IOSR Journal of Engineering
Mar. 2012, Vol. 2(3) pp: 473-477

Effect of Noise on image steganography based on LSB insertion and RSA encryption

Garima Tomar
Faculty of Electrical and Electronics,MITS Ujjain

Abstract: This project simulates an effective data hiding technique i.e. steganography based on LSB insertion and RSA encryption in order to provide seven million times better security about hidden data ,than the previous work. The Main idea of proposed scheme is to encrypt secret data by RSA 1024 algorithm, convert it in to binary sequence bit and then embedded into each cover pixels by modifying the least significant bits (LSBs) of cover pixels. The result image is known as steganography image. Steganalysis is the method used by attackers to determine if images have hidden data and to recover that data. In this paper the images names are Baboon, Lena ,Boat are used for experimental purpose. The PSNR value of this steganography image is 54.34 db. 53.32 db,52.55 db respectively..This steganography image is transmitted through AWGN channel, and effects of noises are simulated. The image and hidden data are reconstructed with the SNR level ≥9 dB. The steganography method proposed in this paper is superior to that used by current steganography tools.Beceause by matching data to an image, there is less chance of an attacker being able to use steganalysis to recover the data and Before hiding the data in an image the application first encrypts in it.

Key words: Steganography, LSB, RSAalgorithm, PSNR,

I. INTRODUCTION

In companies with rapid growth of computer and communication networks, internet has been established worldwide that brings numerous convenient applications. Internet is an open system to transmit secret data securely is an issue of great concern. Security could be introduced by hiding this secret information. To hide secret information steganography and cryptography are cousins in the information hiding family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen.

Networks must be able to transfer data from one device to another with complete accuracy. A system that cannot guarantee that the data received by one device are identical to the data transmitted by another device is essentially useless. Reliable systems must have a mechanism for detecting and correcting the errors and are done by using error detection and correction methods. The popularity of the Internet offers a great convenience to the transmission of a large amount of data over networks. The internet is not a single network, but a worldwide collection of loosely connected networks which are accessible by individual computer hosts, in a variety of ways, to anyone with a computer and a network connection. Thus, individuals and organizations can reach any point on the internet without regard to national or geographic boundaries or time of day. However, along with the convenience and easy access to information come risks. Information may be about employees, customers, research, products or financial operations .Among them are the risks that valuable information may be lost, stolen, changed, or misused. If information is recorded electronically and is available on networked computers, it is more vulnerable than if the same information is printed on paper and locked in a file cabinet. Intruders do not need to enter an office or home they may not even be in the same country. They can steal or tamper with information without touching a piece of paper or a photocopier. They can also create new electronic files, run their own programs, and hide evidence of their unauthorized activity.

So Security viewed by information systems has become vital. The term information security means protecting information and information systems from unauthorized access, use, disruption, or destruction. From here the concept of information security is introduced. [1]

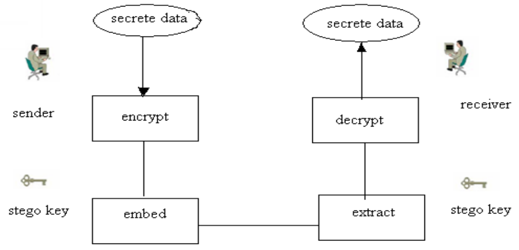


Fig 1 steganography Mechanism

This paper documents the design and development of our data hiding application using steganography. The goal of our application is to help users maintain their data's confidentiality. To achieve this goal, our application uses defense in depth. Not only does it hide the user's data within an image, but it also encrypts the user's data using the public key RSA algorithm. A user friendly GUI is incorporated to ensure psychological acceptability. The application does not rely on keeping its steganography algorithm a secret, nor is

RSA a secret algorithm; our application follows the secure programming principle of open design. To combat steganalysis, our application performs an analysis on the user's library of images. This analysis allows users to hide their data in the image that is least likely to be vulnerable to steganalysis.In this paper also simulates the reconstruction performance of stego image at receiver when these images are transmitted through AWGN channel.

