Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 14-19 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Implementation Of Pohlig-Hellman Algorithm And Steganography Combination Of First Of File (Fof) And End Of File (EOF) For File Security

Reni Rahmadani[1], Hervei Desmon Hutahaean[2]

[1, 2]Department of Electrical Engineering, Universitas Negeri Medan, Medan, Indonesia

E-mail: renirahmadani@unimed.ac.id, harvei.hutahaean@gmail.com

ARTICLE INFO

Article history:
Received: 26 February 2020
Revised: 01 Maret 2020
Accepted: o1 May 2020

Keywords:
Cryptography, Pohlig-Hellman, Lehmann, Steganography, Combination of FOF and EOF.

ABSTRACT

The method of steganography First of File (FOF) has an additional lines at the beginning of image and End of File (EOF) method has an additional lines at the bottom of the image. To reduce the suspicion then FOF and EOF methods are combined produces stego image that has border at the top and bottom. To improve the security of message Pohlig-Hellman cryptographic algorithm is used. Pohlig-Hellman algorithm uses two keys (n and e) to process the encryption. Key n is a prime number algorithm tested with Lehmann. Key e have the legal conditions 1 <e <ϕ (n) where ϕ (n) = n-1. Stego image produced has additional lines at the top and bottom of the image, it is because the ciphertext is inserted at the beginning and end of the image matrix. The result shows that the encryption process takes longer than the decryption process. Processing 129 character message encryption process takes 78 milliseconds and the decryption process takes just 16 milliseconds. Cover image of size 148 KB becomes 150 KB after embedding process of 1132 characters ciphertext.

1. Introduction

Some types of messages are very sensitive. This cannot be shared with the crowd. Many people do not feel safe to send messages for fear of wiretapping, interruption, or modifications made by irresponsible parties. For this reason cryptography is used to encode a message. One cryptographic algorithm that can be used is the Pohlig-Hellman algorithm.

Pohlig-Hellman is a cryptographic algorithm that is similar to RSA because it has the same encryption and decryption formula. Encryption is the process of converting an original message called a plaintext into a ciphertext or encrypted message. Decryption is the opposite of encryption. This process returns ciphertext to plaintext. In RSA there are two keys that are used for encryption namely "e" and "n" both of these keys are public keys. And "d" is used for decryption which is the private key[12][13]. But in Pohlig-Hellman all keys used are private keys. The attack to this algorithm factorization of the keys is required[8].

In addition there is another algorithm used for secret messages. Steganography is a method of hiding messages into an intermediary media. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”[9][10]. One of the media that can be used is image. Many methods can be used in steganography such as LSB (Least Significant Bit), Spread Spectrum, FOF (First of File) and EOF (End of File). In the FOF method the message is inserted at the beginning of the image and EOF inserts the message at the end of the image. The message insertion made the picture has a black part on the part that was inserted so as to cause suspicion. To reduce suspicion, a combination of FOF and EOF algorithms is done by inserting a message at the beginning and end of the message so that it will look like a frame in the picture.

Accredited “Rank 4”(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 14-19 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

2. Study of Liturature

2.1. Cryptography

Cryptography is the study of the method of sending messages in secret [7]. Etymologically, cryptography comes from the Greek language where kryptos means "hidden" (hidden) and graphien which means "writing" (writing) [11].

The cryptographic system consists of five parts viz:[6],

1) Plaintext: original message or data.
2) SecretKey: the input for the encryption algorithm is a free value of the original text and determines the output of the encryption algorithm.
3) Ciphertext: output from the encryption algorithm.
4) Encryption Algorithm: The encryption algorithm has two inputs, original text and a secret key. The encryption algorithm transforms the original text to produce cipher text.
5) Decryption Algorithm: the decryption algorithm has two inputs namely the ciphertext and the secret key. The decryption algorithm restores the cipher text to the original text if the secret key used by the decryption algorithm is the same as the secret key used by the encryption algorithm [3].

2.2. Lehmann Prime Generator

To search prime numbers with the Lehmann algorithm consists of several stages, for example the author wants to determine whether p prime numbers [14].

1) Find the random number a with conditions $1 < a < p$
2) Calculate $L = (a/p) \equiv a^{((p-1)/2)} \bmod p$
3) If $L \neq 1$ and $L \neq -1$ then p composite
4) If $L = 1$ or $L = -1$ thenthe posibility of p is prime are bigger than 50%
5) If stage 4 has been fulfilled, repeat as many digits of the prime number sought.

