Data Hiding using Advanced LSB with RSA Algorithm

Varsha
Department of Computer Science & Application
M.D. University, Rohtak, Haryana

Rajender Singh Chhillar, Ph.D
Professor, Department of Computer Science & Application, M.D. University
Rohtak, Haryana

ABSTRACT
In this paper, RSA algorithm is used to encrypt the secret message and advanced LSB technique is used to hide the encrypted message. Firstly, the message is encrypted and then encrypted message is being divided in two parts. First part of the encrypted message is xored with odd position and second part with even position of LSB+1. After that the xored encrypted message is being hidden on LSB position.

Keywords
Steganography, cryptography, RSA algorithm, Least Significant Bit

1. INTRODUCTION
Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence respectively[1]. Cryptography is the art and science of keeping messages secure. The word is derived from the Greek *kryptos*, meaning hidden. Steganography is art of transmitting data in such a way that the existence of message is unknown. The word steganography is combination of two Ancient Greek words steganos means "covered or concealed" and graphein means "writing". Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. Even though both methods provide security, a study is made to combine both cryptography and Steganography methods into one system for better confidentiality and security.

It is always a good practice to use Cryptography and Steganography together for adding multiple layers of security. By combining, the data encryption can be done by a software and then embed the cipher text in an audio or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel [2]. The figure below depicts the combination of cryptography and steganography:

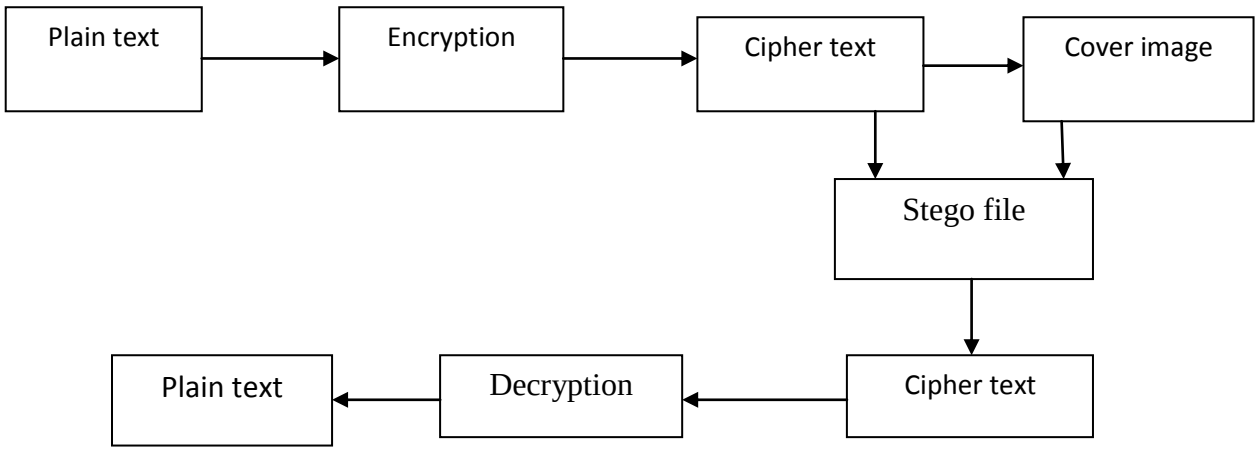

Fig 1.3: Combination of Cryptography and Steganography [3]

2. PROPOSED WORK
The aim of proposed scheme is to make a more secure and robust method of information exchange so that confidential and private data must be protected against attacks and illegal access. To order to achieve the required robustness and security cryptography and steganography is combined. Image is taken as a cover medium for steganography and RSA algorithm is used for encryption.

In this proposed method our advanced LSB bit manipulation method is used for embedding the message in the image file and the message is itself encrypted using the existing RSA encryption method. For embedding the text in image file firstly both the text and image file are converted into binary equivalent and then text is encrypted using RSA. The encrypted text is then embedded into the image file using our advanced LSB algorithm.

At the receiver side, stego image file must be selected to extract the message .After selecting the file and advanced lsb method is applied to extract the encrypted message and this message is decrypted using the RSA algorithm. A comparison is made between the original image file and the embedded one to indicate that less distortion even after changing the LSB bit of original file and for this PSNR, RMSE is calculated. PSNR and RMSE value indicates imperceptibility and transparency is evaluated by comparing the graph of image file before and after steganography. Also a histogram analysis has been done to show the imperceptibility.

2.1 Flow Chart

The proposed method is presented with the help of block diagram [4].

