Two Level Security in Delivering Message Using Encryption and Steganography Techniques

Nadzirah Mohamad Zamri¹, Syed Muhammad Hazry Asraf¹a and Syed Zulkarnain Syed Idrus²b

¹Faculty of Information and Communication Technology, Universiti Teknikal Melaka Malaysia
²School of Human Development and Techno-communication, Universiti Malaysia Perlis

a hazrasyed@gmail.com; b syzul@unimap.edu.my;

Abstract. Data hiding is a process that secretly embedding information inside a data source without changing its original quality. Two popular techniques are steganography and cryptography [1]. Steganography is the art and science of hiding information by embedding messages into another image, audio or video [2]. Cryptography use mathematics to encrypt and decrypt data and transform plaintext into cipher text [3]. This study is about securing message by implementing the combination of steganography using Least Significant Bit (LSB) technique and cryptography using Vigenere cipher [4]. The methodology use is cyclic waterfall model. This model is simple and easy to understand. The phases also do not overlap with each other. The testing involves the process of embedding plaintext and cipher text into cover image. The results from the testing are the Mean Squared Error (MSE) and Peak Signal Noise Ratio (PSNR) value of the stego-image. The lower the MSE value and the higher the PSNR value is better image quality.

1. Introduction

In this Internet era, information hiding has received much attention as security of information has become a big concern to the users. Nowadays, there are many ways to secure the communication between sender and receiver. Two popular ways of sending vital information in a secret way are Cryptography and Steganography. Steganography and cryptography are the techniques to secure the messages, but both are using different concept. This research focuses on hiding secret message using steganography technique and encrypts the secret message using cryptography algorithm. Steganography is a Greek word which means the covered writing. Steganography can be classified into four types which are text, image, audio and video. Image Steganography is a popular technique used to hide data as it provides a safe and easy way to transmit information over the Internet [5]. The basic model of the steganography process using image format is illustrated in Figure 1.
Cryptography is the science of using mathematics to encrypt and decrypt data to keep messages secured by transforming intelligible data form (plaintext) into unintelligible form (cipher text). Cryptosystem consists of plaintext, encryption algorithm, decryption algorithm, cipher text and key. Plaintext is message or data which are readable. Encryption is the process of converting plaintext to cipher text by using key [6,7]. The results from encryption by applying the encryption key on the plaintext are called cipher text. Decryption is the process of retrieving the plaintext back from the cipher text. The key is used info to control the cryptosystem and it is only known by the sender and receiver only [8]. The basic model of the cryptographic process using image format is illustrated in Figure 2.

The combination of these two techniques is often achieving higher levels of security [9]. They complement each other's weaknesses. In cryptography the content of secret message is encrypted while in steganography the secret message is embedded into the cover medium. The model of the combination of Cryptography and Steganography is illustrated in Figure 3.
Finally, we can provide additional layer of security to the message by implementing cryptography along with steganography. The message will be encrypted first before being hidden into the medium.

Today's information world is a digital world. Data transmission over an unsecure channel is becoming a major issue of concern nowadays. In this type combination we simply do not hide simple text message. In Steganography, once the hidden message is detected, the message is become known. The use of only pure steganography to protect message during transmission expose that data to the attacker by using various steganalysis tools have been made for detecting the hidden message in steganography image make it no longer secured. Thus, the hidden message is not secured enough when just use pure steganography technique to secure the hidden information.

2. Methods and Analysis
Planning of this research combines two hiding techniques, which are steganography and cryptography. The secret messages will be converted into an encrypted format using a key and then this cipher text is hidden into an image. Research methodology also can be defined as the basic principles, processes and procedures involved in undertaking a study geared towards solving a identified problem. It focuses on the methods adopted in the collection and analysis of data. In steganography, Least Significant Bit (LSB) is the most popular technique that has been used to conceal the information [10]. Furthermore, Least Significant Bit (LSB) is the easiest way to secret information within the cover media. In this technique, the binary representations of the secret data have been taken and the LSB of each byte is overwritten within the image [11].

