Information Hiding Using Least Significant Bit Steganography and Cryptography

Shailender Gupta
Department of Electrical & Electronics Engineering, YMCAUST, Faridabad, India
Email: shailender81@gmail.com

Ankur Goyal
Department of Electrical & Electronics Engineering, YMCAUST, Faridabad, India
Email: eng.goyal@gmail.com

Bharat Bhushan
Department of Electrical & Electronics Engineering, YMCAUST, Faridabad, India
Email: bhrts@yahoo.com

Abstract—Steganalysis is the art of detecting the message’s existence and blocking the covert communication. Various steganography techniques have been proposed in literature. The Least Significant Bit (LSB) steganography is one such technique in which least significant 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

I. 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 it is left as such.

D. Distortion techniques

In this technique [12-15] 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 [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.

II. 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 by LSB 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.

III. 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 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.

A. Simulation Setup

The various simulation parameters are given in Table 1.

<table>
<thead>
<tr>
<th>TABLE I. SIMULATION SETUP PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Pixels (NXN)</td>
</tr>
<tr>
<td>Number of bits changed</td>
</tr>
<tr>
<td>Image Type</td>
</tr>
<tr>
<td>Encryption</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
</tr>
<tr>
<td>Simulation Tool</td>
</tr>
</tbody>
</table>

The plain text, encrypted text using RSA and Diffie Hellman 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 points may 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 pure steganography.
- As the number of pixels in image increases, the number of instruction (complexity) at the sender and 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 image with data. The data can be in encrypted or plain textual form. The following points may be noted:

- There is a slight change in the picture quality as 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 steganography combined with Diffie Hellman algorithm.
D. Impact of Three Bit Steganography on Images

Fig. 10 shows the impact of changing three bits of image with data. The data can be in encrypted or plain textual form. The following points may be noted:

- Distortion is much more prominent in comparison to one and two bit steganographic schemes.
- 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 Hellman algorithm is nearly same.
Information Hiding Using Least Significant Bit Steganography and Cryptography

Figure 8. Complexity vs Image size at sender side

Figure 9. Complexity vs Image size at receiver side

Figure 10. Impact of Three bit steganography
E. Impact of Four Bit Steganography on Images

Fig. 13 shows the impact of changing four bits of image with data. The data can be in encrypted or plain textual form. The following may be noted:

- The picture quality deteriorates significantly as is evident from the Fig. 13
- The complexity increases for every scheme as is evident from the graphs as shown in Fig. 14 and Fig. 15.

IV. INFERENCES

The following inference can be drawn:

- As the size of the image increases the complexity 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.
Information Hiding Using Least Significant Bit Steganography and Cryptography

V. 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 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


[20] Sujay Narayana and Gaurav Prasad, "TWO NEW APPROACHES FOR SECURED IMAGE STEGANOGRAPHY USING CRYPTOGRAPHIC TECHNIQUES AND TYPE CONVERSIONS", in
Mr. Shailender Gupta is B.Tech (Electronics Engineering), M.Tech (Computer Engineering) and pursuing his Ph. D in the area of ad-hoc mobile network security. His academic interests include network security, Signal Processing, automata theory and fuzzy logic. Currently working as Assistant Professor in Electronics Engineering department at YMCA University of Science and Technology, Faridabad, India.

Mr. Bharat Bhushan is B.Tech (Electronics Engineering) and M.Tech (Electronics Engineering). His academic interests include Mobile Ad-hoc Network, Network Security. Currently he is working as Assistant Professor in Electronics Engineering department at YMCA University of Science and Technology, Faridabad, India.

Mr. Ankur Goyal is B.Tech (Electronics Engineering) and pursuing his M.Tech in Electronics Engineering from YMCA University, Faridabad India. His academic interests include Mobile Ad-hoc Network, Network Security and Steganography.