Base64, End of File and One Time Pad for Improvement Steganography Security

To cite this article: R Rahim et al 2018 IOP Conf. Ser.: Mater. Sci. Eng. 407 012161

View the article online for updates and enhancements.
Base64, End of File and One Time Pad for Improvement Steganography Security

R Rahim¹, R Ratnadewi², D Prayama³, E Asri³ and D Satria³

¹Department of Management, Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia
²Electrical Engineering, Universitas Kristen Maranatha, Bandung, Indonesia
³Department Information Technology, Politeknik Negeri Padang, Padang, Indonesia

Abstract. The aim of the study was to increase the level of security of data hiding and make it harder for cryptanalysts to know the hidden information. Improving confidentiality data is very important and can be performed by using a cryptography algorithm and combining few algorithms. End of File (EOF) were one of steganography method that widely used because it easily implemented in any media, combination of Base64 algorithm and One Time Pad as encoding and encryption process on data or object before embedded process using EOF method will produce a strong ciphertext that is good because one time pad using dynamic key as length message, ciphertext will be embedded in bytecode using EOF method and with the combination already perform it will not be easy to read by irresponsible party.

1. Introduction

The security of data in today's digital age is very important [1-6], steganography and cryptography can be used to secure data in the form of text messages, documents, images, audio and video [7-9]. Pictures [10,11] are the most widely used objects both offline and online and also some images are confidential and should not be publicized which is maybe a picture of research or just personal consumption. Pictures and other data should be secured this is where cryptography and steganography use is necessary.

Steganography is a technique to hide secret information into various types of files such as images, video, and audio [9,12,13], the problems that occur in steganography is to require different types of algorithms to secure specific data [13,14], for example, to ensure messages can use the method LSB, MSB and Pixel Value Differencing [9], to hide images or document files can use the Zhang LSB algorithm and so to protect other file types [15], to facilitate the process of embedded messages and various file types then used EOF and Base64 methods [16-18]. The base64 method is used as the process of encoding messages or files into a printable text, while the EOF method is used to hide secret message into the cover media. The use of EOF and Base64 methods alone is not safe enough because the decoding process using Base64 can be done directly without secret key, to improve the security level of the hidden information One Time Pad algorithm are used as additional security. One Time Pad was chosen because the encryption process is very secure and until now it very difficult to attack, one of because the process of encryption and decryption requires the same key length with the message [19,20]. Previous research by Ramalingam [8], which applies EOF method and combined with cryptography algorithm to secure message in video, another research by Iswahyudi [21] combines two encryption algorithms to secure
data. Based on the results of this research it concluded that the combination of algorithms can be done with good results.

The use of the One Time Pad algorithm in the EOF steganography process is supposed to increase the level of security of data hiding and make it harder for cryptanalysts to know the hidden information.

2. Methods
The mechanisms of Base64, EOF and One Time Pad methods used to hide and secure information on media (carrier) can be seen in Figure 1:

![Figure 1. Base64, EOF, and One Time Pad Process.](image)

The above process is a security procedure of the embedded data using EOF method, the first step is converting the data into printable text with Base64 method, after that the printable text encrypted using One Time Pad algorithm, for Base64 process method is perform by changing the data 8 bits into 6 bits value based on Table 1 below:

| Index | Value | Index | Value | Index | Value | Index | Value | Index | Value |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| 0     | A     | 1     | B     | 2     | C     | 3     | D     | E     | F     |
| 1     | B     | 13    | N     | 26    | a     | 39    | n     | 52    | 0     |
| 2     | C     | 14    | O     | 27    | b     | 40    | o     | 53    | 1     |
| 3     | D     | 15    | P     | 28    | c     | 41    | p     | 54    | 2     |
| 4     | E     | 16    | Q     | 29    | d     | 42    | q     | 55    | 3     |
| 5     | F     | 17    | R     | 30    | e     | 43    | r     | 56    | 4     |
| 6     | G     | 18    | S     | 31    | f     | 44    | s     | 57    | 5     |
| 7     | H     | 19    | T     | 32    | g     | 45    | t     | 58    | 6     |
| 8     | I     | 20    | U     | 33    | h     | 46    | u     | 59    | 7     |
| 9     | J     | 21    | V     | 34    | i     | 47    | v     | 60    | 8     |
| 10    | K     | 22    | W     | 35    | j     | 48    | w     | 61    | 9     |
| 11    | L     | 23    | X     | 36    | k     | 49    | x     | 62    | +     |
| 12    | M     | 24    | Y     | 37    | l     | 50    | y     | 63    | -     |

Table 1. Base64 Index Value.

One Time Pad is a development of Vernam Cipher[19], [20]. The One Time Pad algorithm is part of the block cipher in classical cryptography using XOR operations. One Time Pad will become an unsolvable algorithm [20] if it meets the following requirements:
The key length should be equal to the length of the plaintext
The key used should be random and should be used only once

\[
E(x) = (F(x) + K(x)) \mod 26
\]

\[
(x) = (C(x) + K(x)) \mod 26
\]

End Of File (EOF) is one of the techniques used in steganography[22]. This technique uses by inserting the data at the end of the file. This technique can be used to add data of size as needed. The file size that has been embedded data is equal to the size of the file before the data embedded plus the size of data inserted into the file[17,21]. EOF is a development of the method of Least Significant Bit (LSB). LSB adds data into files at the end of bit- then EOF instantly adds data at the end of the file.

