A NEW METHOD FOR IMAGE STEGANOGRAPHY USING RSA ALGORITHM

Rajkumar Yadav

Assistant Professor
U.I.E.T, M.D. University, Rohtak-India
rajyadav76@rediffmail.com

***Abstract*— 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 advanced LSB bit manipulation method is used for embedding the message in the image file and the message is itself encrypted using the 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 the advanced LSB algorithm. At the receiver side, embedded 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.**

***Keywords*— Image Steganography, Cryptography, PSNR, MSE.**

I. Introduction

With the growth of computer network, security of data has become a major concern and thus data hiding technique has attracted people around the globe. Steganography techniques are used to address digital copyrights management, protect information, and conceal secrets. [1]

Cryptography is the art and science of achieving security by encoding messages to make them non readable. In this, the structure of message is scrambled to make it meaningless and unintelligible unless the decryption key is available. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of something or someone. Cryptanalysis is the reverse engineering of cryptography.

There are several ways of classifying cryptographic algorithms. The three types of algorithms are:(1) Secret key Cryptography: Uses a single key for both encryption and decryption(2) Public Key Cryptography: Uses one key for encryption and another for decryption.(3) Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information. [2]Cryptography, thus not only protects data from theft or alteration, but can also be used for user authentication. [3]

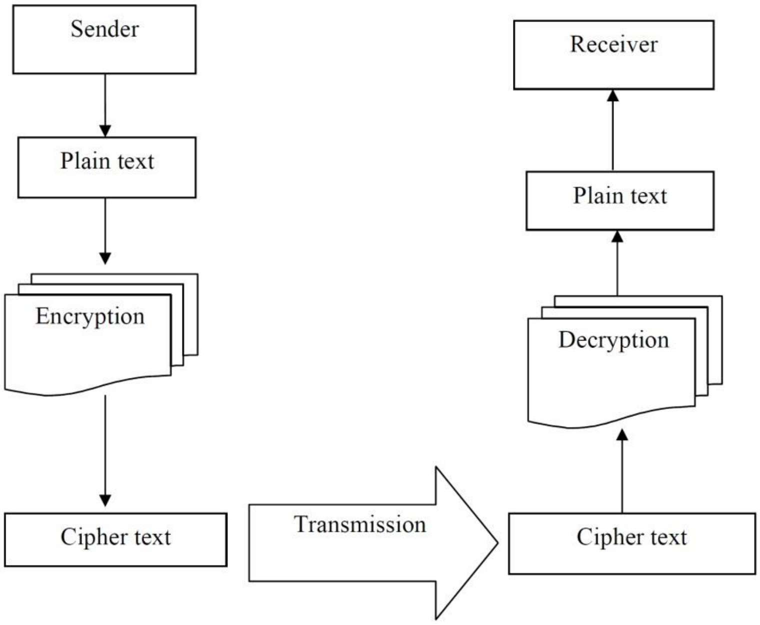


Fig.1. Elements of cryptographic operation [4]

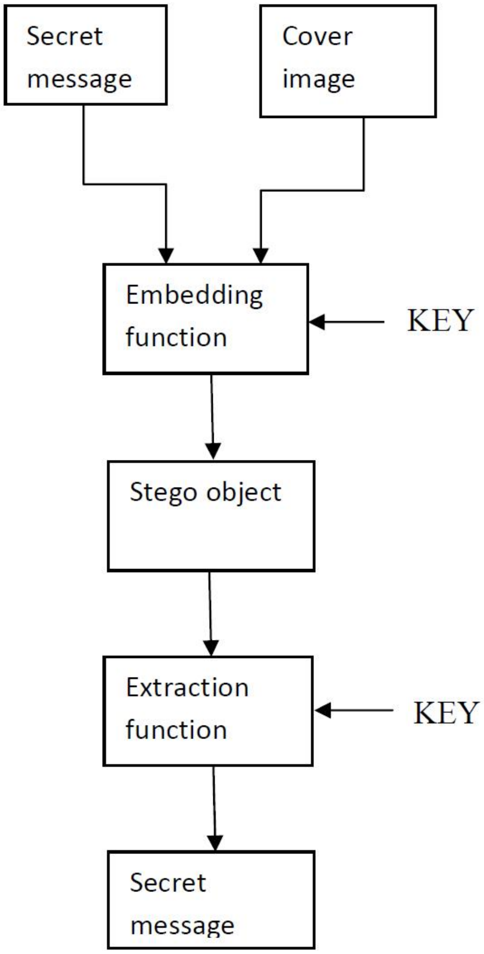


Fig.2. A model of the steganography system. [5]

However, 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. The figure below depicts the combination of cryptography and steganography.

