classified as pure, symmetric and asymmetric steganography. Pure Steganography does not need any key for exchange of data or information, while symmetric and asymmetric steganography needkeys to exchange of data or information prior to sending the message.Steganographic techniques are highly dependent on the type of media being used to hide the data or information. Image Steganography is the most preferred media because it is harmless and attractive. The need of such methods of exchanging secret messages over the shared communication channels is more increases during the last one year during covid-19, because people cannot move from one place to another. The important work cannot be suspended for a long period, so the need or importance of steganography increases more in such situations.

In this paper, we are proposing an innovative method of image steganography and the Image that will be used as cover here is a gray scale LSB image. We first apply the bit plane separation algorithm to separate the eight bit planes of the gray scale image, and then use the first bit plane i.e. Least Significant Bit plane of the gray scale image as cover to hide the secret message. After hiding the secret message under the LSB image cover i.e. the final stego image. This final stego is also a LSB image or Bit Plane 1 of the gray scale image. This LSB image then combined with the rest seven bit planes to form the recombined image. This recombined image will then be send to the receiver over the shared communication channel like internet.

2. Least Significant Bit (LSB) Insertion Steganography

Least Significant Bit (LSB) inclusion is a well- known technique used in Image based steganography. It is a way towards changing the least significant piece pixels of the transporter image. It is a straightforward method for inserting the message bits into the Least Significant pixels position of the image. In this technique some data from the pixels of the transporter image is supplanted with the message bits so that it cannot be seen by the human visual framework, in such a manner that it abuses a few confinements of the human visual framework.

The Least Significant Bit inclusion method differs as per the number of bits available in the picture. If there are 8-bits in every pixel of the picture, then the least noteworthy bit is the eighth bit of every byte of the picture, and using this technique that eighth bit will be changed by the 1-bit of mystery message. The LSB steganography includes the activity on least significant bits of spread picture, sound, or video. This technique used for implanting bits and varies as indicated by the quantity of bits in a picture.

3. Application of Encryption Algorithm in Steganography

Cryptography is a technique used to secure the message by converting the data from one form to another form of data. There are various cryptography techniques are proposed and in practice also for the converting the data for exchanging in communication. Some of the popular cryptography techniques are DES, RSA, AES, etc.

There are two types of encryption standards used for converting plaintext into cipher-text. One is the symmetric key encryption method and another is the asymmetric key encryption method. In the symmetric key encryption method, a symmetric key i.e. same key for encryption and decryption is used. Whereas in the asymmetric key method, two different keys called as private and public keys are used for encryption and decryption respectively. Private key is kept safe with user who does the encryption and public key is distributed to all the recipient of the cipher-text. When asymmetric key is used a lot of computational power have to be done. But if symmetric key is used comparatively less computational power is required and results proves that process with the application of symmetric key are around 1000 times faster than the processes with the applications of asymmetric key. And because they are faster, symmetric ciphers are much more useful for bulk encrypting large amounts of data.

AES is a symmetric key encryption standard i.e. it uses same key for encryption and decryption of the plaintext into cipher-text and vice-versa. It is an open standard that is free to use for any public, private, commercial, or non-commercial use. The AES encryption algorithm encrypts and decrypts data in blocks of 128 bits. It can do this using

128-bit, 192-bit, or 256-bit keys. AES using 128-bit keys is often referred to as AES-128, and so on. AES-128 key is very secure as it requires around one billion billion (one quintillion) years to break it with world's fastest supercomputers.

3. Proposed Model and Methodology

In this paper, we are proposing an innovative model for the implementation of steganography with LSB image and AES encryption. The basic requirements for this proposed model are: (1) Gray Scale PNG image, (2) Mystry or secret message, (3) Symmetric Key for encryption.

The steps for performing the steganography and steganalysisare listed below in the LSB_stego () algorithm &Reverse_stego() algorithm and are shown in the figure 2(a) and 2(b) as flow charts.In the LSB_stego() algorithm, there are three main functions: (1) Execution of Bit Plane separation function, (2) Encryption of secret or mystery message, and (3) Merging the Bit Planes after hiding the secret message.

