Pixel image steganography using EOF method and modular multiplication block cipher algorithm

Robbi Rahim 1*, Darmawan Napitupulu 2, Heri Nurdiyanto 3, Usti Fatimah Sari 4, Firahmi Rizky 5, Dicky Nofriansyah 5, Oris Krianto Sulaiman 6, Abdurrozzaq Hasibuan 7, R Ratnadewi 8, Mohamad Ihwani 9

1 School of Computer and Communication Engineering, Universiti Malaysia Perlis, Kubang Gajah, Malaysia
2 Research Center for Quality System and Testing Technology, Indonesian Institute of Sciences, Jakarta, Indonesia
3 Department of Informatics, STMIK Dharma Wacana, Metro Lampung, Indonesia
4 Department of Computer System, STMIK Triguna Dharma, Medan, Indonesia
5 Department of Information System, STMIK Triguna Dharma, Medan, Indonesia
6 Department of Informatics Engineering, Universitas Islam Sumatera Utara, Medan, Indonesia
7 Department of Industry Engineering, Universitas Islam Sumatera Utara, Medan,
8 Electrical Engineering, Universitas Kristen Maranatha, Bandung, Indonesia
9 Universitas Negeri Medan, Medan, Indonesia

*usurobbi85@zoho.com

Abstract. This study aims to hide data or information on pixel image using EOF method and to improve the security of hidden data than combine with cryptography algorithm Modular Multiplication Block Cipher algorithm for the encryption process. The image file used as the test sample consists of 3 types of image types (JPG, BMP, PNG), this file type is the most widely used by users with different width and height as well as various file sizes. The results of this study prove that the data could embed in pixel image using EOF method and the file size of carrier will increase its capacity as byte of embedded text.

1. Introduction

The era of information as it is today, data or information that is important and secret has become a precious asset [1]–[5]. Such valuable data or information will undoubtedly pose a risk if it can be freely accessed by unauthorized parties [6]–[8]. Therefore, how data to be secure needs particular attention [9], [10].

One way to avoid crime against a data is to hide data from other media such as image [11], [12], this technique is called steganography technique[13], [14]. Steganography is the science and art of hiding messages within other media so that the existence of messages cannot be known [13], [15]. One of steganography method that is simple and easy to implement is End Of File (EOF) method. The weakness of the EOF method is the secret messages can be easily extract using EOF method as well [16]. An improvement of embedded messages is necessary like using cryptography algorithm [16], one of an algorithm that can be used is Modular Multiplication Block Cipher [2], in this research Modular Multiplication Block Cipher (MMBC) are combined with EoF method for additional security, research related to MMBC algorithm as text message security have been done some researchers like Rahim(2016)[2],
[17]. [18] and Sahu(2011)[19]where the results of this study indicate that the cipher text result of MMBC algorithm is very strong and can be combined with many algorithms

This research tries to combine Modular Multiplication Block Cipher with EOF method for securing embedded message in the pixel image, this combination is expected to secure data or messages better than third party cryptanalysis and also takes a long time to attack with a brute force attack.

2. Methodology

The EOF method can insert the messages in image pixels or at the end of a byte of an image, this research focuses on embedded ciphertext result from encryption using Modular Multiplication Block Cipher in image pixels, see figure 1 below for the combination process.

![Figure 1. Combination Process of Security Message](image)

Based on figure 1 above, the first step is encryption using Modular Multiplication Block Cipher (MMB) algorithm to produce cipher text, and next process cipher text will be inserted into the end of pixel image by giving the identifier before and after the embedded (cipher text) message, and for decryption also vice versa.

| Encryption Function | Decryption Function |
|---------------------|---------------------|
| for i = 0 to 3      | f(x_0,x_1,x_2,x_3)  |
| x_i = x_i XOR k_i   | for i = 0 to 3      |
| next i              | x_i = x_i XOR k_{i+2} |
| f(x_0,x_1,x_2,x_3)  | for i = 0 to 3      |
| for i = 0 to 3      | f(x_0,x_1,x_2,x_3)  |
| x_i = x_i XOR k_{i+1} | next i            |
| next i              | f(x_0,x_1,x_2,x_3)  |
| for i = 0 to 3      | f(x_0,x_1,x_2,x_3)  |
\[ x_i = x_i \text{ XOR } k_{i+2} \quad \text{for } i = 0 \text{ to } 3 \]
\[ \text{next } i \]
\[ f(x_0, x_1, x_2, x_3) \quad \text{next } i \]

Block diagram process of the algorithm Modular Multiplication Block Cipher on encryption and decryption[2] can be seen in Figure 2.