2.1.1 Embedding Text in Image
2.1.2. Extracting Text from Image

2.1.1. Embedding text in Image

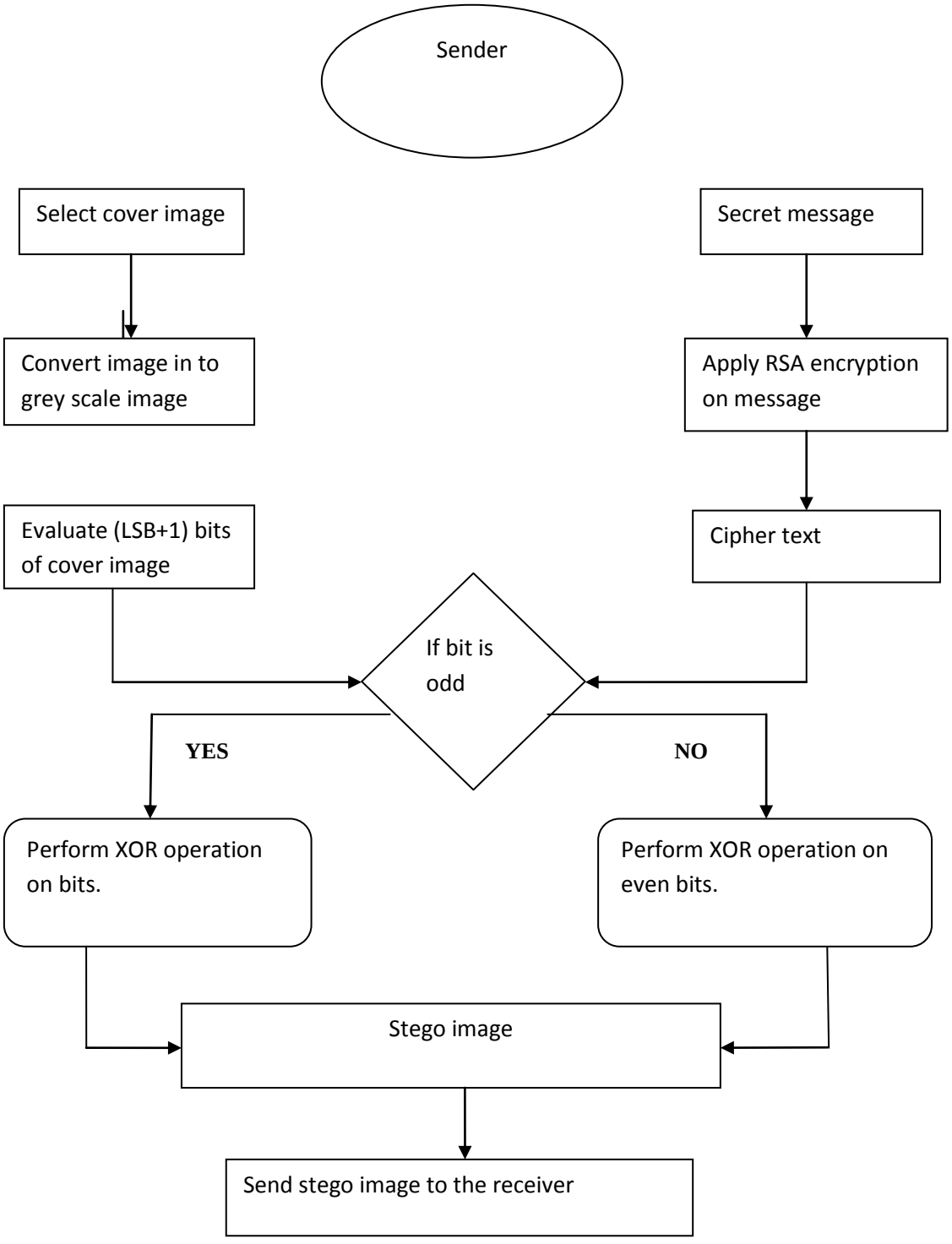

Fig 1: Flow Chart of Embedding Text

2.1.2. Extracting text from image

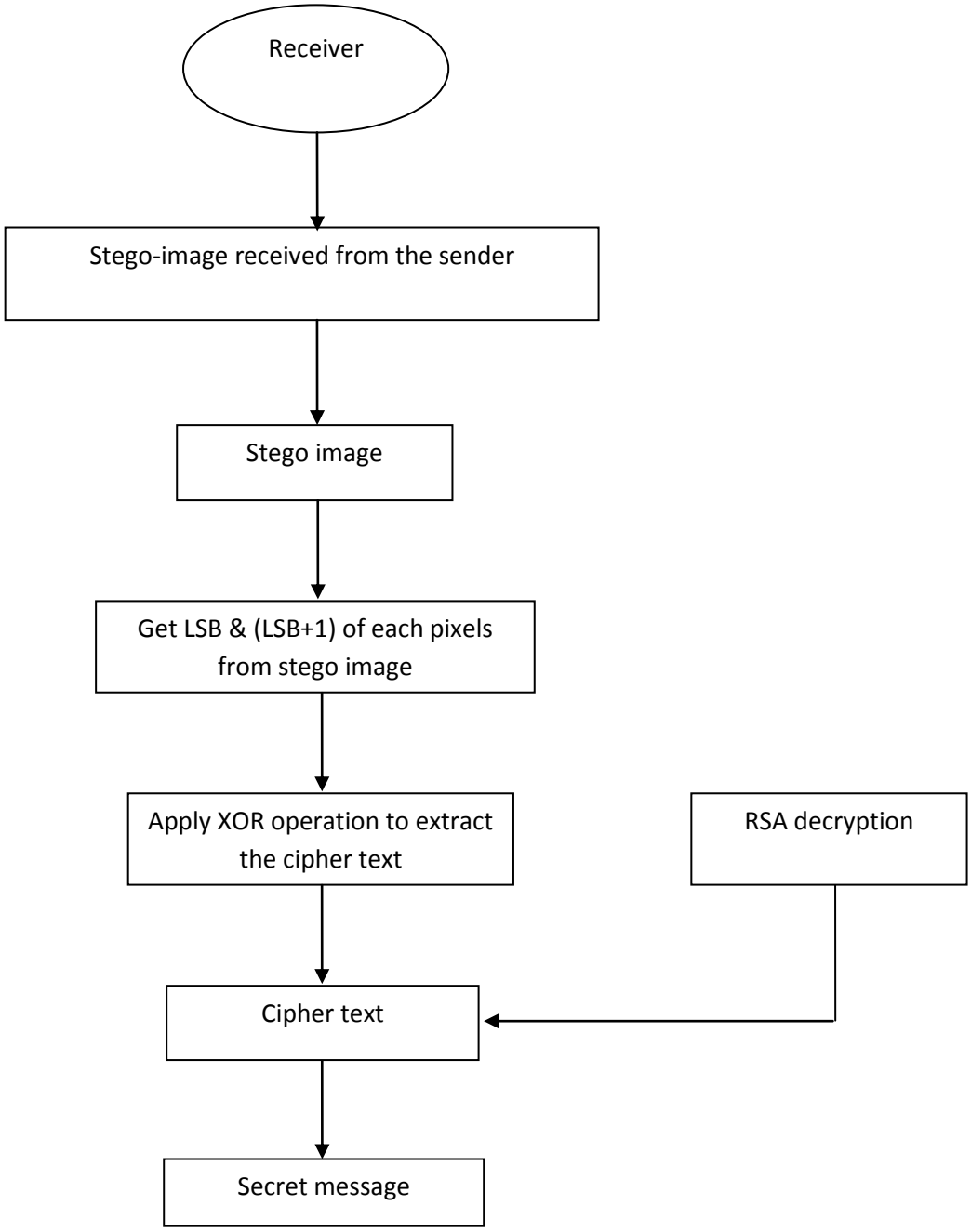

Fig 2: Flow Chart of Extracting Text

3. PROPOSED ALGORITHM

The proposed algorithm is based on our advanced LSB coding method and the RSA algorithm for encryption. In this an image file is taken for embedding the secret text. Both files are converted in binary equivalent. A XOR operation is applied on embedding process to make the method more secure. The text is encrypted using the RSA algorithm and this encrypted text is embedded into binary converted image file. Encrypted text is embedded into the file LSB bit of each block. The embedded image file is called as stego image.

3.1 RSA ALGORITHM

The algorithm was given by three MIT's Rivest, Shamir & Adelman. RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and then the product of these values is used to create a public and a private key, which is further used in encryption and decryption. The RSA algorithm could be used in combination with advanced LSB in a way that original text is embedded in the cover image in the form of cipher text. By using the RSA algorithm we are increasing the security to a level above. In case of steganalysis only cipher text could be extracted which is in the encrypted form and is not readable, therefore will be secure [4].

RSA algorithm procedure can be illustrated in brief as follows:

1. Choose two large prime no. p & q.
2. Calculate N=p*q

3. Calculate f(z)=(p-1)*(q-1)Find a random number e satisfying 1 < e < f (n) and relatively prime to f (n) i.e., gcd (e, f (z)) = 1.
4. Calculate a number d such that d = e-1 mod f (n).
5. Encryption: Enter message to get cipher text. Ciphertext c= mod ((message. ^e), N).
6. Decryption: The cipher text is decrypted by :

Message=mod ((c. ^d), N) [4]

3.2 Advanced LSB

Algorithm for embedding the message:

Step1. Input the Encrypted message using RSA Algorithm that to be hidden in the cover image.