3. Results and Discussion
Implementation of Base64, EOF and One Time Pad Methods on data security is tried with several different objects like the message or even file, the first experiment to hide data as below:

Data/Message = INCITEST IS THE BEST

The data is transformed to Base64 based on table 1 that has described before, and the result is below:

Encoding Text = SU5DSVRFU1QgSVMgVEhFIEJFU1Q=

The conversion process for the file is not much different from the data message, the encoding result is then encrypted by using One Time Pad algorithm, for encryption process is done by converting encoding text into binary and One Time Pad key generated randomly so that it fulfills the requirements of One Time Pad algorithm, so the result:

Encoding Text = SU5DSVRFU1QgSVMgVEhFIEJFU1Q=

Binary =

Key =

Ciphertext Binary =

Cipherext= î-ïâIz°W P Íc @êpê¬âÅ-

Convert the plaintext, and the key does the above experiment into the binary form, and then performed the encryption process. The message security that is hidden with the One Time Pad algorithm depends on the One Time Pad key which is randomly mathematically so that the key used will not be possible with the same message. Table 2 is a result of some objects such as messages or files that have been converted into printable text using a Base64 method and encrypted using the One Time Pad algorithm.
Table 2 contains the object information want to hide, the size of the object, the base64 result and also the key used for the encryption and decryption process with the One Time Pad algorithm. The keys in table 2 generated randomly will make it difficult for cryptanalysts to find hidden messages, according to Kerckhoff's principle [23] that the algorithm used to secure information is known without providing a key so that the security of this research has been tested that it takes \( n \) million years to find out hidden messages if you do not know which keys to use.

4. Conclusions
The use of One Time Pad algorithm to increase the security of hidden data is successful, the security level of protected information depends on the very random key that was used, and it is generated computationally mathematically, and also the key must match the length of the message, and this helps the security of the hidden data.

References
[1] Xiaojuan M 2017 Research and Implementation of Computer Data Security Management System Procedia Eng. 174 p. 1371–1379.
[2] Nurdiyanto H, Rahim R and Wulan N 2017 Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement J. Phys. Conf. Ser. 930, 1 p. 12005
[3] 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–
[4] Rahim R. 2017 Man-in-the-middle-attack prevention using interlock protocol method ARPN J. Eng. Appl. Sci. 12. 22 p. 6483–6487.

[5] 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.

[6] 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.

[7] 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.

[8] Ramalingam M and Isa N A M, 2015 A steganography approach over video images to improve security Indian J. Sci. Technol. 8. 1 p. 79–86.

[9] 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.

[10] Kester Q 2013 A Visual Cryptographic Encryption Technique for Securing Medical Images arXiv Prepr. arXiv1307.7791 3. 6 p. 3–7.

[11] Zhou Y, Panetta K and Agaian S, 2009 Image encryption using binary key-images in 2009 IEEE International Conference on Systems, Man and Cybernetics p. 4569–4574.

[12] Altaay A A J, Sahib S Bin and Zamani M, 2012 An Introduction to Image Steganography Techniques in 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT) p. 122–126.

[13] Wang H and Wang S, 2004 Cyber Warfare: Steganography vs. Steganalysis Commun. ACM 47. 10 p. 76–82.

[14] Rahim R 2018 Searching Process with Raita Algorithm and its Application J. Phys. Conf. Ser. 1007 1 p. 12004.

[15] Zhang T Li W Zhang Y and Xijian P 2010 Detection of LSB matching steganography based on distribution of pixel differences in natural images in IASP 10 - 2010 International Conference on Image Analysis and Signal Processing p. 548–552.

[16] Fiscus K and Shinburg D 2011 Base64 Can Get You Pwned.

[17] Anggraini Y and Sakti D V S Y, 2014 Penerapan Steganografi Metode End of File ( Eof ) Dan Enkripsi Metode Data Encryption Standard ( Des ) Pada Aplikasi Pengamanan Data Gambar Berbasis Java Konf. Nas. Sist. Informasi, STMIK Dipanegara Makassar September 2016 p. 1743–1753.

[18] Rahim R 2018 Combination Base64 Algorithm and EOF Technique for Steganography J. Phys. Conf. Ser. 1007 1 p. 12003.

[19] Rubin F 1996 One-time pad cryptography Cryptologia 20. 4 p. 359–364.

[20] Matt C and Maurer U, 2013 The one-time pad revisited in IEEE International Symposium on Information Theory - Proceedings p. 2706–2710.

[21] 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.

[22] 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.

[23] Schmidt D and Jaeger T, 2013 Pitfalls in the automated strengthening of passwords in Proceedings of the 29th Annual Computer Security Applications Conference on - ACSAC ’13 p. 129–138.