2.1. Steps of Least Significant Bits (LSB) Method
Supposing that we have three neighbouring pixels (nine bytes) with the following RGB encoding:

```
01101010 11110010 00110110
01101001 11110000 00110101
01100000 11101111 00110100
```

Now if we wish to embed the following 9 bits of compressed secret information:

```
010010011
``
If we insert these 9 bits over the LSB of the 9 bytes above, we get the following sequence of bits (where bits in red colour have been modified):

\[
\begin{align*}
01101010 & 11110110 00110110 \\
01101000 & 11110001 00110100 \\
01100000 & 11101111 00110101 \\
\end{align*}
\]

Note that we have successfully hidden 9 bits but at a cost of only modifying 5 of the LSB bits. Since the 9-bit requires five bytes to hide it in, the sixth byte of the three pixels can be used to begin hiding the next character of the hidden message.

2.1.1. Embedding Process
In this work, the secret message will be stored as stego-image resulting after hiding the secret message in the cover image. It has the following steps:

i. Read cover image
ii. Input hidden messages
iii. Output stego-image

Step 1: Read cover image.
Step 2: Extract the pixels of the cover image.
Step 3: Extract the character of the text message.
Step 4: Choose first pixel and place it in first component of pixel.
Step 5: Insert characters of secret message in each last component of the next pixels by replacing it.
Step 6: Repeat step 6 till all the characters has been embedded.
Step 7: Obtain stego-image

2.1.2. Data Extraction
i. Input stego-image
ii. Output secret text message

Step 1: Extract the pixel of the stego-image.
Step 2: Start from first pixel and extract characters from first component of the pixels.
Step 3: Go to next pixels and extract secret message characters from first component of the next pixels.
Step 4: Extract secret message.
2.2. Logical and Physical Design
The LSB method will be evaluated using MATLAB by using the following algorithm [12]. The secret message will be embedded into a cover image.

2.2.1. Embedding Algorithm
START
Input: Cover image, message image
Calculate the pixel of the cover image
Encode the secret message to binary code
Calculate the pixel that the message will used
Embed the secret message into the cover image
Output: Stego image
END

2.2.2. Embedding Algorithm
START
Input: STEGO-IMAGE
Decode binary code to message
Output: SECRET MESSAGE
END

2.3. Metric Measurement
Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) is the standard measurement to test the performance of stego image quality due to the hiding of message. The aim is to achieve higher value of PSNR that indicates a better reconstruction.

2.3.1. Mean Squared Error (MSE)
It is the most common estimation method used to check the fidelity of image. MSE is employ by PSNR to evaluate image quality. The lower the MSE value, the better the result by the following equation:

\[
MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (x(i,j) - y(i,j))^2
\]  

(1)
2.3.2. Peak Signal-To-Noise Ratio (PSNR)

PSNR is used to determine the ratio of the cover image quality before and after inserting the message, by the following equation:

\[
PSNR = 10 \log_{10} \left( \frac{2^r - 1}{\sqrt{MSE}} \right) = 10 \log_{10} \left( \frac{255^2}{MSE} \right)
\]

(2)

3. Testing

The purpose of testing is to ensure that the system running smoothly or vice versa. Besides that, it is also to know either the study has achieved their objectives or not. Therefore, the testing will be conducted from the sender side and receiver side. The result obtained will be analysed to view the testing outcome. In this study, the reading of peak to signal ratio (PSNR) value and mean square error (MSE) value are the prove of the simulation testing. The higher the PSNR and the lower the MSE values, the better the result is. The system testing covers testing activities and scope of the system. Proper planning is essential to avoid any disturbance during testing. In this test plan, test organization, test environment and test schedule will be determined.

There will be two parts of test. First is the steganography testing and next is the combination of steganography and cryptography testing [13]. The PSNR and MSE value from each test will be calculated and analysed.

