Pixel Image Steganography Using EOF Method and Modular Multiplication Block Cipher Algorithm

Robbi Rahim

Abstract
Purpose- This study aims to hide data or information on pixel image by using EOF method, and to improve the security of hidden data is performed by using Modular Multiplication Block Cipher algorithm for encryption process.
Design/Methodology/Research- 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.
Findings- The results of this study prove that the data can be embedded in the pixel of image using EOF method after encryption process are perform, and also all embedded data can also be extracted and read well without any restrictions, pixel image also back to original form before steganography processed.
Originality/Value- This is the first combination of EOF method and the Algorithm of Modular Multiplication Block Cipher in data masking in pixel image.

Keywords Data Hiding, Steganography, Cryptography, Combination Technique, Image Steganography

Paper Type Research Paper

1. Introduction

The era of information as it is today, data or information that is important and secret has become a very valuable asset (Rahim, 2017a, 2017b, Rahim and Ikhwan, 2016a, 2016b). Such valuable data or information will certainly pose a risk if it can be freely accessed by unauthorized parties (Putera et al., 2016; Rahim et al., 2017). Therefore, how data to protect need a special attention (Arvin S. Lat et al., 2013; xiaojuan, 2017).

One way to avoid crime against a data is to hide data into other media such as image (Champakamala et al., 2014; Rachmawati et al., 2017; Sethi and Kapoor, 2016), this technique is called steganography technique. Steganography is the science and art of hiding messages within other media so that the existence of messages cannot be known (Bhardwaj and Sharma, 2016; Rachmawati et al., 2017; Wandani et al., 2012). One of steganography method that is simple and easy to implement is End Of File (EOF) method (Wandani et al., 2012). The weakness of the EOF method is that secret messages can be easily extract using EOF method as well and easy to read (Iswahyudi et al., 2012), to improve the security of embedded messages it is necessary to add another security that is cryptographic algorithm, this research used Modular Multiplication Block Cipher (Rahim and Ikhwan, 2016b) for additional security.

This research combines the process of Encryption of Modular Multiplication Block Cipher algorithm with EOF method as the process of embedded data or message on image

pixel, embedded message in pixel will make a distortion in pixel as if the image is damaged due to faulty retrieval or unfinished data transmission process (Liśkiewicz et al., 2017), the distortion in image is the message itself and to read the message must use the EOF method and Modular Multiplication Block Cipher algorithm with specific keys.

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 messages in image pixels. The message is a cipher text of the encryption process using the algorithm of Modular Multiplication Block Cipher, see figure 1 below for the combination are perform.