**Figure 2.** Process Encryption and Decryption Modular Multiplication Block Cipher

Analyzing combination of EOF method and algorithm of Modular Multiplication Block Cipher can see in the following example:

A. Encryption and EOF Process

1. Plaintext and Key
   - Key = micomsisthebest.
   - Plaintext = ConferenceMICOMS
   
The size of the image that is used to hide the message has Width and Height 300x157 (see Figure 3) with image size 17 KB, and also a 16-byte message length as an example of data to be hidden.

2. Modular Multiplication Block Cipher Process
   
The encryption process using the MMBC algorithm according to figure 1 as follows:
   
   \[ X(0) = X(0) \text{ XOR } K(0) \]
   
   \[ = 01000011011011110110111001100110 \text{ XOR } 0110110110110100100110011011111 \]
   
   \[ = 001011100000110100001101000010001 \]
   
   \[ X(1) = X(1) \text{ XOR } K(1) \]
   
   \[ = 011001110110110100110111011101110 \text{ XOR } 0110110110110110110011001111 \]
   
   \[ = 000011001100000001100000110100001110 \]
   
   \[ X(2) = X(2) \text{ XOR } K(2) \]
   
   \[ = 01100101100111010001101101100100000001101000011110 \text{ XOR } 01101100011011000110100010000110 \]
The above process is part of the process of MMBC and the end result of the MMBC process can be cipher text = -0¶Ô1'4ÁÍŠ• ]c

3. Steganography Embedded Process

Cipher text = -0¶Ô1'4ÁÍŠ• ]c, this cipher text converted into decimal form before embedded in pixels image and obtain 45 111 194 182 195 148 11 49 7 39 52 195 130 26 195 143 197 160 127 93 99, figure 3 is the images that were used as media to cover message with end of a pixel value as follows:

![Figure 3. Image and Pixel Value](image)

Ciphertext decimal will be embedded at the end of RGB pixel in the image and give parity "ï" at the beginning of ciphertext that has a decimal value of "255", and the result as figure 4.

![Figure 4. Pixel Image after Embedded using EOF Method](image)

B. Decryption and Extraction

Decryption and extraction process is not much different from encryption and embedded process, here is step process:
1. The first step is to execute the message extraction \(m\) process by reading parity "\(\ddot{y}\)", where the hex value between the parity is a hidden message.

2. \(m\) which contains the hexa value and then converted back into ASCII form to be decrypted by using the MMBC algorithm with the following process:

   CipherText= -off\(14\)A\(1\)S\(1\)c

   binary:
   00101101101111110110110110111010000001101001100011101011001111000011101101100110
   0001000011010101110111110001101011000111110110111011011100

   \[X(3) = X(2) \oplus X(3) \oplus X(0)\]
   \[= 00110100110001100001110110110100011110100011010100\]

   \[X(2) = X(1) \oplus X(2) \oplus X(3)\]
   \[= 0001011110110100100011110001111111010110010000111101011100\]

   \[X(1) = X(0) \oplus X(1) \oplus X(2)\]
   \[= 00111000110011101000111111111011100100001111111101111000\]

   \[X(0) = X(3) \oplus X(0) \oplus X(1)\]
   \[= 00111000110011101000111111111011100100001111111101111000\]

   If \(\text{LSB}(X(0)) = \text{LSB}(00110100110001100001110110110100011110100011010100) = 1 \Rightarrow \text{TRUE}\)

   \[X(0) = X(0) \oplus C\]
   \[= 00111000110011101000111111111011100100001111111101111000\]

   If \(\text{LSB}(X(3)) = \text{LSB}(100101001101100011101011100011111000111110001) = 0 \Rightarrow \text{TRUE}\)

   \[X(3) = X(3) \oplus C\]

The above process is part of the whole process of decryption process using MMBC algorithm, the final plaintext = Conference MICOMS.

3. Result and Discussion

The experiment of steganography process with different message lengths are performed on three types of image files (JPG, BMP, PNG), the result can be seen in table 2.