II. RELAT ED WORK

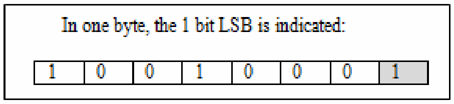
There are many steganography tools which are capable of hiding data within an image. These tools can be classified into five categories based on their algorithms: (1) spatial domain based tools; (2) transform domain based tools; (3) document based tools; (4) file structure based tools; and (5) other categories such as video compress encoding and spread spectrum technique based tools [2]. The spatial domain based steganography tools use either the LSB or Bit Plane Complexity Segmentation (BPCS) algorithm. The LSB algorithm uses either a sequential or scattered embedding schemes for hiding the message bits in the image. In the sequential embedding scheme, the LSBs of the image are replaced by the message bit sequentially (i.e. one by one in order, as mentioned in the introduction). In the scattered embedding scheme, the message bits are randomly scattered throughout the whole image using a random sequence to control the embedding sequence. Two basic types of LSB modifications can be used for the embedding schemes described above. They are LSB replacement and LSB matching. In LSB replacement, the LSB of the carrier is replaced by the message bit directly. On the other hand, in LSB matching if the LSB of the cover pixel is the same as the message bit, then it remains unchanged;

Otherwise, it is randomly incremented or decremented by one. This technique, however, requires both the sender and the receiver to have the same original image, which makes LSB matching very inconvenient [2]. The current Steganography tools based on the LSB algorithms include S-Tools, Hide and Seek, Hide4PGP and Secure Engine Professional. These tools support BMP, GIF, PNG images and WAV audio files as the carriers [2]. Each of these tools has unique features. S-Tools reduce the number of colors in the image to only 32 colors. Hide and Seek makes all the palette entries divisible by four. In addition, it forces the images sizes to be 320x200, 320x400, 320x480, 640x400 or 1024x768 pixels.Hide4PGP embeds the message in every LSB of an 8-bit BMP images, and in every fourth LSB of a 24- bit BMP image. These applications are flawed because they do not analyze the image file after it has been embedded with data to see how vulnerable it is to steganalysis. The transform domain based steganography tools embed the message in the transform coefficients of the image. The main transform domain algorithm is JSteg [2].These applications can only work with JPGs because most other image formats do not perform transforms on their data. The document based steganography tools embed the secret message in document files by adding tabs or spaces to .txt or .doc files [2]. These applications are limited because they only work with document files. They also cannot hide much data because there are a very limited number of tabs or spaces they can reasonably be added to a document. In addition, they are vulnerable to steganalysis because it is easy for an attacker to notice a document file that has been embedded with additional tabs or spaces. The file structure based steganography tools embed the secret message in the redundant bits of a cover file such as the reserved bits in the file header or the marker segments in the file format [2]. These applications cannot hide very large data files because there are a very limited number of header or marker segments available for embedding hidden data.

There are also steganography tools based on video compression and spread spectrum techniques. The large size Of video files provides more usable space for hiding of the message. The spread spectrum technique spreads the energy of embedded message to a wide frequency band, making the hidden message difficult to detect [2]. These steganography tools are inconvenient because they require the users to send an entire video file every time they want to send hidden data.

III LEAST SIGNIFICANT BIT INSERTION METHOD

Least significant bit insertion is a common, simple approach to embed information in a cover file [3]. Usually, three bits from each pixel can be stored to hide an image in the LSBs of each byte of a 24-bit image. The resulting stego-image will be displayed indistinguishable to the cover image in human visual system [4].

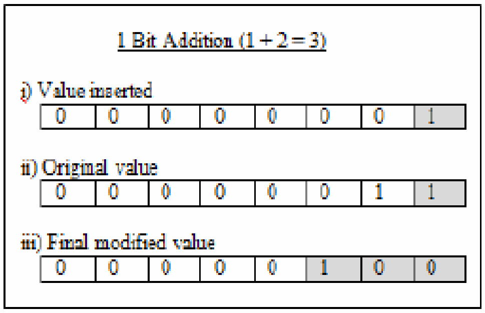


In one byte, the 1 bit LSB is indicated:

1	0	0	1	0	0	0	1

Fig. 2: Least Significant Bit

The last bit of the byte is selected as least significant bit in one bit LSB as illustrated in Figure 2 because of the impact of the bit to the minimum degradation of images [5]. The last bit or also known as right-most bit is selected as least significant bit, due to the convention in positional notation of writing less significant digit further to the right [6]. In bit addition, the least significant bit has the useful property of changing rapidly if the number changes slightly. For example, if 1 (binary 00000001) is added to 3 (binary00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100).



