Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A New Approach to Data hiding using Replacement of LSB and MSB

Basant Sah
Research Scholar(BIT Mesra,Ranchi)
India

Vijay Kumar Jha
Associate Prof(BIT Mesra Ranchi)
India

Abstract—In This paper we propose to hide the information inside the image. As we know that information is one of the important in our life. To protect the information from unauthorised accessing from intruder, we find the approach to hide the information inside the image, in this paper we just propose to replacement LSB and MSB bit of image with the information although it degrade the quality of image, but later we find the best approach to hide the information.

Keywords— Staganography, RSA,MSB, LSB,Cryptography.

I. INTRODUCTION

Information security play the very important role in every field like E-business, mobile banking and military etc. Protecting the private information from being attacked is regarded as one of the major problems in the field of information security. Apart from encryption, steganography has been one of the solutions to protecting data transmission over the network [1].Steganography is the science of cover writing that conceal the existence of secret information embedded in cover media over an insecure network. In this paper basically we focus that provide more security using replacement of LSB and MSB using steganagraphy and also encrypt the data then send using secure medium.

II. RELATED WORK

Over the past few years, a number of attempts have been made to study steganography.

A. LEAST SIGNIFICANT BIT (LSB) METHOD

This approach [3-8] is very simple. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. First of all read the image and convert it into the pixel intensity and least bit is replace with data but this method is useful when very less no of data is to be hide. Human eye can't detect because image quality very slightly decrease so this very useful.

10000010, 01111001, 10001100, 01010101 IMAGE

00110010 DATA

STAGO IMAGE

10000010, 01111000, 10001101, 01010101…… SO ON

B. TRANSFORM DOMAIN TECHNIQUES

This approach [9-10] embeds secret information in the frequency domain of the signal. Transform domain methods hide messages in significant areas of the cover image which make them more robust to attacks such as: compression, cropping, and some image processing, compared to LSB approach.

C. STATISTICAL METHODS

This approach [11] encodes information by changing several statistical properties of a cover and uses a hypothesis testing in the extraction process. The above process is achieved by modifying the cover in such a way that some statistical characteristics change significantly i.e. if "1" is transmitted then cover is changed otherwise it is left as such.

D. DISTORTION TECHNIQUES

In this technique [12-13] the knowledge of original cover in the decoding process is essential at the receiver side. Receiver measures the differences with the original cover in order to reconstruct the sequence of modification applied by sender. This paper tries to overcome the disadvantage of the LSB method [6-10] by appending encrypted data in image in place of plain textual data. To encrypt the data RSA [4] algorithms were used. To check the efficacy of the proposal, we calculated the number of instructions executed at sender and receiver site since the number of instructions executed is a measure of time complexity of the process.

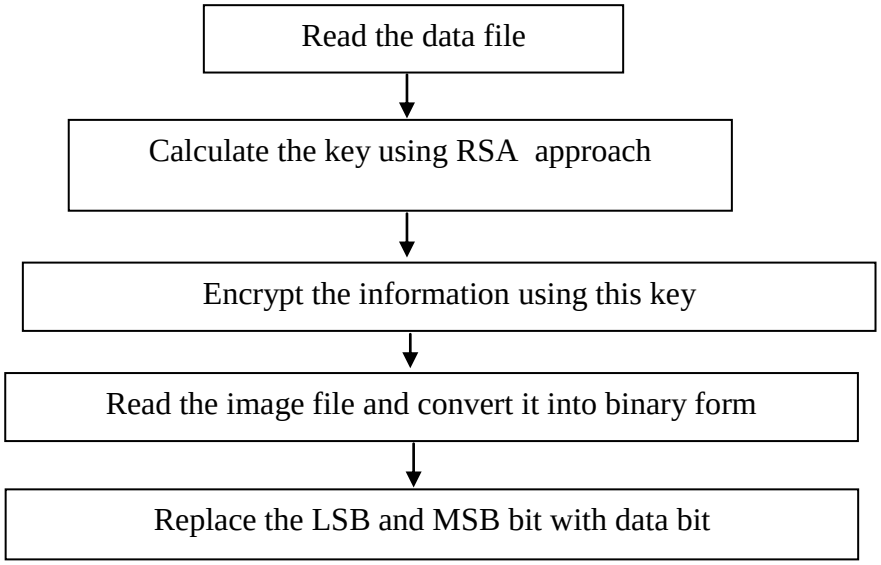
III. PROPOSE METHOD

In this paper we proposed that first of all find the public key and private key according to RSA approach and encrypt secret information. To provide higher security the secret information is encrypted first and encrypted ASCII value is converted in binary form .encrypt the data and then after replace the LSB bit and MSB bit with data. The proposed scheme uses RSA to encrypt secret information. To provide higher security the secret information is encrypted first and encrypted ASCII value is converted in binary form. The image pixels at the same time are also converted into binary form. The image is now used as a cover to embed the encrypted information. This process is done by LSB encoder which replaces the least significant bit of pixel values with the encrypted information bits.

A Sender Side

Algorithm

1 First of all read the text file i.e. information.
2 Find out the public and private key using RSA approach.
3 Encrypt the data i.e. information
4. Read the image file.
5. Replace every LSB and MSB (check MSB bit and data bit same then Replace MSB bit with data bit otherwise only LSB bit Replace.
6. Transfer the data via secure channel.



B. Receiver Side

Upon reception of Stego image the receiver firstly converts the pixels into their corresponding binary values. The LSB decoder then detaches the encrypted data from image pixel values. The encrypted data is decrypted using key value generated by RSA approach receiver side. This is how; the plain text is recovered from image.

IV. SIMULATION AND RESULTS

We simulate the process MATLAB-7.01. Since the number of instructions executed is a measure of time complexity of the algorithm therefore we calculated the number of instructions executed both at sender and receiver side to compare the performance of pure steganography and our proposed scheme.

