Message Security Implementation by Using a Combination of Hill Cipher Method and Pixel Value Differencing Method in Mozilla Thunderbird Email Client

B Siregar¹, H Gunawan¹, MA Budiman², Sulindawaty³

¹Dept. of Information Technology, Faculty of Computer Science and Information Technology, Universitas Sumatera Utara
²Dept. of Computer Science, Faculty of Computer Science and Information Technology, Universitas Sumatera Utara
³STMIK Pelita Nusantara

E-mail: baihaqi@usu.ac.id

Abstract. One of the problems in this field of communication is the insecurity of messages sent across computer networks. Even though sometimes the contents of a message can be something that is sensitive and prone to abuse. One method that can be used to overcome this problem is by using a combination of cryptography and steganography. In this research, an add-on menu for Mozilla application was developed to secure messages to be sent via e-mail using Hill Cipher's cryptographic method on messages and insert them using steganographic pixel value differencing method on image files to be extracted and returned to the form originally. The results of this study indicate that with experiments using messages with length and image file extensions that are also different, namely .bmp, .jpg, .png, and .gif can insert the initial message into the image file and be returned to its original form with a maximum length limit message 1000 characters and no manipulation of the image file from the insertion message.

1. Introduction
Along with developments in the computer field, the amount of communication made between networks has increased rapidly throughout the world, including e-mail which is generally used as one of the message delivery media. One of the problems in this communication field is the security of messages sent across computer networks. Even though sometimes the contents of a message can be something that is sensitive and prone to abuse. To prevent this, there are two ways you can do to increase the security of messages sent. First, using cryptography, the randomization of messages so that they appear to have no meaning and randomness. However, this has the disadvantage that the encrypted message can still be decrypted to return the message to its original form. To cover these weaknesses the second method is used, namely steganography. Steganography is a way to hide a message into computer files, for example image, sound or text files.

In this research, we combine both methods, namely cryptography and steganography so that the message will have double protection. First, the message will be encrypted using the Hill cipher method. This method was chosen because it is a simple method using polygraph substitution. Hill cipher was developed by Hill [1]. Second, after the message is encrypted, there is still the possibility...
of decryption of the message, then the author will use steganography to hide the encrypted message into the image file .bmp, .jpg, .png, and .gif. We chose this extension because the image file is a type of file that is commonly used in steganography techniques. The method we use is the pixel value differencing method. This method is a new steganography method developed to replace the least significant byte (LSB) method that has been commonly used before [2].

One message delivery media that is widely used today is sending messages via email. E-mail media makes sending messages short and precise. However, this media is vulnerable to theft attacks on the content of messages sent, even though sometimes the contents of messages sent are sensitive and personal. One method used to secure the sending of messages is by cryptography, but this method has a weakness in the attack of returning messages that have been scrambled to their original form such as brute-force attack. Another method is by steganography, but this method has a disadvantage to the possibility of extracting hidden messages that are not random. In this study the authors combine the two methods, namely cryptography and steganography so that the security of messages increases in a double. The cryptographic method used is Hill cipher method, while the steganography method used is the pixel value differencing method.

Research on securing this message has been pretty much made by previous researchers, both using cryptographic methods or steganography methods. Lee and Chen implemented the steganography method into image files using an affine transformation technique [3]. Panigrahy, et. al. performed message encryption techniques on images using self-invertible key matrix [4]. This method is based on the Hill cipher algorithm. Syahrul implements the least significant byte steganography algorithm in image files [5]. The least significant byte method is one method commonly used in steganography.

2. Material and Method

There are two methods used in this study, namely cryptography and steganography. The cryptographic method used is Hill cipher method. This method detects the message length to be scrambled within the 1000 characters limit. If the message length is within the boundary range, it will randomize messages per character by using the specified matrix and key. After the message is scrambled, the user can choose the image file to insert the scrambled message. Extensions that can be inserted are .bmp, .jpg, .png, and .gif. After the image is selected, it will do the method of steganography pixel value differencing to insert a message in the picture. After the process is complete, the output will be in the form of an image file that has been inserted an encrypted message to be stored by the user and sent via email. After the image file is received by the second user, the message extraction process from the selected image file will be carried out. After the encrypted message is extracted, the decryption process will be carried out to return the message to its original form. The flow of the system process can be seen in the general architecture in Figure 1.