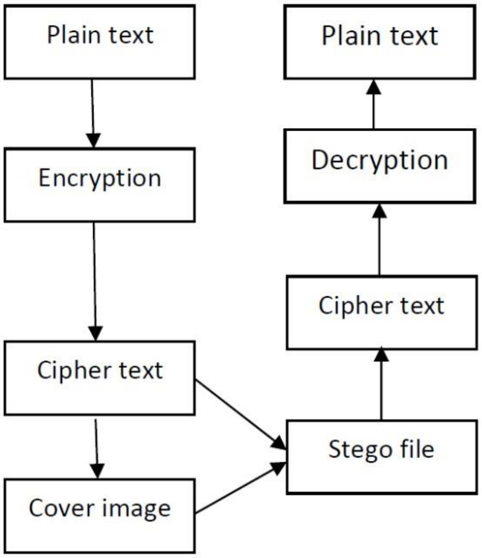


Fig.3 combination of cryptography and steganography[6]

II. PROPOSED ALGORITHM

The proposed algorithm is based on 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.

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.

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) [5]

Algorithm for embedding the message:

1. Input the Encrypted message using RSA Algorithm that to be hidden in the cover image.
2. Select the cover image.
3. Take pixels from cover image.
4. Take the (lsb+1) bit from the pixel.
5. Divide the encrypted message in to two equal parts.
6. Perform xor of first half of encrypted message with the odd position pixel values.
7. Perform xor of second half of encrypted message with the even position pixel values.
8. Now get all the xored values of even and odd position pixel.
9. Now store the xored value of even in even position LSB bit of pixels. And xored value of odd in odd positioned pixel.

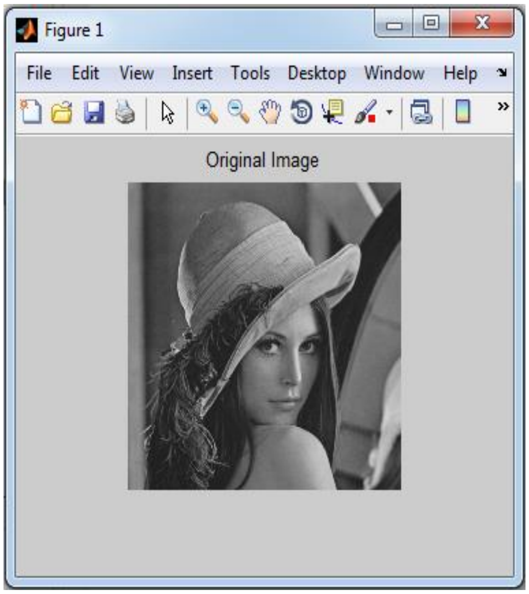
Algorithm for extracting the message:

1. Receive a stego image.
2. Get the lsb & (lsb+1) bit of pixels of embedded message.
3. Apply xor operation on lsb& (lsb+1) bits.
4. Get the xor value of all pixel values.
5. Now retrieve the bits from the xor value alternately.
6. Apply RSA algorithm to decrypt the retrived data.
7. Finally read the secret message.

PERFORMANCE ANALYSIS

For the performance analysis of the ADVANCED-LSB technique to be implemented on three covers images.

In given fig.4 shows the cover image Lenna with its stego image. The PSNR and MSE values have been shown between original Lenna cover image and stego Lenna image.



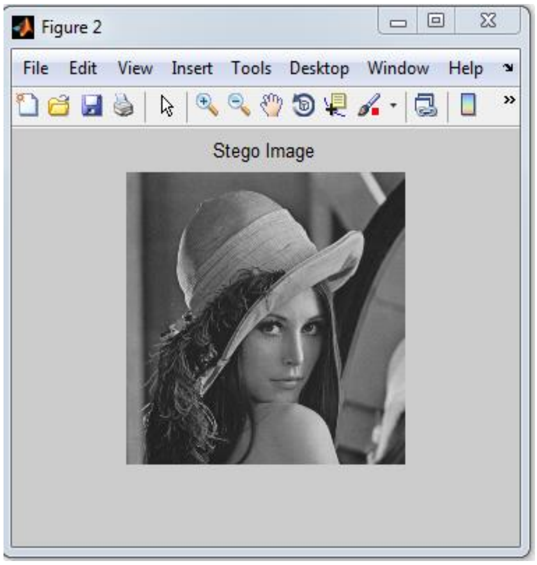
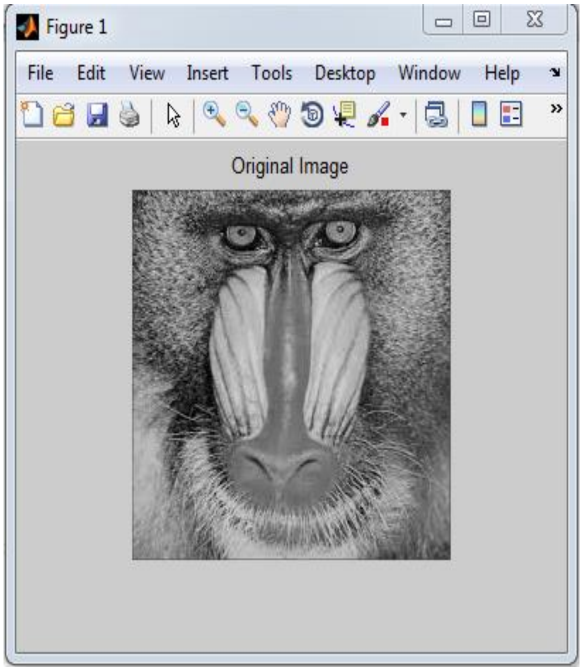