Step 2. Select the cover image.

Step3. Take pixels from cover image.

Step4. Take the (LSB+1) bit from the pixel.

Step5. Divide the encrypted message in to two equal parts.

Step6. Perform XOR of first half of encrypted message with the odd position pixel values.

Step7. Perform XOR of second half of encrypted message with the even position pixel values.

Step8. Now get all the xored values of even and odd position pixel.

Step9. Now store the xored value of even in even position LSB bit of pixels. And xored value of odd in odd positioned pixel.

Algorithm for extracting the message:

Step 1: Receive a Stego Image.

Step 2: Get the LSB & (LSB+1) bit of pixels of embedded message.

Step3. Apply XOR operation on LSB & (LSB+1) bits.

Step4. Get the XOR value of all pixel values.

Step5. Now retrieve the bits from the XOR value alternately.

Step6: Apply RSA algorithm to decrypt the retrived data.

Step 7: Finally the secret message will be get.

4. RESULT

For the performance analysis of the ADVANCED-LSB technique to be implemented on two cover images.

In given fig 3 shows the cover image Leena with its stego image. The PSNR and MSE values have been shown between original Leena cover image and Leena stego image and their histogram also shown in figures.

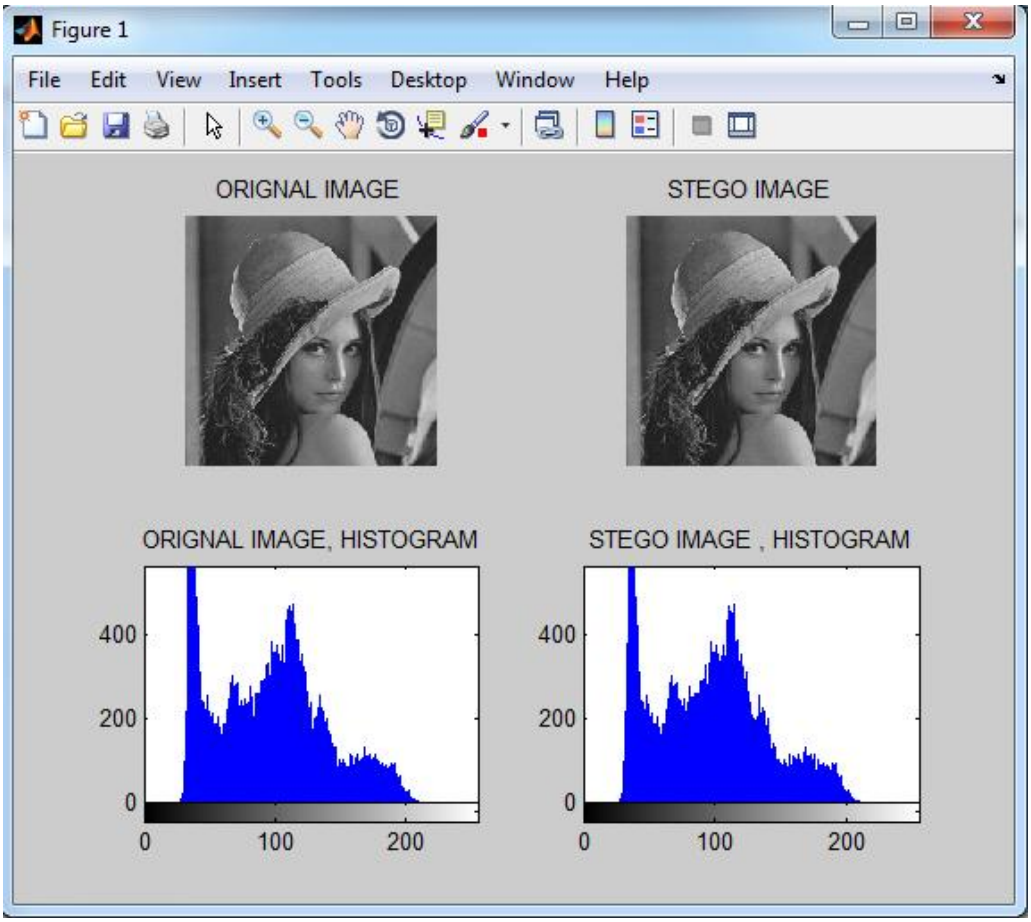

Fig (3): Original image and Stego image with their histogram

PSNR between Original and stego image = 6.6955

MSE between Original and stego image = 1.3917e+004

Fig.4 shows the cover image Baboon with its stego image. The PSNR and MSE values have been shown between original Baboon cover image and stego Baboon image and their histogram also shown in figures.

