Information Hiding Using Least Significant BitSteganography and Cryptography

P.Sandeep Reddy,CH Venkata Navi,N Mahesh Babu
Associate Professor, Assistant Professor[2,3]
Dept. of CSE,
mail-id: sandeepreddycse@anurag.ac.in , chejarla.venkatanavi5@gmail.com, mahesh.nallagatla@gmail.com
Anurag Engineering College,Anatagiri(V&M),Suryapet(Dt),Telangana-508206

***Abstract*—**Steganalysis is the art of detecting the message's existence and blockading the covert communication. Various steganography techniques have been proposed in literature. The Least Significant Bit (LSB) steganography is one such technique in which leastsignificant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This paper uses two popular techniques Rivest, Shamir, Adleman (RSA) algorithm and Diffie Hellman algorithm to encrypt the data. The result shows that the use of encryption in Steganalysis does not affect the time complexity if Diffie Hellman algorithm is used in stead of RSA algorithm.

***Index Terms*—**Cryptography, Image hiding, Least- significant bit (LSB) method, Steganography

INTRODUCTION

With the recent advances in computing technology and its intrusion in our day to day life, the need for private and personal communication has increased. Privacy in digital communication is desired when confidential information is being shared between two entities using computer communication. To provide secrecy in communication we use various techniques. One such technique is Steganography [1-2] that is the art of hiding the fact that communication is taking place, by hiding information in other information. Classification of stenography techniques based on the cover modifications applied in the embedding process is as follows:

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.

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 makes 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 itis left as such.

D. Distortion techniques

In this technique [12-15] the knowledge of original cover in the decoding process is essentail at the receiver side. Receiver measures the differences with the original cover in order to reconstruct the sequence of modificationapplied by sender.

This paper tries to overcome the disadvantage of the LSB method [16-20] by appending encrypted data in image in place of plain textual data. To encrypt the data RSA [21] and Diffie Hellman [21] 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.

The paper has been organized as follows: Section 2 provides the proposal, Section 3 provides the simulation and results, Section 4 provides the inference of the results, Section 5 provides the conclusion followed by references.

THE PROPOSED SCHEME

A. Sender Side

The proposed scheme uses RSA or Diffie Hellman algorithm 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 byLSB encoder which replaces the least significant bit of pixel values with the encrypted information bits. The modified picture is now termed as Stego image. The whole process is explained in Fig. 1.

A. 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 decryption algorithms. This is how, the plain text is recovered from image. Fig. 2 shows the whole process at the receiver side.

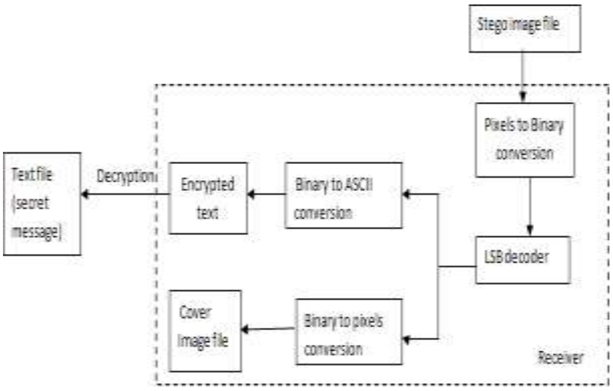
Stego image file
Pixels to Binary conversion
Text file (secret message)
Decryption
Encrypted text
Binary to ASCII conversion
LSB decoder
Cover Image file
Binary to pixels conversion
Receiver

Figure 2. Proposed steganography mechanism for receiver

I. SIMULATION AND RESULTS

We simulate the process as shown in Fig. 1 and Fig. 2 using MATLAB-7.01. Since the number of instructions executed is a measure of time complexity of thealgorithm 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.

A. Simulation Setup

The various simulation parameters are given in Table 1.

TABLE I.
SIMULATION SETUP PARAMETERS

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

The plain text, encrypted text using RSA and DiffieHellman algorithms are shown in Fig. 3.

B. Impact of single Bit Steganography on Images

Fig 4 shows the impact when one LSB of the image is replaced with data. The embedded data can be in encrypted or plain textual form. The following pointsmay be noted:

- There is no visible change in the picture quality for pure as well as Diffie Hellman and RSA steganographic techniques.
- The complexity of Diffie Hellman steganography is nearly same as that of puresteganography.
- As the number of pixels in image increases, the number of instruction (complexity) at the senderand receiver side increases as can be shown in the graphs of Fig. 5 and Fig. 6.