1 Bit Addition (1 + 2 = 3)

i) Value inserted

0	0	0	0	0	0	0	1

ii) Original value

0	0	0	0	0	0	1	1

iii) Final modified value

0	0	0	0	0	1	0	0

Fig. 3: Example of bit addition

There are numbers of steganograpic tools which employ LSB insertion methods available on the web. For example, S-Tools take a different approach by closely approximating the cover image which may mean radical palette changes. Instead, S-Tools reduce the number of colors while maintaining the image quality, so that the LSB changes do not drastically change color values. Another tool which is using LSB manipulation is EzStego. It arranges the palette to reduce the occurrence of adjacent index colors that contrast too much before it inserts the message. This approach works quite well in gray-scale images and may work well in images with related colors [4]. On the other hand, StegCure keeps the advantage of S-Tools and EzStego that is maintaining the image quality, but it can prevent the attack from hackers by restricting user to have only one attempt to perform destego method. If the user has used the wrong destego method for the first time, there is no second attempt to recover the hidden data in the image even though the user has chosen the correct destego method.

IV SIMULATED RESULTS

Tool used: MATLAB Simulink version 7.0 .The name of images are baboon,lena,boat, size of image is 256x256, and format of image is BMP which we have taken for simulation .Here 256x256 meaning that number of rows and column of pixels, and BMP meaning that the format of image i.e. bit map format. These three images are gray scale images i.e. 8 bits per pixel. The proposed method hides secret data bits in LSB of each pixel so we can hide 65536 secret data bits in an image by using row ×column × n relationship. Where n is no of LSBs used.The results are tabulated in Table 3. In Table 3, the column labeled 'Capacity' is the number of bits can be embedded into the host-image and the column labeled 'PSNR' is the peak-signal-to-noise-ratio of the stego-image. The results are the average value of embedding 65536 random bit-streams into the host images.

A simulation results when secret data bits are hide in cover image

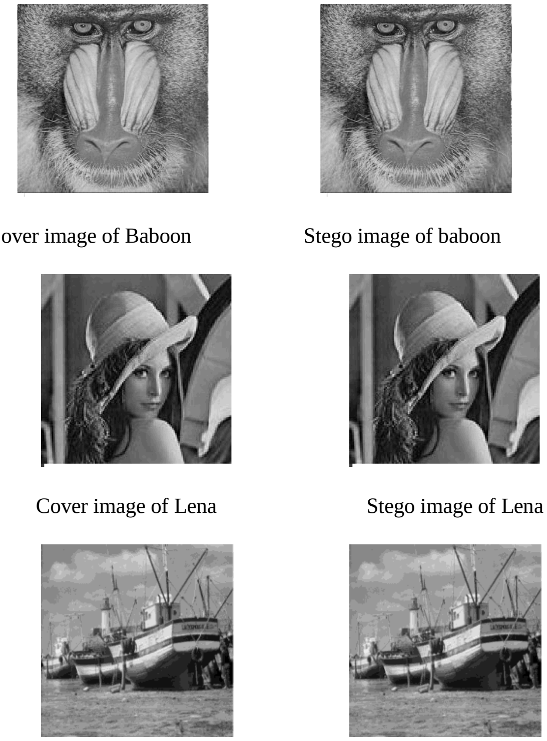
TABLE 3 SIMULATION RESULS WHEN SECRET DATA BITS ARE HIDE IN COVER IMAGE

Name of the images	Embedding secret data capacity in bits	PSNR in db
Baboon	65536	54.34
Lena	65536	53.32
Boat	65536	52.55