LSB_stego() algorithm

Step 1: Select a Cover.png image
Step 2: Execute the BitPlane Separation Function to **c**reate eight bit planes of the selected image i.e. Cover.png.
Step 3: Select the Least Significant Bit (LSB) Plane and saves it as BitPlane1.png
Step 4: Select the Mystery message
Step 5: Apply the AES encryption on the message to secure it
Step 6: Hide the encrypted mystery message under this BitPlane1.png cover and save it as LSB_bitplane.png.
Step 7: Merge the LSB_bitPlane.png image with rest seven Bit Planes i.e. BitPlane2.png – BitPlane8.png and save the final stego image as Recombined.png
Step 8: Final Stego image i.e. Recombined.png is ready to share on the shared communication medium.

When the final stego image i.e. Recombined.png image is received by the intended recipient it will use Reverse_Stego() algorithm to recover the hidden message. The Reverse_Stego() algorithm is explained below:

Reverse_Stego() algorithm

Step 1: Select a Recombined.png image as final stego image.
Step 2: Create eight bit planes of the selected image as BitPlane1.png to BitPlane8.png.
Step 3: Select the Least Significant Bit (LSB) Planeand saves it as BitPlane1.png
Step 4: Apply message extraction function on the BitPlane1.png to obtain the encrypted Mystery message from the BitPlane1.png image

Step 5: Apply the Secret Key using AES decryption algorithm on the encrypted message to recover the original mystery message.

