

Combining Cryptography and Steganography for Efficient Secure Image Transmission

Khin Cho Win

University of Computer Studies, Mandalay
mmyo763@gmail.com

Abstract

The security of data transferring is accepted as the challenging problem all over the world. In this system, the image file of any kinds of format is encrypted by using S-DES (Simplified Data Encryption Standard) in Cryptography, and then the cipher is embedded into the innocuous cover image file by using LSB (Least Significant Bit) in Steganography. Since S-DES is a standard education algorithm providing a tradeoff between encryption speed and security that is required for image encryption, encryption and decryption process of this system is extremely fast. To be more secure, cover image file is used to hide the obtained cipher. As this system takes the advantage of both techniques, image transferring is more confidential. In this paper, the system implements SDES and LSB.

1. Introduction

As the performance of the computer and network components has increased in the last few years, people can now exchange complex multimedia data, image file, speech and video, etc. In communication system, security of the data has an essential importance. Nowadays, cryptography and steganography are the two popular security techniques.

Cryptography is the art of converting the messages into a form that is readable, but not understandable. Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether, forcing people to study other methods of secure information transfer. Businesses have also started to realize the potential of steganography in communicating trade secrets or new product information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit. Hiding information in a

photograph of the company picnic is less suspicious than communicating an encrypted file [3]. Steganography is the art and science of hiding data into different carrier files such as text, audio, images, video, etc.

In cryptography, the secret message that is sent may be easily detectable by the attacker. But in steganography, the secret message is not easily detectable. The people other than the sender and receiver are not able to view the secret message.

Even though both cryptography and steganography provide security in their own respective ways, combining both techniques into one system makes the information better confidentiality and security.

In this system, the image is encrypted with S-DES (Simplified Data Encryption Standard). Then, the resulted cipher is embedded within another image file with LSB (Least Significant Bit) Insertion Method. The overall system flow is described as follows:

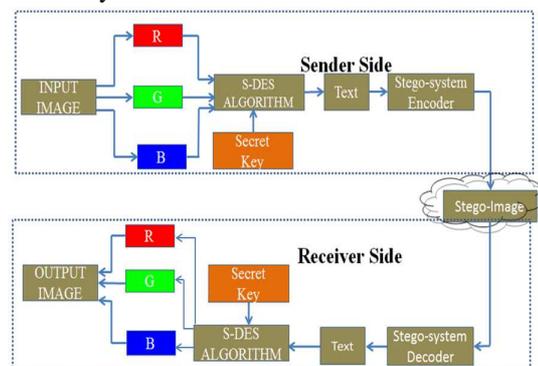


Figure 1. Overall System Flow

The system requires a secure exchange of a shared secret key that is outside of the specification. One of the best methods to transfer the secret key securely is the face-to-face exchange of the key.

2. Related Works

Nowadays, Internet plays an important role in society. As a consequence, people use Internet as data transfer protocol, especially in military. Government, military, financial institution, and private business have

a great deal of confidential images. In communication system, security of these transferred confidential image data has an essential importance, since a breach of security about these such as enemy positions and patient can cause leading to war and wrong treatment.

With the shared volume of sensitive Internet transactions that occur daily, the benefit of securing information using cryptographic processes along with steganography methods becomes a major goal for many organizations. In health (medicine), military image data (defense), personal photo album, financial institution, and private business amass, image data are very important. So, research in image security is still trying in many organizations.

- Within the context of any application-to-application communication, there are some specific security requirements, including:
- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. Steganography hides the existence of the communication.

3. Theoretical Background

3.1. Cryptography

The word cryptography comes from Greek words, “kryptos” meaning “hidden” and “graphain” meaning “writing”, defining as “secret writing”. Cryptography is the science of disguising a message; i.e.; the process of converting an intelligible plaintext into an unintelligible ciphertext. The purpose of cryptography is to conceal the meaning of a message to anyone except for the intended recipient(s).

It is especially useful in the cases of financial and personal data, irrespective of the fact that the data is being transmitted over a medium or is stored on a storage device. Because of the development of electronic commerce, cryptographic techniques are extremely critical to the development and use of

defense information systems and communication networks.

The meaning of Cryptography has now become an industry standard for providing information security, trust, controlling access to resources, and electronic transactions. Its use is no longer limited to just securing sensitive military information. In fact, cryptography is now recognized as one of the major components of the security policy of an organization.

The four objectives in modern Cryptography:

- Confidentiality (unauthorized person will not be able to understand the data)
- Integrity (the data can't be altered in the storage between sender and receiver)
- Authentication (confirmation from the sender and receiver side)
- Non-repudiation (at the last stage, the sender will not be able to refuse the data which is about for transmission)

Generally, all cryptographic processes have four basic parts: plaintext, ciphertext, cryptographic algorithm, and key.

3.1.1. Various Cryptographic Algorithms

There are three kind of cryptographic functions:

- Secret Key Cryptography (SKC): It is used a single key for both encryption and decryption.
- Public Key Cryptography (PKC): It is used one key for encryption and another for decryption.
- Hash Functions: It is used a mathematical transformation to irreversibly “encrypt” information.

3.2. Steganography

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography comes from the Greek “Steganos”, which means covered or secret and “graphy” means writing or drawing.

History is full of facts and myths about the use of steganography. In China, war messages were written on thin pieces of silk and rolled into a small ball and swallowed by the messenger. In Rome and Greece, messages were craved on pieces of wood that were later dipped into wax to cover the writing. Invisible inks (such as onion juice or ammonia salts) were also used to write a secret message between the lines of the covering message or on the back of the paper; the

secret message was exposed when the paper was heated or treated with another substances [1].

There has been a rapid growth of interest in steganography for two main reasons [2]:

- The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products.
- Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

The basic model of steganography consists of Carrier, Message, and Password.

4. Image Encryption and Image Steganography

There are many algorithms for image encryption. And, nowadays, the two main problems in image encryption are (1) computational time, (2) security level. Real time image encryption prefers ciphers that take less amount of computational time without compromising security. The reasons for choosing S-DES as an encryption algorithm are:

- Encryption speed is faster than other algorithms such as AES, Triple-DES
- Design simplicity
- It has all features of DES, with smaller parameter
- S-DES system can encrypt the input binary flow of image, but the fixed system structure and fewer keys will still bring some risks.
- It is flexible.

Table 1. Comparison of Algorithms

| Algorithms | Input Block Size | Length of the key | Out-put Block Size | Speed | Design |
|--------------------------------|------------------|-------------------|--------------------|--|--|
| DES (Data Encryption Standard) | 64-bit | 56-bit | 64-bit | Fast in hardware and relatively fast in software | Simple Complex Structure |
| S-DES (Simplified DES) | 10-bit | 8-bit | 10-bit | A little faster than DES | Very simple, Standard Educational Algorithm |
| Triple-DES | 64-bit | 192-bit | 64-bit | Slower than other block cipher methods | Same as DES, but three times the key length of DES |

| | | | | | |
|------------------------------------|---------------------------|---------------------------|---------------------------|--|--|
| AES (Advanced Encryption Standard) | 128-bit, 192-bit, 256-bit | 128-bit, 192-bit, 256-bit | 128-bit, 192-bit, 256-bit | Slower than DES because of long key length | Replacement of DES, a little more complicated than DES |
|------------------------------------|---------------------------|---------------------------|---------------------------|--|--|

4.1. Encryption Algorithm S-DES

Simplified DES, developed by Professor Edward Schaefer of Santa Clara University is an educational rather than a secure encryption algorithm. It is a reduced version of the DES.

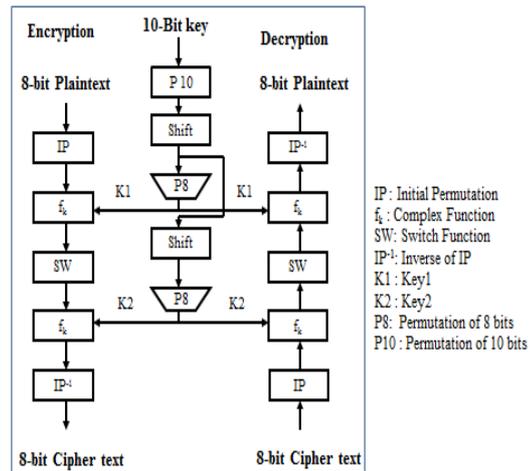


Figure 2. Simplified Data Encryption Standard

4.1.1. SDES Key Generation

As stated in the above figure, the key is first subjected to a permutation (P10). Then a shift operation is performed. The output of the shift operation then passes through a permutation function that produces an 8-bit output (P8) for the first subkey (K1). The output of the shift operation also feeds into another shift and another instance of P8 to produce the second subkey (K2).

$$K1 = P8(\text{Shift}(P10)) \quad (1)$$

$$K2 = P8(\text{Shift}(\text{Shift}(P10))) \quad (2)$$

$$\text{Ciphertext} = IP^{-1}(f_{K2}(SW(f_{K1}(IP(\text{plaintext})))))) \quad (3)$$

$$\text{Plaintext} = IP^{-1}(f_{K1}(SW(f_{K2}(IP(\text{ciphertext})))))) \quad (4)$$

4.1.2. SDES Encryption

The encryption algorithm involves five functions. They are:

1. Initial and final permutation (IP): The input to the algorithm is an 8-bit block of plaintext, which we first permute using the IP function $IP = [2\ 6\ 3\ 1\ 4\ 8\ 5\ 7]$. This retains all 8-bits of the plaintext but mixes them

up. At the end of the algorithm, the inverse permutation is applied; the inverse permutation is done by applying, $IP^{-1} = [4\ 1\ 3\ 5\ 7\ 2\ 8\ 6]$ where we have $IP^{-1}(IP(X)) = X$.

2. The function f_K , which is the complex component of SDES, consists of a combination of permutation and substitution functions. The functions are given as follows.

Let L, R be the left 4-bits and right 4-bits of the input, then, $f_K(L, R) = (L \text{ XOR } f(R, \text{key}), R)$ where XOR is the exclusive-OR operation and key is a sub-key. Computation of $f(R, \text{key})$ is done as follows.

- a. Apply expansion/permutation E/P = [4 1 2 3 2 3 4 1] to input 4-bits.
- b. Add the 8-bit key (XOR).
- c. Pass the left 4-bits through S-Box S_0 and the right 4-bits through S-Box S_1 .
- d. Apply permutation P4 = [2 4 3 1].

3. Since the function f_K allows only the leftmost 4-bits of the input, the switch function (SW) interchanges the left and right 4-bits so that the second instance of f_K operates on different 4-bits. In this second instance, the E/P, S_0 , S_1 and P4 functions are the same as above but the key input is K_2 .

4.1.2. SDES Decryption

The decryption process of S-DES is the reverse process of S-DES encryption algorithm.

4.1.3. Embedding Algorithm LSB

LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden [6]. Consider a 24-bit RGB bitmap image where each pixel is stored as a byte representing color value.

For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

```
(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
```

When the character A, which binary value equals 10000001, is inserted, the following grid results:

```
(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)
```

Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to begin hiding the next character of the hidden message [3].

For embedding the data into an image, two important file is required: cover-image file and the message that needs to be hidden. The cover-image is the innocuous original image.

Before embedding process, the size of the image and the cipher text must be defined by the system. It is very important to ascertain that the cover image file can support the message to be hidden.

The advantages of LSB are its simplicity to embed the bits of the message directly into the LSB plane of cover-image and many techniques use this method [5].

5. Design and Implementation of Proposed System

To provide security in transferring image, this system firstly encrypts the image. Secondly, the resulted cipher hides in an innocuous image that takes as a cover image file. The size of the message file must be quite small compared to the size of the image file. The flow diagram of secure image transfer is shown in figure 3.

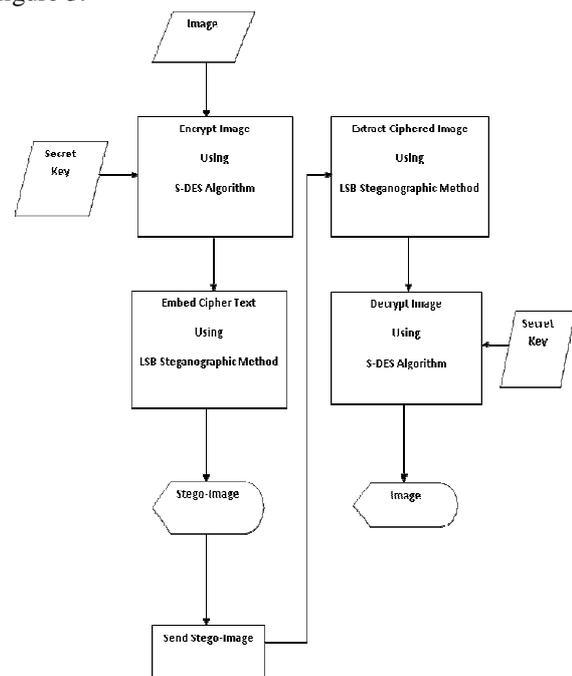


Figure 3. Flow Diagram for Secure Image Transfer

For the message authentication, the message is encrypted with the secret key using the S-DES algorithm. The encrypted message is embedded in the image file (.bmp). And then, it is ready to send the image stego file over the communication channel. Figure 4 shows the sending process.

