Cryptography and Steganography: for Data Hiding

Asha Jaiswal
M Kumari

This work is licensed under a Creative Commons CC_BY-NC International License.

Available at: https://works.bepress.com/article/25/
Cryptography and Steganography: for Data Hiding

Asha Jaiswal, M Kumari
M.Tech CSE Deptt. BPSMV Khanpur Kalan (Sonipat)

Abstract: Now a day's securing of data is a big issue. Most of the data sending and receiving on internet, so it is difficult to make data secure. So cryptography and steganography combine to secure data while transmitting in the network. In this paper using two techniques cryptography (AES, DES) and steganography (SLSB).compares their performance of encrypt techniques based on transmitting, receiving and total time use when combine the techniques. The entire process has done in Matlab.

Keyword: cryptography, steganography, DES, AES, SLSB.

I. INTRODUCTION

Now a day development of communication system demands is very high so securing of information is must. Therefore the confidentiality and the reliability of the data protected from unauthorized person. For the protection of information cryptography and steganography are the two security tools used. Confidentiality, accessibility and integrity are main concepts of information security Cryptography and Steganography are the security tools available for the protection of the secret information [1].

1. Cryptography

Cryptography is an encryption technique used to convert the readable information into secreted form. For keeping message secure and free from attacks. Cryptography is the art of achieving security by encoding the data into secrete form [2]. Generally, all cryptographic processes have four basic parts:

1. Plaintext - Unscrambled information to be transmitted. It could be a simple text document, a credit card number etc, transmitted between organizations.

2. Cipher text- plain text convert into secreted form by the application of a mathematical algorithm. Cipher text encrypted plain text that is transmitted to the receiver.

3. Key- A mathematical value or process that determines how a plaintext message is encrypted or decrypted.

4. Cryptographic Algorithm – A mathematical formula used to scramble the plain text to yield cipher text. Converting plain text to cipher text using the crypticographic algorithm is called encryption, and converting cipher text back to plain text using the same cryptographic algorithm is called decryption

There are two types of encryption algorithms: In Symmetric key encryption sender and receiver will have the same key for the process of encryption and decryption of data. In asymmetric key encryption algorithm different keys are used at sending and receiving site for encryption and decryption.

2. Steganography

Steganography is a technique used to transmit a secret message from a sender to a receiver in a way which provides privacy of text or images to protect from disputers [1]. This can be done by embedding the secret message within another digital medium such as text, image, audio or video. Steganography is a Greek origin. Stegano means “covered or protected”, and graphy meaning “writing” messages will appear to be something else: images, articles, shopping lists, or some other “cover-text” and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. It is a high security technique for long data transmission. [3].

II. RELATED WORK

At present, various types of cryptographic algorithms provide high security to information on networks, but there are also has some drawbacks. This hybrid algorithm is designed for better security by combinations of AES and DES.each byte of the plaintext is uses AES or DES algorithms; ka and kd represent the key for AES and DES. For example, we have 8 bit size of plaintext, first bit uses AES to encrypt and second bit uses DES to encrypt. The decryption process is invert of the encryption process. The AES, DES and Hybrid algorithms have been implemented in VC++ and the following results were obtained. I. AES Encryption, II. AES Decryption, III. DES Encryption, IV. DES Decryption, V. Hybrid Algorithm Encryption, VI. Hybrid Algorithm Decryption, VII. Encrypt/Decrypt file, VIII. Encrypt/Decrypt String [4]. The analysis work surveyed the previous encryption methods including AES, DES along with RSA algorithms in addition to LSB alternative method. Individuals encryption methods tend to be learnt along with assessed very well to market the effectiveness with the encryption procedures in addition to guarantee the safety measures.
Based on the experimental result it turned out figured AES formula consumes minimum encryption along with decryption occasion along with barrier use compared to DES formula. Although RSA eat far more encryption occasion along with barrier use can also be high. Most of us in addition discovered that will decryption connected with AES formula surpasses other algorithms. From your simulation result, most of us evaluated that will AES formula are more preferable as compared to DES along with RSA formula [5].

III. ADVANCED ENCRYPTION STANDARD (AES)

AES is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. AES encrypt the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. Brute force attack is the only effective attack known against this algorithm. AES encryption is fast and flexible [6]. AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of $4 \times 4$ that is called the state. For both encryption and decryption, the cipher begins with an AddRoundKey stage. However, before reaching the final round, this output goes through nine main rounds, during each of those rounds four transformations are performed 1. Sub-bytes 2. Shift-rows 3. Mix-columns 4. Add round Key. In the final (10th) round, there is no Mix-column transformation [7], [8].

IV. DATA ENCRYPTION STANDARD (DES)

DES as defined is a block encryption algorithm it was designed in 1970’s by IBM. It uses one 64-bit key, 56 bits make the independent key and reaming 8 bits are used for error detection. The main operations are bit permutations and substitution in one round of DES. Six different permutation operations are used both in key expansion part and cipher part. Decryption of DES algorithm is similar to encryption, only the round keys are applied in reverse order. The biggest disadvantage of DES is the 56 bit key size today it is very small size, it is easily break by hacker [6] [9].

V. SLSB

In the following paragraphs, the explanation of the operations that are doing by the Segmented LSB (SLSB) will be given. Before listing the algorithm’s steps that describe the operations of (SLSB):

1. Message B: is a list that contains a binary representation (bits) of all characters in the secret Message. The number of elements of this list is $(n*8)$, where $n$ is the number of characters in the secret Message.
2. Data B: is a list of the Least Significant Bit (LSB) of all pixels in the Stego-image. The number of elements (size) of this list is $(m)$, where $m$ is the size of the Image and its equal $(\text{Width} \times \text{Height} \times \text{Palette})$.
3. Segment Length: is a positive integer number between $(2 \ldots (n*8)/2)$ which represents the length of each segment (number of bits) in the Segment List.
4. Segments List: is a list of segments that is created from the Message B by splitting it to $k$ segments, where $k = (n*8) / \text{Segment Length}$. And each segment has number of bits equal Segment Length.
5. Segment Index: is a list of indices, each index represents the first index of a sequence of bits in Data B that is having a best match with the bits of one of the segments in Segments List. We must note that there is no overlapping between the sequences of match bits in this technique [10].

VI. PROPOSED WORK

In the present research work planning has been made to proposed technique(s) to enhance the information security. AES and DES is most popular technique used by sender for encryption of data. Key size of AES is large so it is time consuming techniques to overcome this problem SLSB steganography technique use. Brute force attack is most effective against AES so we use DES encryption on output of AES to make it more secure. But as time passes new algorithms replace old algorithms due to some best features. So combination of AES, SLSB with steganography and then DES will replace old technique in case of time consumption in encryption/decryption. These techniques used on transmitter and receiver side.
VII. FLOWCHART

Enter 16 plain text bytes as input

Current plaintext from hexadecimal (string) to decimal representation

VIII. RESULT ANALYSIS

The histogram represents the timing of data receiving and transmitting after encoding in AES algorithm. Red color on x-axis represents transmit time and represents receiving time of AES algorithm, DES data with Blue color. In comparison, AES is time consuming.

Figure 1. Comparative graphs of DES and AES

Figure 2: Total time consume by all three techniques

Table-I
Comparative table for all techniques in combined approach (DES+AES+SLSB)

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Technique Name</th>
<th>Transmit Time (ms)</th>
<th>Receiving Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DES</td>
<td>0.35</td>
<td>0.31</td>
</tr>
<tr>
<td>2</td>
<td>AES</td>
<td>1.29</td>
<td>0.78</td>
</tr>
<tr>
<td>3</td>
<td>SLSB</td>
<td>0.1</td>
<td>Not Exist</td>
</tr>
<tr>
<td>4</td>
<td>DES+AES+SLSB</td>
<td>Total Time = 2.83</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3: Time consume by only AES in combination approach of AES + SLSB
Figure 4: represents time consuming by SLSB and histogram 4 represents total time consuming by combined approach AES+SLSB

Table-II
Comparative table for all techniques in combined approach (AES+SLSB)

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Technique Name</th>
<th>Transmit Time (ms)</th>
<th>Receiving Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>AES</td>
<td>0.9</td>
<td>0.7</td>
</tr>
<tr>
<td>2.</td>
<td>SLSB</td>
<td>0.1</td>
<td>Not Exist</td>
</tr>
<tr>
<td>3.</td>
<td>AES+SLSB</td>
<td>Total Time = 1.7</td>
<td></td>
</tr>
</tbody>
</table>

Table-III
Comparative table for combined approach (DES+AES+SLSB) & (AES+SLSB)

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Technique Name</th>
<th>Total Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>DES+AES+SLSB</td>
<td>2.83</td>
</tr>
<tr>
<td>2.</td>
<td>AES+SLSB</td>
<td>1.7</td>
</tr>
</tbody>
</table>

IX. CONCLUSION

Some data is much important that it may be harmful for organization/institute if it reaches in hands of unauthorized person. Information security is must; there are both techniques cryptography and Steganography apply for securing the information. So combination of AES and DES with steganography will replace old technique in case of time consumption in encryption/decryption.

X. FUTURE SCOPE

We have discussed that AES and DES encrypt text with SLSB in this thesis work. Now some following work can enhance the result:

1. In future RSA separately can implement with SLSB technique for better results.
2. Neural will also enhance this work if using with combination of RSA and SLSB

REFERENCES