2.3. Pohlig-Hellman

Initially the Pohlig-Hellman algorithm was invented by Roland Silver, but it was published by Stephen Pohlig and Martin Hellman [4]. The Pohlig-Hellman algorithm is patented in the United States and Canada. The Pohlig-Hellman encryption scheme is similar to RSA. This algorithm is not a symmetric algorithm because the keys used for encryption and decryption are different. This algorithm is not a public-key scheme because the encryption and decryption keys must be kept secret. Thus it is appropriate to say that the Pohlig-Hellman algorithm is a non-public key asymmetric algorithm.

Pohlig-Hellman Formula

$C = P^e \bmod n$

$P = C^d \bmod n$

where

$ed \equiv 1 \pmod{\phi(n)}$

$\phi(n)$ reads totient n is an Euler function where $n \geq 1$ and expresses the number of positive integers< n which are relatively prime with n.

Unlike RSA, n does not have to be defined as two large prime numbers. If the values of e and n are known, then the value d can be calculated. Without knowing the value of e or d, someone will be very difficult in doing calculations [5]. The implementation of the Pohlig-Hellman algorithm is sufficient to meet two cryptographic objectives namely confidentiality and data integrity.

2.4. End of File (EOF)

In the EOF method a message is inserted at the end of the image file. With this method, the number of messages inserted is unlimited. But the side effect is that the file size becomes larger than the original size [1]. In inserting with this method the image will also have a visible black part at the bottom of the image.

2.5 First of File (FOF)

The First of File method is not much different from the End of File method. According to the understanding of the word it can be said that in the First of File method the message is inserted at the

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 14-20 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

beginning of the file. Insertion with this method also has the same drawbacks with the End of File method only the part that appears black is at the beginning of the image.

2.6. Kombinasi FOF dan EOF

This method is a combination of FOF and EOF methods. In this method the message is inserted at the beginning and end of the image matrix. The message to be entered is divided into two, the first message section is inserted at the beginning of the matrix and the second message section is inserted at the end of the matrix.

3. Finding and Discussion

In this study, we run the test with several different messages and keys for each picture. The test results can be seen in table 1.

TABLE 1
TESTING RESULTS OF IMAGES

No	Pesan	Pjg Karakter dan Kunci	Gambar Awal	Gambar Stego
1	IMPLEMENTASI ALGORITMA POHLIG-HELLMAN DAN TEKNIK STEGANOGRAFI KOMBINASI FIRST OF FILE (FOF) DAN END OF FILE (EOF) PADA SISTEM KEAMANAN DATA	139 Kunci n = 79730927 Kunci e = 16196781	 640x426 789 KB	 640x428 802 KB
2	abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789 !@#$%^&*()_+{}|:"<>?~ `,./;[]\'	96 Kunci n = 76498241 Kunci e = 59550997	 1517x1009 4.37 MB	 1517x1011 4.38 MB
3	It is a curious thing, but perhaps those who are best suited to power are those who have never sought it. Those who have leadership thrust upon them, and take up the mantle because they must, and find to their own suprise thet they wear it well.	245 Kunci n = 93265339 Kunci e = 20641091 Kunci n = 90001253 Kunci e = 72553777	 450x294 388 KB	 450x298 393 KB
5	Accept who you are. Unless you're a serial killer.	50 Kunci n = 83852869 Kunci e = 70679387 Kunci n = 10607671 Kunci e = 5074433	 191x264 148 KB	 191x266 149 KB

Encryption and decryption time testing is done to see how the relationship between the number of messages and ciphertext with the length of time the encryption and decryption process. In this test the same key is used for all messages. The n key used is 34242449, e key is 5904305, and the d key is 13140081.