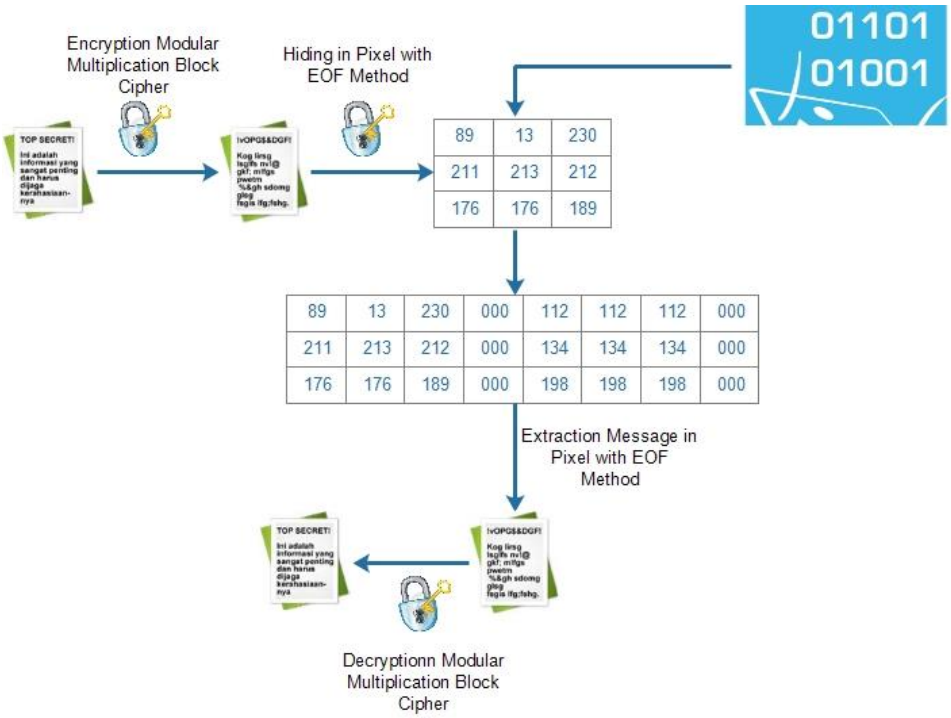

Figure. 1. Combination Process Modular Multiplication Block Cipher and EOF Method

Based on figure 1 above, first step are encrypting using Modular Multiplication Block Cipher (MMB) algorithm, and the cipher text insert into the end of the pixel image by giving the identifier before and after the embedded message, and for decryption also vice versa.

Block diagram process of the algorithm Modular Multiplication Block Cipher on encryption and decryption(Rahim and Ikhwan, 2016b) can be seen in Figure 2.

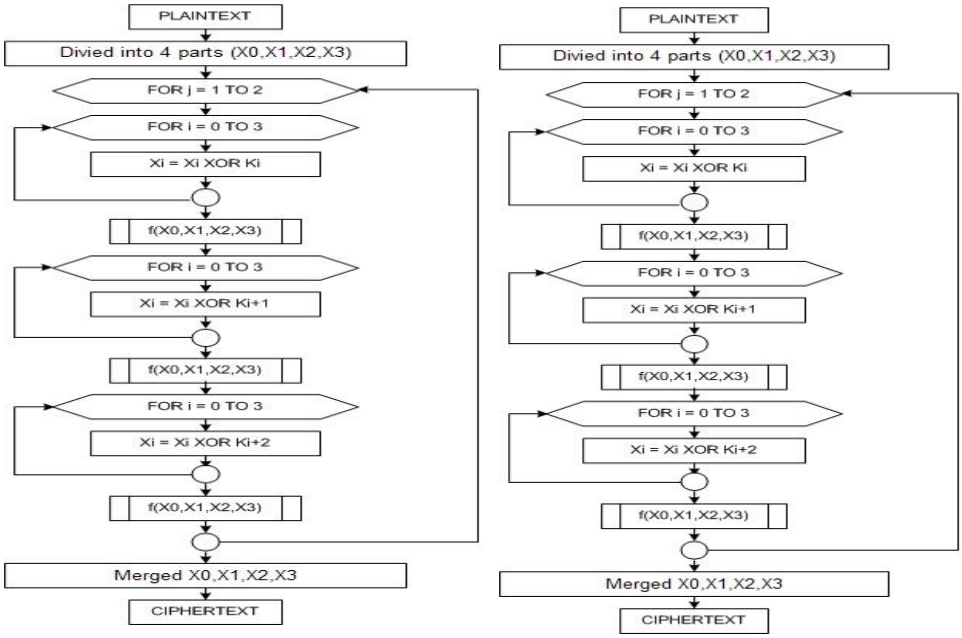

Figure. 2. Process Encryption and Decryption Modular Multiplication Block Cipher

Analyzing combination of EOF method and algorithm of Modular Multiplication Block Cipher can see in the following example:
Key = micomsisthebest.
Plaintext= ConferenceMICOMS
Encryption process by using key and plaintext will obtain ciphertext = -o¶Ô 1'4ÂÏŠ •]c, this ciphertext result converted into decimal form to be insert in pixels image, decimal value obtained from conversion = 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 are used as media to insert the message with end of pixel value as follows:.

103	84	87
109	88	99
178	131	154
127	230	81
78	78	80
111	87	105
156	32	88
98	90	88
90	92	71

Figure. 3. Image and Pixel Value

Pixel RGB in image will be inserted ciphertext "45 111 194 182 195 148 11 49 7 39 52 195 130 26 195 143 197 160 127 93 99". Ciphertext decimal will be added as the final value in the RGB image pixel. At the beginning and end of the ciphertext is given a "ÿ" marker character that has a decimal value of "255", and the result as figure 5.