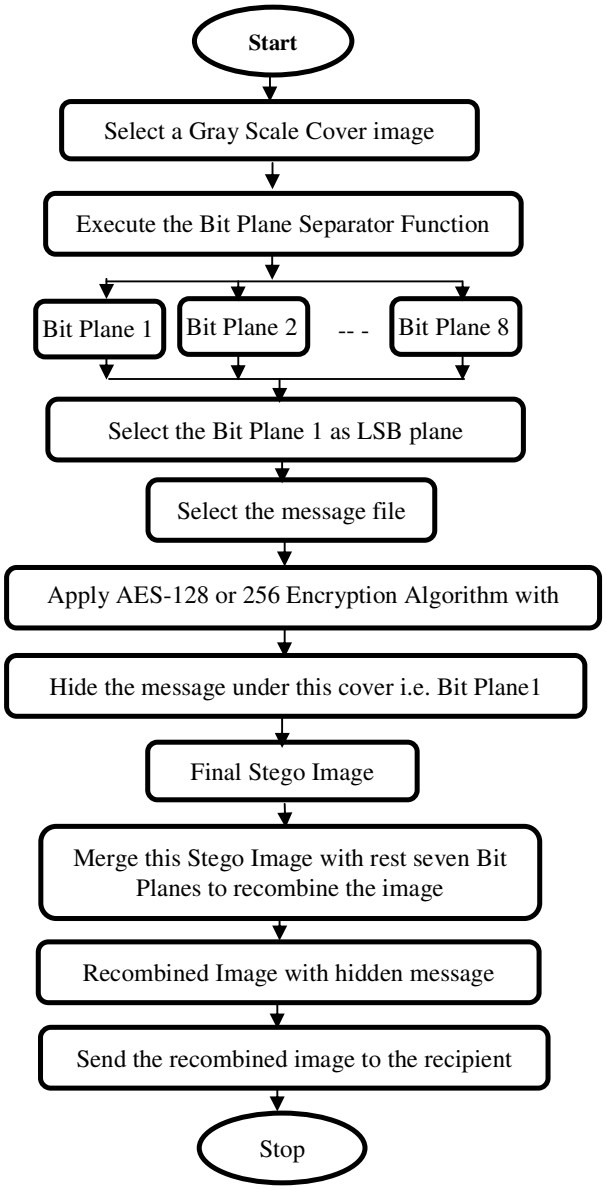

Figure 2(a): Flow chart ofLSB_stego() algorithm

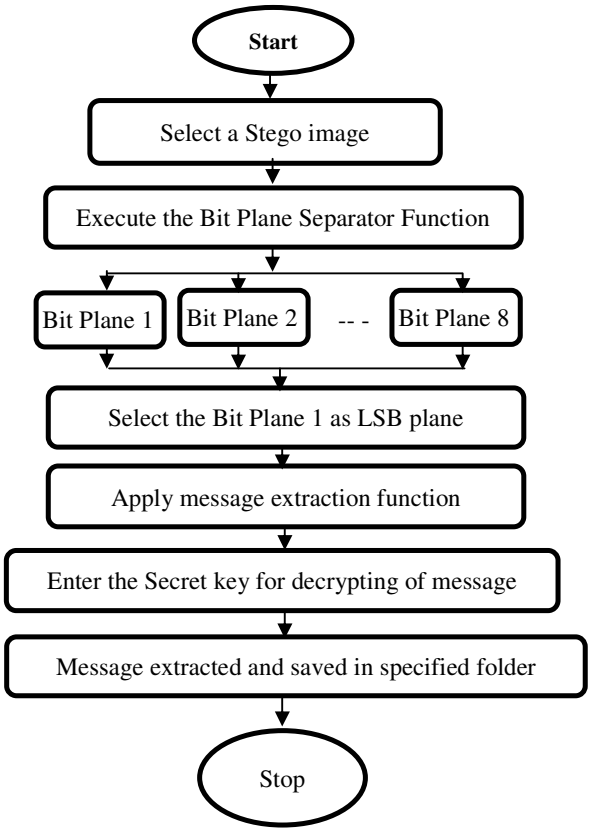

Figure 2(b): Flow chart of Reverse_stego( ) algorithm

4. Implementation of the Proposed Model

In this section, the implementation of the proposed model and methodology on the actual data is illustrated. Now first take a gray scale image original.png as shown in figure 3 and a mystery message message.docx file shown in figure 4.



Figure 3: original.png

Hi Narendra, it is an internal and confidential message these prices will be applied after one month. This Message is regarding IT security system of Tata steel and the price fluctuation in shares. According to analysis shares price will degrade with 7.2%. To get this degraded price use credentials as follows. Username: Stock@Hotmail.com Password: Stock#12&Tata&steel97

Private key: 1M61#@WEhgA74AQ0

public key: 8al#$12pWLa3E1Oo

Figure 4: message.docx

The bit plane separation program will be executed to separate all the eight bit planes of the original.png image as shown in figure 5 and the LSB image or first Bit plane will be saved as BitPlane1.png as shown in figure 6.