- ➢ Here PSNR is calculated by following relation

$$MSE=\frac{1}{H\times W}\sum_{I=1}^{H}.\sum_{J=1}^{W}\left(PVOFCOVER\ IMAGE\ (I,J) - PV\ OF\ STEGO\ IMAGEI,J)2 \right. \quad (3)$$

$$PSNR = 10\log\frac{255^{2}}{MSE} \quad (4)$$



Cover image of Baboon

Stego image of baboon

Cover image of Lena

Stego image of Lena

Cover image of Boat

Stego image of Boat

Fig 4 images used in this simulation

When these images are transmitted through AWGN channel, noises are introduced in it, thereby this stego images may be corrupted by noise and also hidden secret data bits are affected by that noise. The experimental results have shown in table 4, 5, and 6 that how much stego bits and data bits are corrupted by noise. The size of image is 256x256 i.e.65536 total no of pixels or 524288 data streams are transmitted through noisy channel. Additive white Gaussian noises are used in this experiment. The characteristic of this communication system with bit error rate (*BER*) versus signal noise ratio (*SNR*, E_b/N_0, *dB*), where E_0 is energy per bit and N_0 is noise spectral density. Such a controlled noise was added in every channel and that stego image is transmitted over the channel bit by bit. The number of error bits was measured at every controlled noise level to obtain BERs for test image during the stego image transmission. The received stego bits are used to reconstruct the stego image, and extract secret data bits by using decryption algorithm. The error correction results of the proposed method are given in the table 4, 5, 6.

B. simulation results when Baboon stego image (data stream) is transmitted through AWGN channel.

Table 4 simulation results when stego image is transmit through AWGN channel

SNR IN db	No of bits corrupted through AWGN/ 524288	No of hidden data bits corrupted through AWGN /65536
0	41086	5080
1	29086	3688
2	11958	1466
3	6491	815
4	3231	411
6	1217	146
8	86	14
9	24	4
10	2	1

C. simulation results when Lena stego image (data stream) is transmitted through AWGN channel .

Table 5 simulation results when stego image is transmit through AWGN channel

SNR IN db	No of bits corrupted through AWGN /524288	No of hidden data bits corrupted through AWGN /65536
0	40086	5180
1	20086	3088
2	10958	1566
3	6291	715
4	3331	401
6	1227	136
8	76	13
9	10	3
10	3	1

D.simulation results when Boat stego image (data stream) is transmitted through awgn channel.

Table 6 simulation results when stego image is transmit through AWGN channel

SNR IN db	No of bits corrupted through AWGN/ 524288	No of hidden data bits corrupted through AWGN /65536
0	42086	5180
1	23086	3788
2	10958	1366
3	6391	715
4	3031	421
6	1117	136
8	96	13
9	20	3
10	2	1

V CONCLUSION

The conclusion of these experimental results is that- The proposed data hiding scheme is an efficient data hiding scheme based on the LSB insertion and RSA encryption method by its PSNR value of image like baboon is 54.34 dB, 53.32dB, 52.55dB which is not noticeable by human eyes. Enhance security of hidden data by $7x10^6$ times than the RSA-512 in terms of its time complexity, and 2650 times in space complexity. The steganography images are transmitted through AWGN channel, and reconstruction performance is simulated. The image and hidden data are reconstructed with the SNR level ≥9 dB.

REFERENCES

1. Implementing Cisco IOS Network Security (IINS) Catherine Piquet Copyright © 2009 Cisco Systems, Inc. Published by: Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.
2. Ming, Chen, Z. Ru, N. Xinxin, and Y. Yixian, “Analysis of Current Steganography Tools: Classifications & Features”, Information Security Beijing University of Posts & Telecommunication, Beijing, December 2006. Centre.
3. Chandramouli R and Memon N, “Analysis of LSB based image steganography techniques”, *Proceedings 2001 International Conference on Image*, Vol. 3, pp. 1019-1022.
4. StegCure: An Amalgamation of Different Steganographic Methods inGIF Image L.Y. Por1, W.K. Lai2, Z. Alireza3, B. Delina4 Faculty of Computer Science and Information Technology University of Malaya 50603, Kuala Lumpur MALAYSIA .
5. S. Katzenbeisser, Fabien A.P. Petitcolas, *Information Techniques for Steganography and Digital Watermarking*, Artech House, Boston, London, 2000.
6. John Kadvany, “Positional Value and Linguistic Recursion”, *Springer Netherlands*,Vol. 35, December 2007, pp. 487-520.