Fig. 4.

PSNR between Image (1) and Image (2) = +43.01

MSE between Image (1) and Image (2) = 0.0071

Fig. shows the cover image Baboon with its stego image. The PSNR and MSE values have been shown between original Babbon cover image and stego Baboon image.



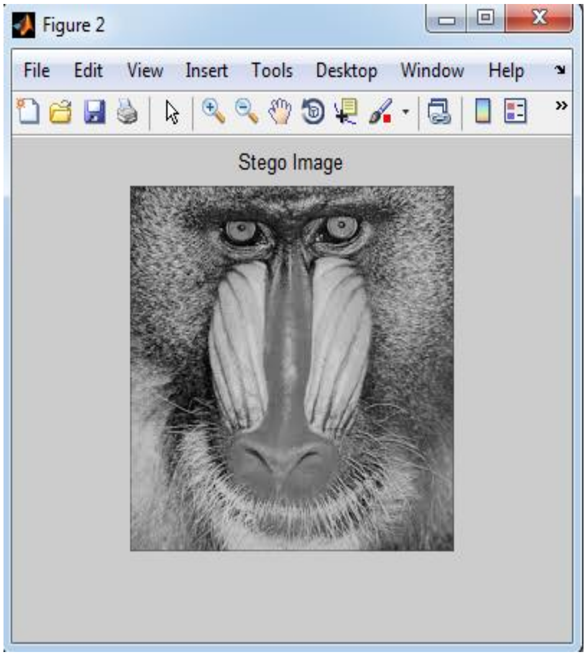
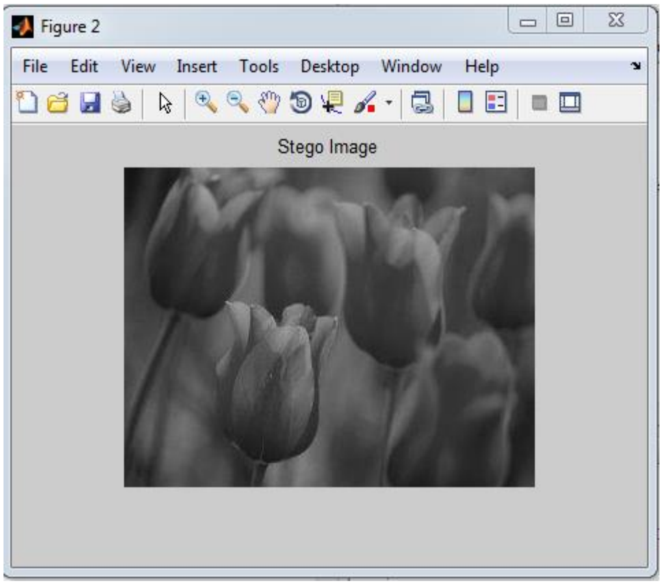


Fig. 5.

PSNR between Image (1) and Image (2) = +47.04

MSE between Image (1) and Image (2) = 0.0044

Fig. shows the cover image Tulip with its stego image. The PSNR and MSE values have been shown between original Tulip cover image and stego Tulip image.



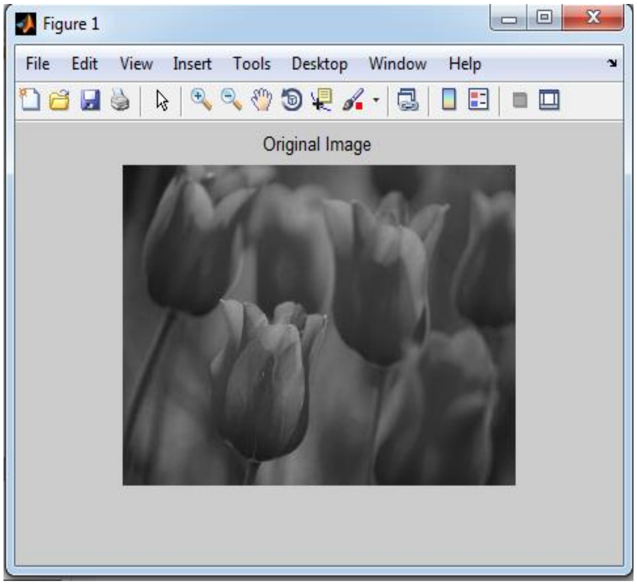


Fig. 6.