### Table 2. Security Message Experiment

| No | File Name    | Original Size (Byte) | Message Length (Byte) | Result Size (Byte) |
|----|--------------|----------------------|-----------------------|-------------------|
| 1  | Kripto.jpg   | 61,302 byte          | 30                    | 61,332            |
| 2  | Stegano.png  | 48,789 byte          | 45                    | 48,834            |
| 3  | House.bmp    | 81,120 byte          | 30                    | 81,150            |
| 4  | Dragon.jpg   | 50,871 byte          | 26                    | 50,897            |
| 5  | Smartphone.png | 45,620 byte      | 100                   | 46,620            |
Steganography with EOF method and Modular Multiplication Block Cipher algorithm can be accomplished well, based on table 2 above seen embedded process can be done on media carrier and significantly will increase the original size of file. The experimental results are only done on small data messages and if perform on large data then the file size also bigger than the original file.

4. Conclusion
Combinations Eof and Modular Multiplication Block Cipher can be done well and the messages can hide in the pixel image. An experiment showing that the carried file size will increase by the number of bytes from text and of course it is not good because it makes the file size bigger, in the future development it can be tried to combine with text compression algorithm on the message before inserted.

References

[1] Hariyanto E and Rahim R, Oct. 2016 Arnold’s Cat Map Algorithm in Digital Image Encryption Int. J. Sci. Res.5, 10 p. 1363–1365.
[2] Rahim R and Ikhwan A, 2016 Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher Int. J. Sci. Res. Sci. Technol.2, 6 p. 71–78.
[3] Rahim R, 2017 Man-in-the-middle-attack prevention using interlock protocol method ARPN J. Eng. Appl. Sci.12, 22 p. 6483–6487.
[4] Rahim R Hartama D Nurdiyanto H Ahmar A S Abdullah D and Napitupulu D, 2018 Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm J. Phys. Conf. Ser.954, 1 p. 12008.
[5] Kartikadarma E Listyorini T and Rahim R, 2018 An Android mobile RC4 simulation for education World Trans. Eng. Technol. Educ.16, 1 p. 75–79.
[6] Putera A Siahaan U and Rahim R, Aug. 2016 Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm Int. J. Secur. Its Appl.10, 8 p. 173–180.
[7] Rahim R Dahria M Syahril M and Anwar B, 2017 Combination of the Blowfish and Lempel-Ziv-Welch algorithms for text compression World Trans. Eng. Technol. Educ.15, 3 p. 292–297.
[8] Nurdiyanto H Rahim R and Wulan N, Dec. 2017 Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement J. Phys. Conf. Ser.930, 1 p. 12005.
[9] Arvin S. Lat J Xavier R. Bondoc R and Atienza K C V., 2013 SOUL System: secure online USB login system Inf. Manag. Comput. Secur.21, 2 p. 102–109.
[10] xiaojuan M, 2017 Research and Implementation of Computer Data Security Management System Proceedia Eng.174 p. 1371–1379.
[11] Champakamala B S Padmini K Professors R D K A and Bosco D, 2014 Least Significant Bit algorithm for image steganography Overview of Steganography Int. J. Adv. Comput. Technol.3, 4 p. 5.
[12] Sethi P and Kapoor V, 2016 A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography in Procedia Computer Science87 p. 61–66.
[13] Nurdiyanto H and Rahim R, 2017 Enhanced pixel value differencing steganography with government standard algorithm in 2017 3rd International Conference on Science in Information Technology (ICSITech) p. 366–371.
[14] Rahim R et al., Apr. 2018 Combination Base64 Algorithm and EOF Technique for Steganography J. Phys. Conf. Ser.1007, 1 p. 12003.

[15] Bhardwaj R and Sharma V, 2016 Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution in Procedia Computer Science93 p. 832–838.

[16] Iswahyudi C Setyaningsih E and Widyastuti N, 2012 Pengamanan kunci enkripsi citra pada algoritma super enkripsi menggunakan metode end of file Pros. Semin. Nas. Apl. Sains Teknol. Periode III November p. 278–285.

[17] Rahim R Winata H Zulkarnain I and Jaya H, Dec. 2017 Prime Number: an Experiment Rabin-Miller and Fast Exponentiation J. Phys. Conf. Ser.930, 1 p. 12032.

[18] Abdullah D Rahim R Apdilah D Efendi S Tulus T and Suwilo S, 2018 Prime Numbers Comparison using Sieve of Eratosthenes and Sieve of Sundaram Algorithm in Journal of Physics: Conference Series978, 1 p. 12123.

[19] Sahu S K and Pradhan M, 2011 Implementation of modular multiplication for RSA algorithm in Proceedings - 2011 International Conference on Communication Systems and Network Technologies, CSNT 2011 p. 112–114.