103	84	87
109	88	99
178	131	154
127	230	81
78	78	80
111	87	105
156	32	88
98	90	88
90	92	71
255	45	111
194	182	195
148	11	49
7	39	52
195	130	26
195	143	197
160	127	93
99	255	255

Figure. 4. Pixel Image after Embedded using EOF Method

The result of the matrix is mapped as RGB image and this image is called the stego image.

3. Results and Discussion

Testing of message insertion with different message lengths is done on 3 types of image files (JPG, BMP, PNG), the result can be seen in table 1.

Table 1. Experiment Result

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 done well, and the stego image will have noise at the end of pixel image like damaged image.

4. Conclusion

Combinations can be done well and messages can be hidden in pixel image, improvisation could be perform in this combination process is the result decimal value can be modified to close the value of neighboring pixel RGB so the distortion pixel is not too visible and minimize suspicion for others.

References

Arvin S. Lat, J., Xavier R. Bondoc, R. and Atienza, K.C. V. (2013), "SOUL System: secure online USB login system", *Information Management & Computer Security*, Vol. 21 No. 2, pp. 102–109.

Bhardwaj, R. and Sharma, V. (2016), "Image Steganography Based on Complemented

Message and Inverted Bit LSB Substitution", *Procedia Computer Science*, Vol. 93, pp. 832–838.
Champakamala, B.S., Padmini, K., Professors, R.D.K.A. and Bosco, D. (2014), "Least Significant Bit algorithm for image steganography Overview of Steganography", *International Journal of Advanced Computer Technology*, Vol. 3 No. 4, p. 5.
Iswahyudi, C., Setyaningsih, E. and Widyastuti, N. (2012), "Pengamanan kunci enkripsi citra pada algoritma super enkripsi menggunakan metode end of file", *Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) Periode III*, No. November, pp. 278–285.
Liśkiewicz, M., Reischuk, R. and Wölfel, U. (2017), "Security levels in steganography – Insecurity does not imply detectability", *Theoretical Computer Science*, Vol. 692, pp. 25–45.
Putera, A., Siahaan, U. and Rahim, R. (2016), "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm", *International Journal of Security and Its Applications*, Vol. 10 No. 8, pp. 173–180.
Rachmawati, D., Amalia, A. and Surya, J. (2017), "Combination of Huffman Coding Compression Algorithm and Least Significant Bit Method for Image Hiding", *Journal of Physics: Conference Series*, Vol. 801, available at:https://doi.org/10.1088/1742-6596/801/1/012059.
Rahim, R. (2017a), "128 Bit Hash of Variable Length in Short Message Service Security", *International Journal of Security and Its Applications*, Vol. 11 No. 1, pp. 45–58.
Rahim, R. (2017b), "Man-in-the-middle-attack prevention using interlock protocol method", *ARPN Journal of Engineering and Applied Sciences*, Vol. 12 No. 22, pp. 6483–6487.
Rahim, R., Dahria, M., Syahril, M. and Anwar, B. (2017), "Combination of the Blowfish and Lempel-Ziv-Welch algorithms for text compression", Vol. 15 No. 3, pp. 292–297.
Rahim, R. and Ikhwan, A. (2016a), "Study of Three Pass Protocol on Data Security", *International Journal of Science and Research*, Vol. 5 No. 11, pp. 102–104.
Rahim, R. and Ikhwan, A. (2016b), "Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher", *International Journal of Scientific Research in Science and Technology (IJSRST)*, Vol. 2 No. 6, pp. 71–78.
Sethi, P. and Kapoor, V. (2016), "A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography", *Procedia Computer Science*, Vol. 87, pp. 61–66.
Wandani, H., Budiman, M. and Sharif, A. (2012), "Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem", *Alkhawarizmi*, available at: http://jurnal.usu.ac.id/index.php/alkhawarizmi/article/view/500.
xiaojuan, M. (2017), "Research and Implementation of Computer Data Security Management System", *Procedia Engineering*, Vol. 174, pp. 1371–1379.

Authors Affiliations

Robbi Rahim, Department of Informatics, Institut Teknologi Medan, Medan, Indonesia

Corresponding Author

Robbi Rahim can be contacted at: usurobbi85@zoho.com