Image Pixels (NXN)	N = 64, 128, 192, 256
Number of bits changed	K = 1, 2, 3 and 4
Image Type	bmp
Encryption	32 bit
Encryption Algorithm	RSA,
Simulation Tool	MATLAB 7.01

V. EXPERIMENT RESULT

We carry out experiments by taking most widely used images and some other images for evaluating their performances and compared them with some existing techniques [13]. The image quality metrics used are Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Root Mean Square Error (RMSE). High PSNR value and low MSE value signifies good quality image. PSNR is measured in decibel (db). The images taken in our experiments include Chrysanthemum, Koala, Lighthouse, Penguins, and Tulips each of different dimensions. The secret data taken in our experiments is Abraham Lincoln's letter to his son's teacher that is embedded into each of these images which is of size 1785 bytes. The resultant stego images with hidden secret message, employing our proposed method are shown in Figures below. The performance results are shown in Table 1.1, 1.2, and 1.3. Table 1.1: PSNR values of Different Approaches on different Images.

Table 1.1

Cover Image	Data hiding with LSB Algorithm	Proposed Algorithm
Chrysanthemum.jpg	67.1833	68.9992
Koala.jpg	67.3960	68.1254
Lighthouse.jpg	69.6649	70.7051
Penguins.jpg	71.8620	72.5735
Tulips.jpg	70.8246	71.6841

Table 1.2
MSE values of Different Approaches on different Images.

Cover Image	Data hiding with LSB Algorithm	Proposed Algorithm
Chrysanthemum.jpg	0.0124	0.0062
Koala.jpg	0.0118	0.0061
Lighthouse.jpg	0.0070	0.0031
Penguins.jpg	0.0042	0.0021
Tulips.jpg	0.0054	0.0024

Table 1.3
RMSE values of Different Approaches on different Images.

Cover Image	Data hiding with LSB Algorithm	Proposed Algorithm
Chrysanthemum.jpg	0.1115	0.0706
Koala.jpg	0.1088	0.0694
Lighthouse.jpg	0.0838	0.0391
Penguins.jpg	0.0651	0.0126
Tulips.jpg	0.0733	0.0428

(a) Chrysanthemum (b) Chrysanthemum

Fig 3 Chrysanthemum (a) Cover image and (b) Stego image

(a) Koala (b) Koala

Fig 4 Koala (a) Cover image and (b) Stego image

(a) Lighthouse (b) Lighthouse

Fig 5 Lighthouse (a) Cover image and (b) Stego image

(a) Penguins (b) Penguins

Fig 6 Penguins (a) Cover image and (b) Stego image

VI. CONCLUSIONS

The LSB modification technique provides an easy way to embed information in images, but the data can be easily decoded. It hide only small data set but in this paper we proposed to hide the information using replacement of LSB and MSB bit so that size just will be double hidden with stega-image.The proposed scheme used in this paper encrypts the secret information before embedding it in the image. Certainly the time complexity of the overall process increases but at the same time the security achieved at this cost is well worth it. This cryptographic scheme can be used for other steganographic techniques also.

REFERENCES

[1] Neil F. Johnson and Sushil Jajodia, "Steganalysis of Image Created Using Current Steganography Software", Workshop of Information Hiding Proceedings, Portland Oregon, USA,15-17 April,1998. Lecture Notes in Computer Science, Vol.1525, Springer-Verlag (1998).

[2] Clair,Bryan,"Steganography:How to Send a Secret Message", 8 Nov. 2001 www.strangehorizons.com 2001/20011008/steganography.shtml

[3] Bender, W., D. Gruhl, and N. Morimoto, "Techniques for data hiding", IBM Systems Journal , vol. 35, no. 3/4, 1996, pp. 131-336.

[4] Moller. S.A., Pitzmann, and I. Stirand, "Computer Based Steganography: How It Works and Why Therefore Any Restrictions on Cryptography Are Nonsense, At Best", in Information Hiding: First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, 1996, pp.7-21.

[5] Gruhl, D., A. Lu, and W. Bender, "Echo Hiding in Information Hiding", First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer,1996, pp. 295-316.

[6] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf [2] N. Tiwari and M. Shandilya, "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth", International Journal of Security and Its Applications Vol. 4(4), Oct. 2010.

[7] H. B. Kekre, A. Athawale, P. N. Halarnkar, "Performance Evaluation of Pixel Value Differencing and Kekre's Modified Algorithm for Information Hiding in Images", International Conference on Advances in Computing, Communication and Control, 2009 pp 342-346

[8] Deshpande Neeta, Kamalapur Snehal, "Implementation of LSB Steganography and Its Evaluation for Various Bits" K.K.Wagh Institute of Engineering Education & Research, Nashik India

[9] Morkel, T., Eloff, J.H.P & Olivier, M.S., "An overview of Image Steganography", Proceedings of the Information Security South Africa (ISSA) Conference, 2005.

[10] H. Yang, X. Sun, G. Sun. "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution". Journal: Radio engineering Year: vol. 18, 4 Pages/record No.: 509-516, 2009.

[11] H.C. Wu, N.I Wu, C.S. Tsai and M.S. Hwang, "Image Steganographic scheme based on pixel-value differencing and LSB replacement methods", VISP(152), No. 5, October 2005

[12] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Member, IEEE, and Hung-Min Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. pp. 488-497. 3rd September 2008. [9] H. B. Kekre, Archana Athawale, Pallavi N.

[13] Basant Sah,Ankush garg "Enhancing the Data Hiding Capacity of Kekre Algorithm Using the Lempel–Ziv–Welch Technique " Volume 3, Issue 7, July 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering .