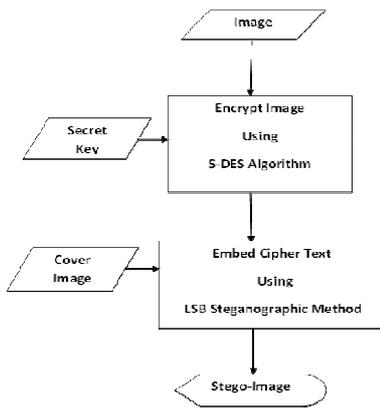


Figure 4. Sender Side

Average encryption time for four image files of different type is shown in figure 5.

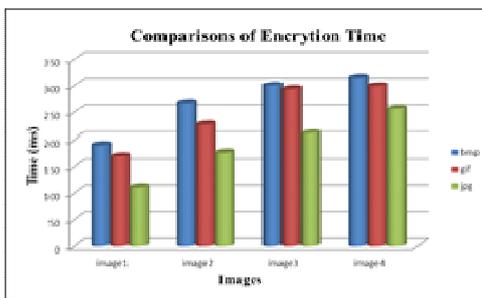


Figure 5. Comparison of Encryption Time

As shown in figure, large file takes much encryption time. So, it is the best to use bmp file type as the cover image file.

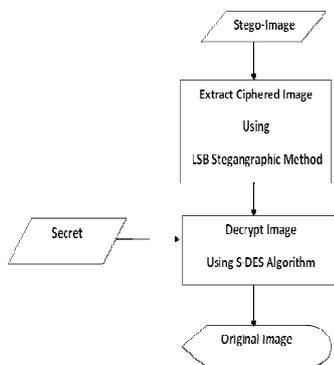


Figure 6. Receiver Side

In the receiver side, with the image stego file the LSB are recovered first and the decryption process with the secret key of the receiver is carried out via S-DES. And then, the secret message is recovered from the stego

file. Figure 6 shows the process of recovering the secret message.

6. Conclusion

Cryptography and steganography are two major branches of data security. The system takes the advantages of Cryptography and Steganography. With the use of Cryptography, the data is transformed from some readable format into the unreadable one, and Steganography hides the presence of the message. Therefore, it can enhance confidentiality of information and provide a means of communication. By using this system, the tradeoff between high encryption time and security can be obtained and private image data can be securely transferred.

References

- [1] Behrouz A.Forouzan Cryptography and Network Security, pp.3, Mc GRAW-HILL INTERNATIONAL EDITION.
- [2] D.Stinson (1995) Cryptography: Theory and Practice, Second Edition, CRC Press, Boca Raton.A.B. Smith, C.D. Jones, and E.F. Roberts, "Article Title," in Proc. IEEE Int. Symp. Circuits and Systems, Monterey, CA, pp. 11-14, June 1998.
- [3] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia Application of LSB Based Steganographic Technique for 8-bit Color Images, World Academy of Science, Engineering and Technology 50 2009.
- [4] Maninder Singh Rana, Bhupender Singh Sangwan, and Jitendra Singh Jangir (2012) Art of Hiding: An Introduction to Steganography, pp.11_12, International Journal of Engineering and Computer Science, India.
- [5] Rajashekarappa and Dr.KM Sunjiv Soyjaudah (2012) Comparative Cryptanalysis of Simplified-Data Encryption Standard Using Tabu Search and Simulated Annealing Methods, International Journal of Engineering Research and Development, Bangalore, e-ISSN: 2278-067X, p-ISSN : 2278-800X.
- [6] Vijay Kumar Sharma and Visual Shrivastava (2012) A Steganography Algorithm for Hiding Image In Image by Improved LSB Substitution by Minimize Detection, pp.3, Journal of Theoretical and Applied Information Technology, India, ISSN: 1992-8645, E-ISSN: 1817-3195
<http://www.jatit.org>