7. comparison between viterbi algorithm soft and hard decision decoding Dr H. MelianiAl-Ahsa College of Technology,KSAA.Guellal University of Blida, Algeria
8. Charon Langton, Coding and decoding with conventional codes1999.
9. N. F. Johnson, S. Jajodia, “Exploring Steganography: Seeing the Unseen,” *IEEEComputer*, February 1998, pp.26-34.*Image*, Vol. 3, pp. 1019-1022. L.Y. Por1, W.K. Lai2, Z. Alireza3, B. Delina4,2008.
10. Mohammed Al-Mualla and Hussain Al- Ahmad, “Information Hiding: steganography and Watermarking”. [Online]. Available:*http://www.emirates.org/ieee/information_hiding.pdf*,[Accessed: March 12, 2008].
11. Andrew D. Ker,“Steganalysis of Embedding inTwo Least-Significant Bits”,*IEEETransactions On Information Forensics And Security*,Vol. 2, No 1, March 2007, pp. 46-54.
12. NeetaDeshpande,SnehalKamalapurandJacobsDaisy,“Implementation of LSBsteganography and Its Evaluation for VariousBits”,*1st International Conference on DigitalInformation Management*, 6 Dec. 2006 pp.173-178.
13. Muthiyalu Jothir,Navaneetha Krishnan,“Statistical models for Secure steganographySystems”, *Digital Rights Management Seminar*, 15th May, 2006.
14. S. Reinsberg, et. al., Phys. Med. Biol. 50, 2651-2661, (2005) T. Morkel, J.H.P. Eloff, M.S. Olivier, “An Overview of Image Steganography”, *Proceedings of the Fifth Annual InformationSecurity South Africa Conference (ISSA2005)*.
15. Mahomet Utku Celik, Gaurav Sharma, Ahmet Murat Tekalp and Eli Saber.“LosslessGeneralized-LSBDataEmbedding”, *IEEETransaction on Image Processing*, Vol. 14, No.2, Feb 2005, pp. 253-266.Sandton, South Africa, 2005.
16. Alain Brainos, “A Study of steganography and the Art of Hiding Information”, *SecurityWriter*,July 27, 2004.
17. Chip Fleming, 'A tutorial on convolutional coding with Viterbi algorithm',2003.
18. Der-Chyuan Lou and Jiang-Lung Liu,“Steganographic Method for Secure Communications”, *Elsevier Science Ltd*, Vol21, No 5, 2002, pp 449-460.
19. Simon Haykin, 'Communication Systems', 4th edition, John Wiley & sons, Inc. 2001.
20. John G. Proakis, 'Digital Communications', Mc.Graw Hill, 4th edition, 2001.
21. Petitcolas, Fabien A.P., “Information Hiding: Techniques for Steganography and Digital Watermarking.”, 2000
22. Krinn, J., “Introduction to Steganography”, 2000
23. S. Katzenbeisser, Fabien A.P. Petitcolas,*Information Techniques for Steganography and Digital Watermarking*, Artech House, Boston,London, 2000.
24. Charon Langton, Coding and decoding with conventional codes', July 1999.
25. Westfield Andreas and Andreas Pfitzmann, Attacks on Steganographic Systems, *Third International Workshop, IH'99 Dresden Germany*, October Proceedings, Computer Science 1768, 1999, pp. 61-76.
26. N. F. Johnson, S. Jajodia, “Exploring Steganography: Seeing the Unseen,” *IEEE Computer*, February 1998, pp.26-34.
27. Memon, N. and Rodila, R. ,“Transcoding GIFimages to JPEG-LS”, Consumer Electronics,IEEE Transactions on Consumer Electronics,Vol. 43, Issue 3, Aug 1997.
28. Raymond Steel, ' Mobile radio communication',Raymond Steel Publishers, London edition,995.
29. Jacques Dupraz, 'Théorie du signal et transmission de l'information', Eyrolles édition,1989.
30. J.C. Bic/ D. Duponteil., J.C. Imbeaux,'Eléments de communications numériques.Transmission sur fréquence porteuse'. Dunod edition, 1986.
31. J.C. Fantou, 'Théorie de la transmission numérique', édition, 1977.
32. J. Clavier, M. Niquil, G. Coffinet, F.Behr 'Théorie et technique de la transmission de des données', Tome1, Masson, Paris édition, 1972.
33. Manjeet Singh,Ian J. Wassel 'Comparison between Soft and Hard decision decoding using quaternary convolutional encoders and thedecomposed CPM model', Laboratory for communications Engineering, Department of Engineering, University of Cambridge.