TABLE 2
ENCRYPTION AND DECRYPTION PROCESSING TIME

No	Massage Length	Encryption Time (milliseconds)	Ciphertext Length	Decryption Time (milliseconds)
1	129	78	1132	16
2	323	203	2871	31
3	929	562	8313	62
4	1193	733	10633	78
5	2708	1716	24765	296
6	3066	1849	27336	359

From table 2 it can be seen that the greater the message and ciphertext, the longer the encryption and decryption process. To further clarify the reading of the table can be seen in Figure 1.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 14-19 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

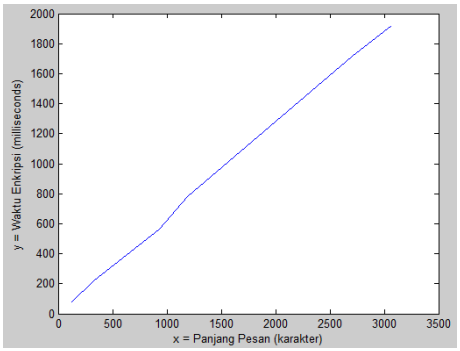

Figure. 1. Graphs of encryption time relation with message length

Figure 1. shows the graphic relation between the length of the message contained on the x-axis and the length of encryption on the y-axis. The graph shows the more messages that are input the longer the encryption process will take. This can be seen from the ascending graphical form. So the number of messages inputted is directly proportional to the length of the encryption process.

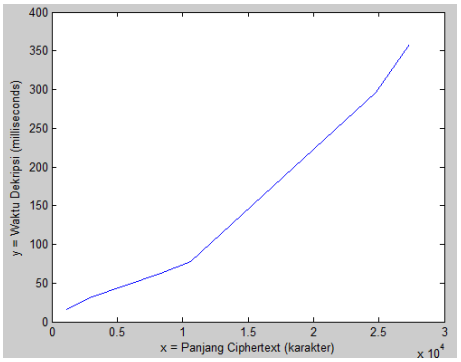

Figure. 2. Graphs of encryption time relation with message length

Similar to the encryption process, the number of ciphertext also is directly proportional to the length of timeof decryption as shown in Figure 2. where the length of the ciphertext is on the x-axis and the length of time of decryption is on the y-axis. It can be seen that the graphs go up with more and more ciphertext inserted.

In addition to testing the relation between the message length and the ciphertext length with the encryption and decryption time, a test is also performed to see the relation between the length of the key used and the length of time it is encrypted. The message used is 129 characters long. The results of this test can be seen in table 3

TABLE 3
ENCYPTION PROCESS

No	n Key Length	Encryption Time (milliseconds)
1	3	16
2	4	20
3	5	43
4	6	52
5	7	63
6	8	78

The relation between the results of the encryption time test and the length of the n key can be seen in the figure 3.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 14-20 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

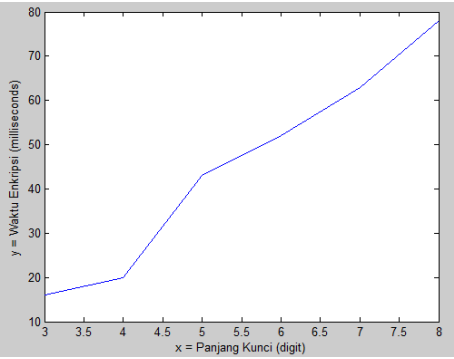

Figure. 3. Graph of key length relation with encryption time

From Figure 3. it can be seen that the graph is increasingly ascending even though the increase is relatively non-permanent, it can still be said that the greater the n key used in the encryption process, the longer the time needed to do the encryption process.

Testing the time for the insert and extract process also uses the same message and key as the encryption and decryption testing process. The image used as the initial image has a size of 148 KB. The results of the testing process of insert and extract can be seen in table 4

TABLE 4
INSERTION AND EXTRACTION TIME

No	Ciphertext Length	Insertion Time (miliseconds)	Stego Image Size	Extraction Time (miliseconds)
1	1132	437	150	406
2	2871	484	153	421
3	8313	546	160	468
4	10633	593	163	499
5	24765	724	183	640
6	27336	749	186	655

From the results of table 4, it can be seen that the more ciphertext is inserted, the longer the insertion and extraction time required. This can be seen in Figure 4.

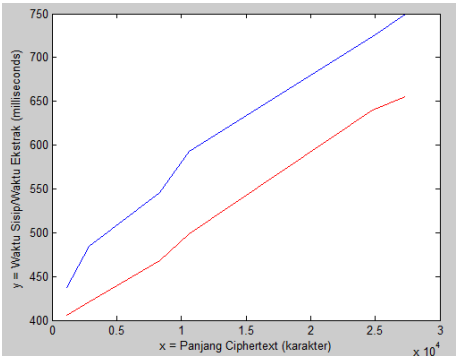

Figure. 4. Graph of the relation between insertion time and extract with ciphertext length

From Figure 4. it can be seen that the number of ciphertext is directly proportional to the length of the extraction and insertion time. The time for the insertion process is marked by a blue line and the time for the extraction process is marked by a red line. It can also be seen that the insert process requires a longer time than the extraction process.