![General Architecture](image-url)

**Figure 1. General Architecture**
2.1. Message Encryption Stages
At this stage the system takes input messages from users. The message security system with the Hill cipher encryption process limits the message input in the form of ASCII characters from 32 to 126, bringing the total number to 95 characters. So, with a manual calculation, the character ‘a’ with ASCII code 97 becomes 65 because it is reduced by 32. With the example of using a key in the form of a 3x3 matrix \([1 \ 1 \ 2 \ 2 \ 1 \ 1 \ 1 \ 1 \ 1]\), the process of encrypting ‘aaa’ messages becomes Equation 1.

\[
\begin{pmatrix}
1 & 1 & 2 \\
2 & 1 & 1 \\
1 & 1 & 1
\end{pmatrix}
\begin{pmatrix}
65 \\
65 \\
65
\end{pmatrix}
= \begin{pmatrix}
260 \\
260 \\
195
\end{pmatrix} \equiv \begin{pmatrix}
70 \\
70 \\
5
\end{pmatrix} \pmod{95}
\]

Equation 1

Because the message input is limited to the ASCII character to 32, the encryption results are added 32 again so that (70 70 5) becomes (102 102 37) which after being translated to ASCII characters becomes ‘ff%’.

2.2. Message Insert Stage
At this stage the system will retrieve encrypted messages to be inserted into the image file with the extension .bmp, .jpg, .png, or .gif that the user has selected. The steganography method used is the pixel value differencing method. First of all, the selected image file will be converted into canvas so that the system can access to the image pixels. The system then selects pixels from the canvas randomly and starts inserting the message length and message characters one by one.

2.3. Stages Showing Images Containing Messages
At this stage after all the messages have been inserted, the system converts the canvas back to the image file. The system then displays the image file that the message has been inserted for the user to save and sent via email.

2.4. Extract stage
At this stage the system will access the selected image file to detect whether there is a message inserted. If there are, the system will start by reading the message length and then the messages that have been inserted one by one until it is complete.

2.5. Message Decryption Stages
At this stage, after the extraction process produces an encrypted message, the next step is to return the message to the original form using the decryption method. In this example an encrypted message that is ‘ff%’ is changed to the ASCII code to (102 102 37). Due to the limitation of ASCII characters by the system from the code character to 32, a reduction of 32 becomes (70 70 5). The decryption process of the message is done by inversing the key matrix \([1 \ 1 \ 2 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1]\) that was used, namely \([0 \ 1 \ -1 \ 1 \ 1 \ 4 \ 1 \ 0 \ -1]\). So, the decryption process of the message "ff%" becomes Equation 2.

\[
\begin{pmatrix}
0 & 1 & -1 \\
1 & 1 & 4 \\
1 & 0 & -1
\end{pmatrix}
\begin{pmatrix}
70 \\
70 \\
5
\end{pmatrix}
= \begin{pmatrix}
65 \\
160 \\
65
\end{pmatrix} \equiv \begin{pmatrix}
65 \\
65 \\
65
\end{pmatrix} \pmod{95}
\]

Equation 2

The results obtained are added 32 again so that it becomes (97 97 97) which after being translated according to the ASCII code becomes ‘aaa’, back as the initial message.
3. Result and Discussion
The results of the system design that has been built are as follows:

3.1. Message Insertion Menu Display
The message insertion menu display is one of the pages that appear when the application is run. In the design of the message insertion menu display there is a message column, encryption key, message that has been encrypted, and a button to select the image file to be inserted a message. The message insertion menu display can be seen in Figure 2 while the message insertion menu display after the insertion process to the picture can be seen in Figure 3.

![Figure 2. Display of message insertion menu.](image2)
![Figure 3. Display of message after insertion process to image.](image3)

3.2. Message Retrieval Menu Display
The message retrieval menu display is one page that appears when the application is run. In the design of the message retrieval menu, there is a button to select the image file to be extracted, the extraction message column, the decryption key and the decrypted message. The message retrieval menu after the message extraction process from the image can be seen in Figure 4 while the message retrieval menu after the message extraction process can be seen in Figure 5.