PSNR between Image (1) and Image (2) = +45.28

MSE between Image (1) and Image (2) = 0.0054

The mean square error (MSE) and the peak signal to noise ratio (PSNR) for different stego images are shown in the Table I. By comparing the PSNR values of all the stego images, it has been analyzed that only

Lenna as a cover image have given the best PSNR value. The same is true in the case for the MSE values while comparing with different stego images, [5]

TABLE I

RESULTS OBTAINED FROM A-LSB WITH RSA TECHNIQUES

Name of the image file	Results obtained using LSB with RSA		Results obtained using A-LSB with RSA	
Image name	PSNR	MSE	PSNR (db)	MSE
Leena	51.0768	0.5097	+43.01	0.0071
Tulip	51.3453	0.4770	+45.28	0.0054
Baboon	51.1490	0.4991	+47.04	0.0044

III. 3. CONCLUSION & FUTURE SCOPE

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.Performance analysis of the developed technique have been evaluated by comparing it with simple LSB technique, which have resulted a very good MSE and PSNR values for the stego images. The future scope for the proposed method might be the development of an enhanced steganography that can have the authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. The Steganography Technique is implemented on jpeg images to increase the performance. The further work may contain combination of this method to message digesting algorithms.

REFERENCES

[1] K.Hemachandran, “*Study of Image steganography using LSB, DFT and DWT*”, International Journal of Computers & Technology, vol 11, oct.25 2013, pp. 2618-2627.

[2] Zin.w, soe. N “i*mplementation and analysis of three steganographic approaches*”, university of computer studies, Mandalay, 2011, pp. 456-460.

[3] Manoj.S, “*cryptography and steganography*”, international journal of computer applications (0975-8887), 2010, vo1-no.12, pp. 63-68.

[4] 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.

[5] 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.

[6] Adewole Kayode S, 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.

[7] Masoud Nosrati , Ronak Karimi “*An introduction to steganography methods*” World Applied Programming, journal, Vol (1)-No (3), August 2011. 191-195.

[8] Application of steganography. Internet source http://www.datahide.com/BPCSe/applications-e.html

[9] Kumar A, Dr Jhakkar S, Makkar S, “*Comparative Analysis between DES and RSA algorithms*”. International Journal of Advanced Research in Computer Science and Software Engineering 2012.

[10] Kumar A, Kumari P. "*Steganography- A Data Hiding Technique*", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, 2010.

[11] Vigyan Sharma, Prof. Hitesh Gupta "*New Approach of Information Security through Steganography by using Wavelet Transformation and Symmetric*" International Journal of Modern Engineering & Management Research Volume 1, Issue 4, December 2013, pp. 73-82.

[12] Mamta Juneja, "*Improved LSB based Steganography Techniques for Color Images in Spatial Domain*", International Journal of Network Security, Vol.16, No.4, July 2014, pp. 302-307.

[13] Shailender Gupta and Ankur Goyal "*Information Hiding Using Least Significant Bit Steganography and Cryptography*" I.J.Modern Education and Computer Science, 2012, pp. 27-34.

[14] Nivedhitha1, Dr.T.Meyyappan "*image security using steganography and cryptography techniques*" Internaitonal Journal of Engineering Trends and Technology Volume 3-Issue 3- 2012, pp.366-371.

[15] Sujay Narayana, Gaurav Prasad "*Two new approaches for secured image steganography using cryptographic techniques and conversions*", An International Journal(SIPIJ) Vol.1- No.2, December, 2010.

[16] A. Joseph Raphael, Dr. V. Sundaram, " *Cryptography and Steganography – A Survey*". Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630.

[17] Mehdi Hussain ,Mureed Hussain, "*A Survey of Image Steganography Techniques*", International Journal of Advanced Science and Technology Vol. 54, May, 2013.

[18] *Matlab Tutorial and Matlab Notes.*

[19] Cooper J. A MATLAB Companion for Multivariable Calculus. Academic Press, 2001.

[20] Matlab Internet source http://en.wikipedia.org/wiki/MATLAB

[21] http://www.mathworks.in/products/matlab/description1.html

[22] http://wiki.answers.com/Q/What_are_the_applications_or_uses_of_matlab