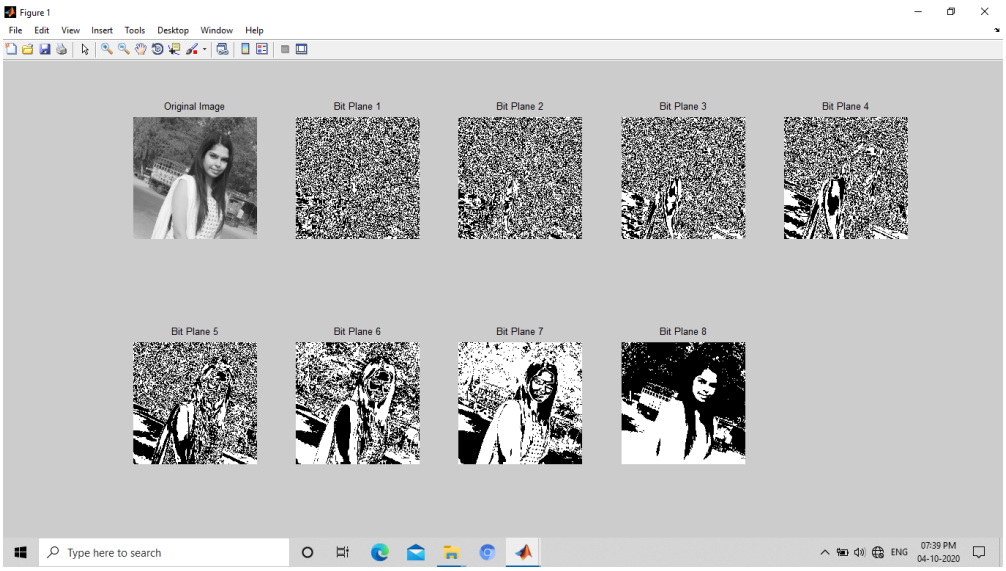

Figure 5: All the Eight bit planes of the original.png image

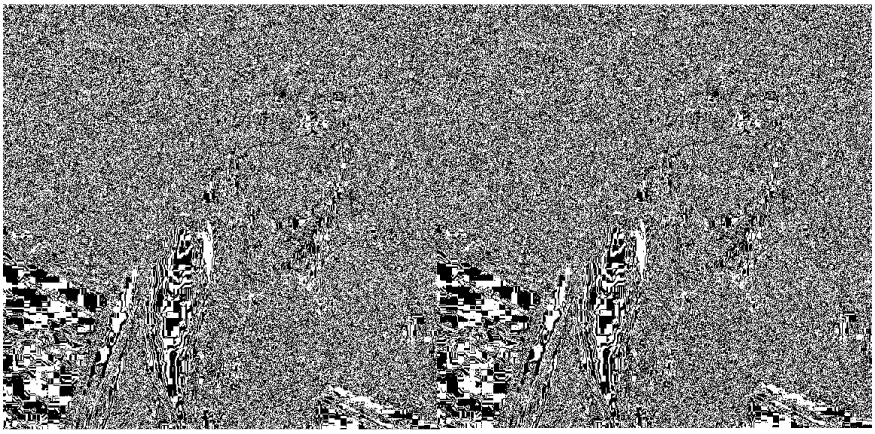

Figure 6: BitPlain1.png Figure 7: Output1.png

Use steganographic tool to hide the message file under the BitPlane1.png cover image and the output will be saved by the name output1.png as shown in the figure 7.

Now, merge this output1.png with rest seven bit planes, i.e. from BitPlane2 to BitPlane8, of the original.png image to recombine it and recombined image will then be saved as recombined.png. This recombined.png is the final stego image that will be shared with intended recipient on the shared communication channel. This process is illustrated in the figure 8 below:

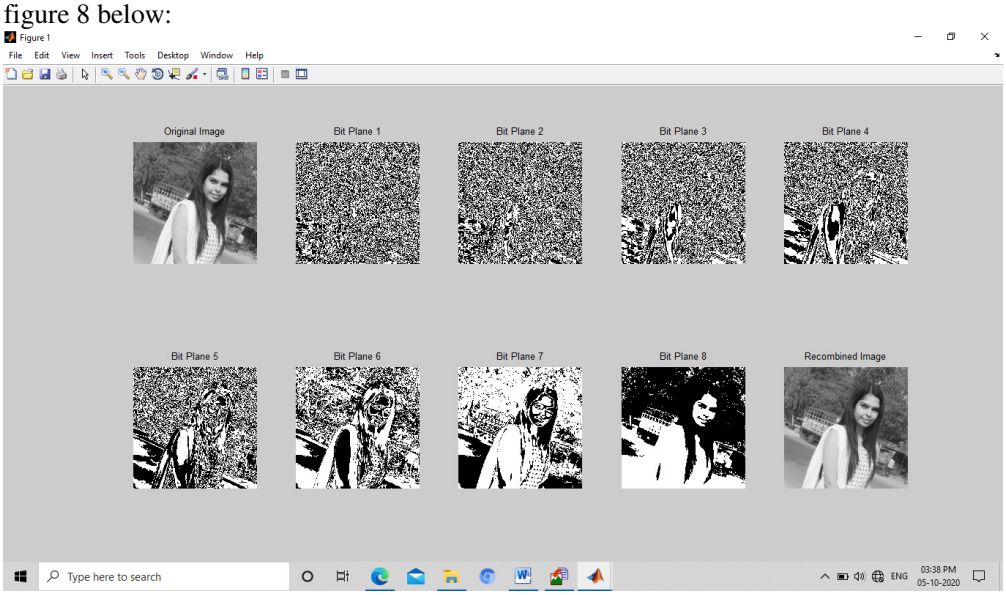

Figure 8: Generating final Stego image Recombined.png

For extracting the mystery message the receiver will apply the reverse process, i.e. it will apply the steganalysis. The receiver will separate the all eight bit planes of the recombined image using Bit Plane separation function on the recombined.png image. It will select the first bit plane i.e. Bit Plane1.png and then apply the steganography tool to extract the hidden message, i.e. message.docx file. The process of steganalysis has been displayed below in the figure 9.