![Figure 4. Display of message retrieval menu after the message extraction process from the image.](image4)
![Figure 5. Display of retrieval menu message after message decryption process.](image5)
3.3. Message Retrieval Menu Display

Application testing is done to ensure that all functions in the application run as desired. The following shows the results of testing the message security process. To get accurate research results, the author conducted a test as much as one time using different length messages, image files, and image file extensions. The following is shown the results of testing the message security process and its return to its original form is shown in Table 1.

| No. | Message                                      | Length (char) | Image Dimension (pixel) | File Type | Result |
|-----|----------------------------------------------|---------------|-------------------------|-----------|--------|
| 1   | aaa                                          | 3             | 177x177                 | .bmp      | Succeed |
| 2   | Apa kabar                                    | 9             | 498x419                 | .jpg      | Succeed |
| 3   | AYO JUMPA BESOK SIANG                       | 21            | 1200x1109               | .png      | Succeed |
| 4   | buang sampah pada tempatnya                  | 27            | 1300x1065               | .gif      | Succeed |
| 5   | Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas porttitor congue massa. | 90            | 1920x1200               | .jpg      | Succeed |

In the process of testing the message security results obtained that the application can encrypt, hide messages in the image file. Bmp, .jpg, .png, and .gif and decrypt the message to its original form. The testing process is carried out with a range of characters in the message up to 90 characters and the dimensions of the image file up to 1920x1200 pixels. During the five tests, the encryption and decryption process of the message was successfully carried out. In the program created, the maximum message length is 1000 characters. The testing process by inserting 720 characters messages was successfully carried out with an additional time of three seconds in the message insertion and extraction process, while the speed of the encryption and decryption process did not change. Testing is also done by trying to manipulate the image file from the insertion of the message and see if the inserted message is not damaged. The test results can be seen in Table 2.
Table 2. Image manipulation test result.

| No. | Message                  | Length (char) | Image Dimension (pixel) | Type of Manipulation | Result |
|-----|--------------------------|---------------|-------------------------|----------------------|--------|
| 1   | buang sampah pada tempatnya | 21            | 419x498                 | Rotate               | Failed |
| 2   | buang sampah pada tempatnya | 21            | 498x419                 | Flip                 | Failed |
| 3   | buang sampah pada tempatnya | 21            | 287x226                 | Crop                 | Failed |
| 4   | buang sampah pada tempatnya | 21            | 249x210                 | Resize               | Failed |
| 5   | buang sampah pada tempatnya | 21            | 498x419                 | Brightness           | Failed |

4. Conclusion
The conclusions that can be taken from making this add on Mozilla Thunderbird are as follows:
- This application add on can encrypt messages using encryption using Hill cipher and hide it into a .bmp, .jpg, .png, and .gif image file to send by e-mail;
- This application add on can re-extract and return the message to the original text form with a limit of under 1000 characters;
- This application add on cannot return messages if manipulation is done in the form of rotate, flip, crop, resize and brightness in image files containing messages.

References

[1] L. S. Hill, "Cryptography in An Algebraic Alphabet," The American Mathematical Monthly, vol. 36, no. 6, pp. 306-312, 1929.
[2] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang, "Image Steganographic Scheme Based on Pixel-value Differencing and LSB Replacement Methods," in IEEE Proceedings - Vision, Image and Signal Processing, 2005.
[3] Y.-K. Lee and L.-H. Chen, "Object-Based Image Steganography Using Affine Transformation," International Journal of Pattern Recognition and Artificial Intelligence, vol. 16, no. 06, pp. 681-696, 2002.
[4] S. Panigrahy, B. Acharya and D. Jena, "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm," in International Conference on Advances in Computing, Chikli, 2008.
[5] Syahrul, "Aplikasi Pengamanan Informasi dengan Teknik Penyisipan Data Menggunakan Algoritma Steganografi Least Significant Byte," STMIK AMIKOM, Yogyakarta, 2012.