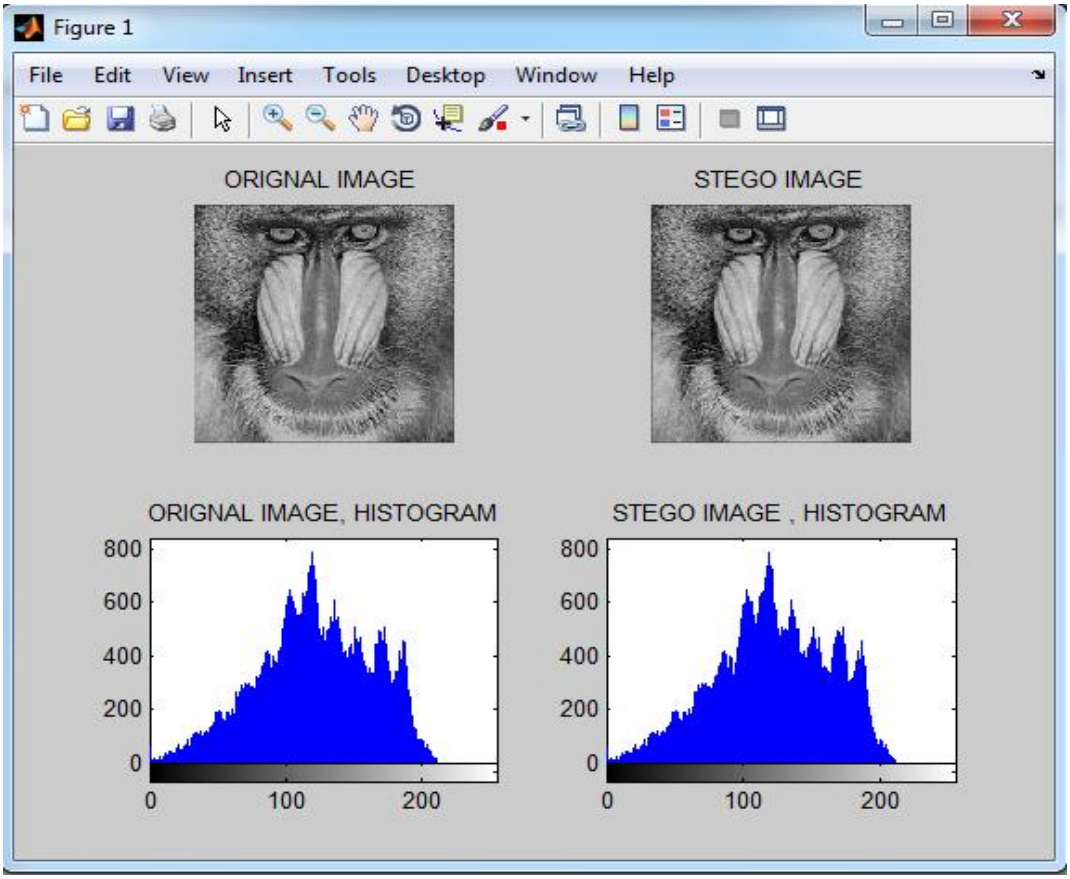

Fig (4): Original image and Stego image with their histogram

PSNR between Original and stego image = 5.1331

MSE between Original and stego image = 1.9942e+004

5. CONCLUSION

A secured ADVANCED based LSB technique for image steganography has been proposed and implemented. An efficient steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through ADVANCED-LSB method. In this work, a new way of hiding information in an image with less variation in image bits have been developed, which makes our technique secure and more efficient than LSB. This technique also applies a cryptographic method i.e. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. RSA algorithm itself is very secure that's why we used in this technique to increase the security of the secret message. A specified embedding technique uses XOR operation and also provide encryption of data uses RSA algorithm; makes our technique a very much usable and trustworthy to send information over any unsecure channel or internet.

6. REFERENCES

[1] Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1 , pp. 127-134 .

[2] Raphael, A. J., and Sundaram, V. 2011. Cryptography and Steganography - A Survey. *International Journal of Computer Technology Application*, 2(3), ISSN: 2229-6093, pp. 626-630.

[3] Adewole Kayode S. and Oladipupo Ayotunde J. *"Efficient Data Hiding System using Cryptography and Steganography*", International Journal of Applied Information Systems (IJAIS), Volume 4– No.11, December 2012, pp. 6-11

[4] Anil kumar, Rohini Sharma "*A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique"* International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013