In testing phase, the system simulation will be run by the tester which is the sender and receiver of the message. Developer need to know how the system works from the beginning until the end. Table 1 shows the detail about the requirement for the testing.

| Tester   | Hardware   | Software              |
|----------|------------|-----------------------|
| 1. Sender| 1. Laptop/PC| 1. MATLAB 2017a       |
| 2. Receiver|          | 2. Windows OS         |

Test environment is concerned about the configuration setup and the location that the testing will be conducted. The computer lab is the suitable place to carry out the testing smoothly and completely. Besides that, this study will used MATLAB software as the platform to test the system functionality. The MATLAB software needs to be installed first either in the Windows or MAC operating system.

This section describes on how the developer design the tests to be carried out in this study over a period of time. During the test process, if any simulation and technical error occur, the problem will be returned to the implementation phase. All the errors will be declared and solved. If the errors and problems cannot be solved, the issues are returned to implementation phase again. This process is a cyclic process until the simulation is successfully run on the system and produces the right output, as illustrated in Figure 5.

![Figure 5: Test process](image)
Simulation testing strategy is used in this study. In simulation testing, the program logic and code that implemented on the system will be examined. This study is mainly focused on using MATLAB R2017a. The main simulation of this study is to encrypt plaintext and embed it into the cover image. The MSE and PSNR value are calculated to make comparison between cover image and stego-image.

In test design, the details about testing will be discussed in test description while the data from testing need to be analysed. The testing part will involve the sender and receiver.

This test encrypts a secret message and covered the cipher text in a cover image. The PSNR and MSE value was obtained to determine the decomposition of image and data hiding between cover image and stego image.

All the results from the testing are called test data. The data collected will need to be analysed, namely: i) Cipher text; ii) Stego-image; iii) MSE value; and iv) PSNR value.

4. Results
Table 2 shows the result from hiding the secret message (plain text) into the cover image.

**Table 2: Testing results (i)**

| Steganography is a Greek word which means the covered writing | MSE     | PSNR     |
|-------------------------------------------------------------|---------|----------|
| Cryptography is the science of using mathematics to encrypt and decrypt data | 0.00    | 73.1566411 |
| In computer security, information hiding is a term about a process of embedding message inside digital media | 0.01    | 71.9751456 |
| Cryptography is a technique that convert plaintext into cipher text | 0.00    | 70.7099988 |
| computer security 123                                       | 0.00    | 76.0056861 |

Table 3 shows the result from the combination of cryptography and steganography.

**Table 3: Testing results (ii)**

| Steganography is a Greek word which means the covered writing | Cipher text | MSE     | PSNR     |
|-------------------------------------------------------------|-------------|---------|----------|
| Cryptography is the science of using mathematics to encrypt and decrypt data | JLMICDLVJSJHLDBZPOTRZVK GAXKGJWDBJZWSDDXETUQQ WXRVSAGHBSNJMZKDD | 0.00    | 72.4827495 |
| In computer security, information hiding is a term about a process of embedding message inside digital media | UBVVEDFTG BFKIXH WSWIKV KRXRGJFWFZREEJYPL VVFVEXTFUJBVVQYBYBWRWIIOTM | 0.01    | 68.0042506 |

| Cipher text | MSE     | PSNR     |
|-------------|---------|----------|
| FDIQCMLWJDYGRTFAKQDFKDCCK DTXOQDFXAVARMDBZIPTRLIXOQ YQGLLDGBFOCVWKKWDFQWXTETUDJ FZKVSDXWYCXBOAEKMDJGQAXZ LERBCBSAS | 0.01    | 70.4771503 |
Cryptography is a technique that converts plaintext into cipher text.

| Test                                 | MSE        | PSNR       |
|--------------------------------------|------------|------------|
| Plain text into the cover image      | 0.00       | 73.1566411 |