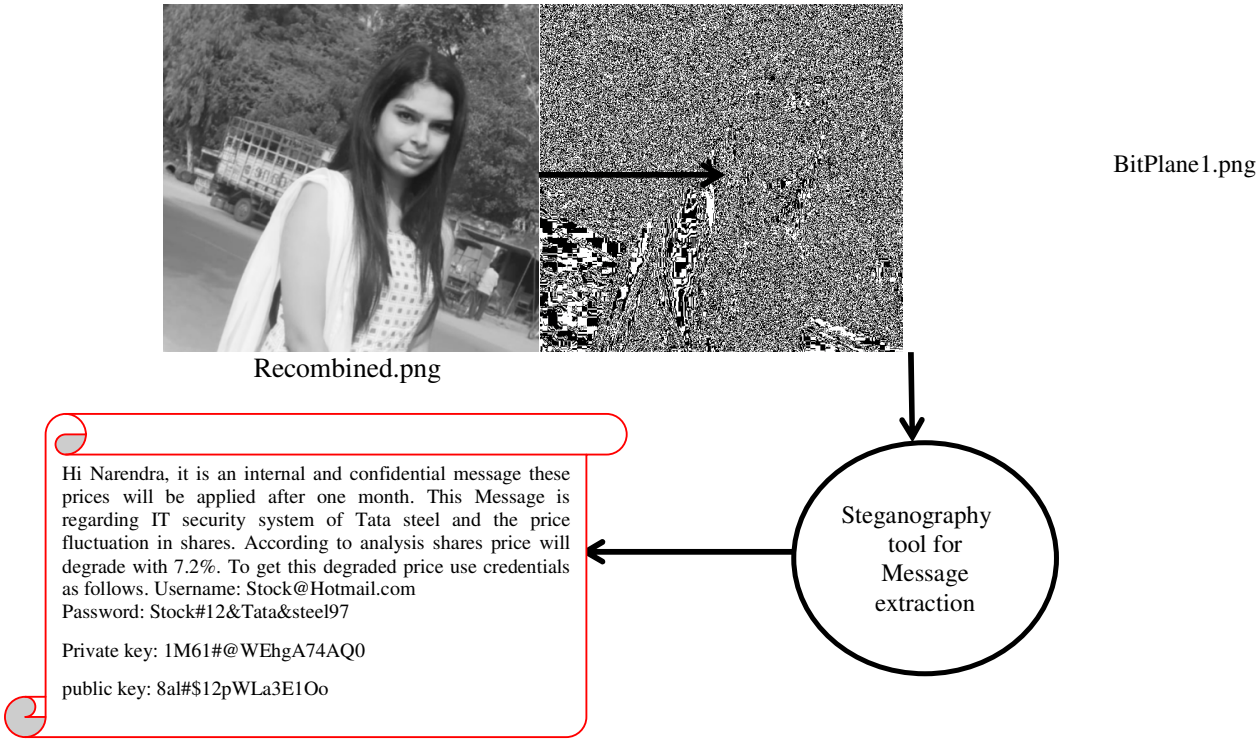

Figure 9: Process of Steganalysis for message extraction from Stego-image

5. Conclusion

Image Steganography is a very useful technique for secret message communication on the commonly shared communication channels like Internet. During the covid-19, requirements of such secret communication techniques are realized more. In this proposed innovative steganography technique, we have used the concept of LSB images cover for hiding the secret or mystery message and then merge this cover with the rest bit planes, so that the unauthorized person cannot detect or have any doubt of having secret message under it. To more secure the message the AES-128 encryption algorithm has been applied. The proposed model and the experimental setup have illustrated the concept well. Hence, it is a successful proposal to send the secret message using steganography with LSB cover over the shared communication channel and retrieving the secret message at the receiver's end.