C. Impact of Two Bit Steganography on Images

Fig. 7 shows the impact of changing two bits of imagewith data. The data can be in encrypted or plain textualform. The following points may be noted:

- There is a slight change in the picture quality as is evident from the picture.
- As the number of pixels in image increases, the complexity at the sender and receiver increases as shown in Fig. 8 and Fig. 9.
- There is an increase of 10% to 66% in the number of instruction execution in comparison to one bit steganography for pure steganography combined with RSA algorithm.
- There is a marginal increase (up to 3%) in the number of instruction in comparison to one bit steganography for pure steganography combined with Diffie Hellman algorithm.
- The complexity of steganography combined with RSA algorithm has higher complexity in comparison to pure and steganographycombined with Diffie Hellman algorithm.

Distortion is much more prominent in comparison to one and two bit steganographicschemes.
The complexity of pure steganography combined with RSA algorithm (three bits) increases by 15 to 40% in comparison to two bit pure steganography combined with RSA.

- As the image size increases the complexity at both the sender and receiver side increases as shown in Fig. 11 and Fig. 12.
- The complexity of Pure Steganography and steganography combined with Diffie Hellmanalgorithm is nearly same The following inference can be drawn:

As the size of the image increases thecomplexity at sender and receiver side increases.

- The RSA algorithm is more secured than Diffie Hellman algorithm when combined with pure steganography but at the same time has highest time complexity.
- Both Diffie Hellman RSA algorithms can be used in combination with pure steganography
- The time complexity increases with the number of embedded bits in image.

CONCLUSION

The LSB modification technique provides an easy way to embed information in images, but the data can be easily decoded. The proposed scheme used in this paper encrypts the secret information before embedding it in theimage. 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

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).

Clair, Bryan, “Steganography: How to Send a Secret Message”, 8 Nov. 2001 www.strangehorizons.com/2001/20011008/steganogr aphy.shtml.

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

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.

Gruhl, D., A. Lu, and W. Bender, “Echo Hiding in Information Hiding”, First International Workshop, Proceedings, vol. 1174 of Lecture Notes in ComputerScience, Springer,1996, pp. 295-316.

Kurak, C., and J. McHughes, "A Cautionary Note OnImage Downgrading", in IEEE Computer Security Applications Conference 1992, Proceedings, IEEEPress, 1992, pp. 153-159.

van Schyndel, R. G., A. Tirkel, and C. F. Osborne, "A Digital Watermark", in Proceedings of the IEEE International Conference on Image Processing, vol. 2,1994, pp. 86-90.

Johnson, N. F., and S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE Computer,vol. 31, no. 2, 1998, pp. 26-34.

Rhodas, G. B., "Method and Apparatus Responsive to a Code Signal Conveyed Through a Graphic Image", U.S. Patent 5,710,834, 1998.

Swanson, M. D., B. Zhu, and A. H. Tewk, "Transparent Robust Image Watermarking", in Proceedings of the IEEE International Conference onImage Processing, vol. 3, 1996, pp. 211-214.

Pitas, I., "A Method for Signature Casting on Digital Images," in International Conference on Image Processing, vol. 3, IEEE Press, 1996, pp. 215-218.

Maxemchuk, N. F., "Electronic Document Distribution", AT&T Technical Journal, September/October 1994, pp. 73-80.

Low, S. H., et al., \Document Marking and Identifications Using Both Line and Word Shifting," in Proceedings of Infocom'95, 1995, pp. 853-860.

Low, S. H., N. F. Maxemchuk, and A. M. Lapone, "Document Identification for Copyright ProtectionUsing Centroid Detection", IEEE Transactions on Communications, vol. 46, no. 3, 1998, pp. 372-383.

Low, S. H., and N. F. Maxemchuk, "Performance Comparison of Two Text Marking Methods", IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, 1998, pp. 561-572.

"Information Hiding Techniques for Steganography and Digital water Mark", Stepfan Katzenbeisser, Fabien A.P. patitcolas chapter no 3, pp no. 56. Also available at amazon.com.

Johnson, Neil F., and SushilJajodia. "Exploring Steganography: Seeing the Unseen", IEEE ComputerFeb. 1998: 26-34.

A. Ker, "Improved detection of LSB steganography in grayscale images," in Proc. Information Hiding Workshop, vol. 3200, Springer LNCS, pp. 97–115, 2004.

A. Ker, "Steganalysis of LSB matching in greyscale images," IEEE Signal Process. Lett., Vol. 12, No. 6, pp. 441–444, June 2005.

Sujay Narayana and Gaurav Prasad, "TWO NEW APPROACHES FOR SECURED IMAGE STEGANOGRAPHY USING CRYPTOGRAPHIC TECHNIQUES AND TYPE CONVERSIONS", in

Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010.

"Cryptography and Network Security: principles and practices", William Stallings, pearsons education, first Indian reprint 2003.