|                                      | 0.00       | 71.9751456 |
|                                      | 0.01       | 70.7099988 |
|                                      | 0.00       | 72.5403454 |
|                                      | 0.00       | 76.0056861 |
| Cipher text into the cover image     | 0.00       | 72.4827495 |
|                                      | 0.01       | 68.0042506 |
|                                      | 0.01       | 70.4771503 |
|                                      | 0.00       | 72.3509788 |
|                                      | 0.00       | 75.4191155 |

From the result, the stego-image containing plain text has low MSE and higher PSNR value compared to stego-image containing cipher text. The higher the PSNR value, the better the quality because the ratio of signal to noise is higher. The 'signal' indicates the original image and the 'noise' is the error in reconstruction. Hence, the quality of the stego-image is slightly degraded with the embedded cipher text compared to plain text.

5. Conclusion and Perspectives

This study reviews on existing steganography and cryptography approach. Security element based on steganography and cryptography has been performed to protect the secret message. The secret message is hidden across the least significant bits (LSB) of the cover image. The resulting MSE and PSNR values are satisfactory and show that the image quality is preserved at a good level. Lastly, our contribution of this study is to modify an existing steganography by implementing cryptography approach to protect the secret message against unauthorized attack that can cause information leakage during transmission.

However, this study can further be improved with the design of an attractive and easy interface to make the users feel comfortable using this system. It also can be more flexible by allowing users to use their own image as the cover image to be used.
References

[1] Saleh, Marwa E. 2016. “Data Security Using Cryptography and Steganography Techniques.” 7(6): 390–97. 8.

[2] Rahmani, Md. Khalid Imam, Kamiya Arora, and Naina Pal. 2014. “A CryptoSteganography : A Survey.” (IJACSA) International Journal of Advanced Computer Science and Applications 5(7): 149–55. 2.

[3] Shukla, Chandra Prakash, Ramneet S Chadha, and Abhishek Kumar. 2014. “Enhance Security in Steganography with Cryptography.” 3(3): 5696–99. 3.

[4] Atee, Hayfaa Abdulzahra, Robiah Ahmad, and Norliza Mohd Noor. 2015. “Cryptography and Image Steganography Using Dynamic Encryption on LSB and Color Image Based Data Hiding Foundation of Technical Education, Baghdad, Iraq.” 23(7): 1450–60. 4.

[5] Anjali A. Shejul, Prof. U. L. Kulkarni, “A DWT based Approach for Steganography using Biometric”, International Conference On Data Storage and Data Engineering, IEEE, pp. 39-43, 2010. 5.

[6] Idrus, S. Z. S., Aljunid, S. A., Asi, S. M., Sudin, S., & Ahmad, R. B. (2008). Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers,”. IJCSNS International Journal of Computer Science and Network Security, 8(1), 20-25.

[7] SZS Idrus, SA Aljunid, SM Asi, S Sudin (2012). Performance Evaluation of Encryption Algorithms’ Key Length Size on Web Browsers. IJCSNS International Journal of Computer Science and Network Security, 12(5). 10.

[8] Idrus, S. Z. S. (2007). Database encryption for a Web-based Claims System.

[9] Al-otaibi, Nouf A. 2014. “2-Layer Security System for Hiding Sensitive Text Data on Personal Computers.” 2(2): 151–57. 7.

[10] Engineering, Instrumentation. 2013. “A REVIEW ON STEGANOGRAPHY.” : 4635–38.6. “Least Significant Bit Steganography Technique for Hiding Compressed Encrypted Data Using.” 2017. 76(10): 12205–31. 6.

[11] Kamdar, Naitik P, Dipesh G Kamdar, and Dharmesh N.khandar. 2013. “Performance Evaluation of LSB Based Steganography for Optimization of PSNR and MSE.” Journal of Information, Knowledge and Research in Electronics and Communication Engineering 2(2): 505–9.

[12] Saputra, Imam, Nelly Astuti Hasibuan, and Robbi Rahim. 2017. “Vigenere Cipher Algorithm with Grayscale Image Key Generator for Secure Text File.” (January).

[13] Manoj, I. Venkata Sai. 2010. “Cryptography and Steganography.” International Journal of Computer Applications 1(12): 63–68. http://www.ijcaonline.org/journal/number12/pxc387414.pdf. 9.