From table 4 also can be seen the relationship between the length of the ciphertext that is inserted with the large stego image.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 14-19 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

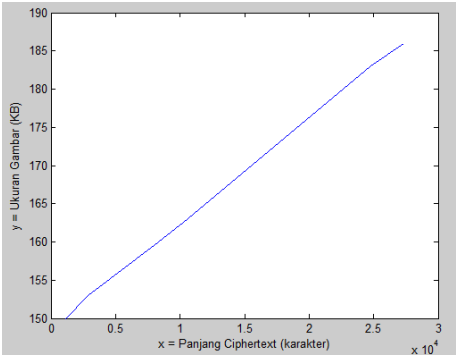

Figure. 5. Graph of the relation of image size with ciphertext length

4. Conclusion

Based on the results of the analysis, design, and testing of the data security system using the Pohlig-Hellman Algorithm and the First of File (FOF) and End of File (EOF) Steganography Combinations obtained the following conclusions:

1) Pohlig-Hellman cryptographic algorithms and FOF and EOF combination steganography can be combined to create a data security system.
2) The time of the encryption and decryption process is directly proportional to the number of messages inputted.
3) The encryption process takes longer than the decryption process. The encryption process for the 129 character message takes 78 milliseconds and the decryption process takes 16 milliseconds.
4) Stego images have a size larger than the original image. The initial image which has a size of 148 KB increases to 150 KB after the ciphertext is inserted as many as 1132 characters.

5. References

[1] *Rivest, R. L., Shamir, A., & Adleman, L., A method for obtaining digital signatures and public-key cryptosystems,Communications of the ACM, vol. 21, pp.120-126, 1978.*
[2] *Rahmadani, R., & Mawengkang, H., Hybrid cryptosystem RSA–CRT optimization and VMPC. In Journal of Physics: Conference Series, vol. 978, pp. 012041.2018.*
[3] *Flores-Carapia, R., Silva-Garcia, V. M., González-Ramírez, M. D., & Renteria-Marquez, C., A reinforced elgamal scheme proposal against a pohlig-hellman attack, Applied Mathematical Sciences, vol. 7, pp. 2909-2916. 2013.*
[4] *Hariri, M., Karimi, R., & Nosrati, M., An introduction to steganography methods. World Applied Programming, vol. 1, pp. 191-195.2011.*
[5] *Sara, K., Mashallah, A. D., Hossein, M. Y., A new steganography method based HIOP (Higher Intensity Of Pixel) algorithm and Strassen's matrix multiplication. Journal of Global Research in Computer Science, vol. 2, pp. 2011.*
[6] *Al-Riyami, S.S. & Paterson, K.G., Certificateless public key cryptography. In International Conference on the Theory and Application of Cryptology and Information Security, pp. 452-473. Springer: Berlin,2003.*
[7] *Budiman, M. A., & Rachmawati, D., Implementation of Super-Encryption with Trithemius Algorithm and Double Transposition Cipher in Securing PDF Files on Android Platform. Journal of Physics: Conference Series, vol. 978, pp. 012088. 2018.*
[8] *Stinson, Douglas. R.,Crytography: Theory and Practice, 2nd Edition, Chapman & Hall/CRC: Florida, 2002.*
[9] *Sadikin, Rifki., Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java, Penerbit Andi: Yogyakarta,2012.*
[10] *Lehmann, D. J., On primality tests. SIAM Journal on Computing, vol. 11, pp. 374-375.1982.*
[11] *Saragih, Nidia. J.,. Analisis dan Perancangan Aplikasi Pengamanan Pesan dengan Pohlig-Hellman Cryptosystem dan Metode End of File. Skripsi. Universitas Sumatera Utara, 2012.*
[12] *Schneier, Bruce.,Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc: New Jersey, 1996*
[13] *Krisnawati, Metode least significant bit (LSB) dan end of file (EOF) untuk menyisipkan teks kedalam citra grayscale,Prosiding Seminar Nasional Informatika 2008 (semnasIF 2008), pp. 39 – 44. 2008.*