Acknowledgments

Steganography is a method used to send secret message in such a manner that the unrelated person does not have any doubt that there is any hidden message. The steganography technique has enough opportunities of innovations in the technique and we have tried it in this proposal also. The authors are thankful to all the people who directly or indirectly involved in the development of this paper.

REFERENCES

[1] *Jawaheralqahtani, DaniyalAlghazzawi and Li Cheng, "STEGANALYSIS ALGORITHM FOR PNG IMAGES BASED ON FUZZY LOGIC TECHNIQUE", International Journal of Network Security & Its Applications (IJNSA) Vol.8, pp 1-15.*

[2] *Souvik Bhattacharyya, Indradip Banerjee and GautamSanyal, "A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier", Journal of Global Research in Computer Science, Volume 2, ISSN: 2229-371X. PP. 1-16.*

[3] *HosseinMalekinezhad, Ali AzimiKashani and Ali Farshidi, "Application of Histogram Examination for Image Steganography", Journal of Applied Environmental and Biological Sciences, ISSN: 2090-4274, pp. 97-104.*

[4] *Mrs.K.Rajasri, Mrs.D.Gayathri, and Ms.T.Indhumathi, "Image Steganography and Steganalysis Using Pixel Mapping Method", International Journal of Engineering Research & Technology (IJERT), Vol. 2, pp. 3274-3279, ISSN: 2278-0181.*

[5] *Arvind Kumar and Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications, pp. 19-23, ISSN: (0975 - 8887),*

[6] *Jingzhi Lin, ZhenxingQian, Zichi Wang, Xinpeng Zhang, and GuoruiFeng, "A New Steganography Method for Dynamic GIF Images Based on Palette Sort",*

[7] *Shamim Ahmed Laskar1 and Kattamanchi Hemachandran2, "A Review on Image Steganalysis techniques for attacking Steganography", International Journal of Engineering Research & Technology (IJERT), pp. 3400-3410, ISSN: 2278-0181.*

[8] *G.SuryakalaEswari ,N.Leelavathy and U.Sandhya Rani , "Fractal Image Steganography Using Non Linear Model", International Journal of Innovative Research in Computer and Communication Engineering, pp. 2644-2649, ISSN(Online): 2320-9801.*

[9] *ParmarAjit Kumar Maganbhai and Prof. Krishna Chouhan, "A Study and literature Review on Image Steganography", ParmarAjit Kumar Maganbhai et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1), pp. 685-688, ISSN: 0975-9646.*

[10] *ParisaGerami, Subariah Ibrahim and MortezaBashardoost, "Least Significant Bit Image Steganography using Particle Swarm Optimization and Optical Pixel Adjustment", International Journal of Computer Applications (0975 - 8887), Volume 55, pp. 20-25.*

[11] *Dr. Ashty M. Aaref, "Hiding Image in Image using Modified method in Least Significant Bit (LSB) substitution based Sobel Edge Detection", International Journal of Enhanced Research in Science, Technology & Engineering, Vol. 4, pp. 66-72, ISSN: 2319-7463.*

[12] *AnumJaveedZargar, "Digital Image Watermarking using LSB Technique", International Journal of Scientific & Engineering Research, Volume 5, pp. 202-205, ISSN 2229-5518.*

[13] *Marwa M. Emam, Abdelmgeid A. Aly, and Fatma A. Omara, "A Modified Image Steganography Method based on LSB Technique", International Journal of Computer Applications (0975 - 8887), Volume 125, pp. 12-17.*

[14] *Ms.ShrideviShetti and Mrs.Anuja S, "A Secure Image Steganography based on RSA Algorithm and Hash-LSB Technique", International Journal of Engineering Research & Technology (IJERT), Volume 3, pp. 1-7, ISSN: 2278-0181.*