A combination of vigenere algorithm and one time pad algorithm in the three-pass protocol

Dian Rachmawati*, *Amer* Sharif, and *Rosalia* Sianipar

Universitas Sumatera Utara, Departemen Ilmu Komputer, Fakultas Ilmu Komputer dan Teknologi Informasi, Jl. Universitas No. 9-A Medan 20155, Indonesia

Abstract. Cryptography is the method of delivery of messages in secret, thus only the intended message recipient can read the message. In this study, the cryptographic algorithms which used are Vigenere Cipher and One Time Pad. However, the security of both algorithms depends on the security of the algorithm key. Three-Pass Protocol is a scheme of work that lets two people exchange secret messages without doing a key exchange. So, both the symmetric cryptographic algorithms combined on a Three-Pass Protocol scheme. The purpose of the combination of two algorithms in the three-pass protocol is to secure the image message without exchange key process between sender and recipient. The results of the research and testing using GetPixel pointed out that safeguarding the image file using the combination of Vigenere Cipher and One Time Pad algorithm restores the original image files intact. Therefore, it meets the parameters of the integrity of the data. The test results based on time parameter shows that time of the program execution process is directly proportional to the size of the image. The result is related with the formula which calculate every pixels of the the image.

1 Introduction

The exchange of information today is effortless, especially for digital images or images. This can be seen from the increasing number of social media that provide the main features to exchange pictures, such as Instagram. Images created from pixels which contain three colors red, green and blue are called as RGB. Each pixel color includes one byte-sized information that indicates the density of the image's color [1].

The ease in transferring images makes people competing to display the best picture when not a few of them are private. A problem is when irresponsible parties are abusing the image of another's property, and this poses a threat to the related party. For that, much needed security for the digital images. One of the data security techniques is cryptography. Cryptography is both the arts and science of protecting the message by encoding it into a form that can no longer be understood [2]. The primary objectives of cryptography are integrity, authentication, confidentiality, and non-repudiation [3].

Vigenere Cipher is a symmetric key algorithm where the encryption key is the same as the decryption key. In the Vigenere Cipher algorithm, the keyword is repeated as much as is required with the length of plaintext.

The One Time Pad algorithm is known as a perfect secrecy algorithm. In the One Time Pad algorithm, the number of keys is the same length as the number of plaintexts.

The security of the two algorithms above depends on the key security of the algorithm. The Three-Pass Protocol is a work scheme that allows two people to exchange messages without exchanging keys.

Symmetric algorithms have a weakness in the key because it is predictable and straightforward, in addition to the network security factor when the key exchange also determines the security of the message. Therefore, the purpose of this research to cover the weakness of symmetry algorithm done by merging two symmetry algorithm and use of three pass protocol scheme to no longer needed key exchange process.

2 Methods

2.1 Cryptography

Cryptography is the science of the way of delivery of messages in secret (i.e., encrypted or disguise form) so that only the intended recipient of the message can let go incognito and read (or understand). The original message called plaintext and the secret word called ciphertext. The process of changing plaintext into ciphertext is called encryption. The method of restoring the ciphertext into plaintext, which is carried out by the recipient who has the knowledge to let go incognito, is called decryption [4].

The purpose of cryptography is four, namely [5]:

1. Confidentiality: information is kept secret from anyone except the official party.
2. Integrity: the message has not been changed at all during the shipping process.

* Corresponding author: dian.rachmawati@usu.ac.id

3. Authentication: the sender of the message is genuine. The alternative term is the authentication of the origin of the data.
4. Non-repudiation: the message sender cannot deny message creation.

2.2 Vigenere Algorithm

The Vigenere Cipher algorithm was first published in 1586 by Blaise de Vigenere. Vigenere Cipher is a method for encrypting alphabetical text using a different set of Caesar Cipher based on the letters in the keyword [6]. This algorithm is a symmetric key algorithm considering that knowing encryption is tantamount to understanding decryption and is a polyalphabetic substitution cipher. The keywords on Vigenere Cipher are repeated as much as necessary to cover all the plaintext [7]. Encryption and decryption in Vigenere cipher can be done easily using an enciphering table and its corresponding deciphering table [8].

Mathematically, the process of encryption and decryption is formulated as follows:

$$Ci = Pi + Ki \ (mod\ n) \quad (1)$$

$$Pi = Ci - Ki \ (mod\ n) \quad (2)$$

where P is plaintext, K is key, C is ciphertext, and n is some characters used.

2.3 One Time Pad Algorithm

Gilbert S. Vernam invented the One Time Pad algorithm in 1917. One Time Pad is an algorithm with a completely random key, used only once and the key length equal to the length of the plaintext. Therefore, this algorithm has perfect secrecy. One Time Pad earned a reputation as a powerful yet simple algorithm with a high level of security. The algorithm is also better than modern cryptographic algorithms.

Mathematically, the process of encryption and decryption is formulated as follows:

$$C = Pi + Ki \bmod n \quad (3)$$

$$P = Ci - Ki \bmod n \quad (4)$$

where P is plaintext, K is key, C is ciphertext, and n is the number of characters used.

2.4 Three-Pass Protocol

The Three-Pass protocol is a framework that allows a party send a message encrypted securely to the other party without having key exchange process [9]. Adi Shamir discovered this protocol. This protocol allows Alice and Bob to communicate securely without the exchange of keys either a secret key or a public key.

This assumes a commutative symmetrical cipher, EA (EB (P)) = EB (EA (P)). Alice's secret key is A. Bob's secret key is B. Alice sends a message (P) to Bob. Here is the scheme works:

1. Alice encrypts P with the key and sends it to Bob

$$C1 = EA\ (P) \quad (5)$$

2. Bob encrypts C1 with his key and sends it to Alice

$$C2 = EB\ (EA\ (P)) \quad (6)$$

3. Alice decrypts C2 with her key and sends it to Bob

$$C3 = DA\ (EB\ (EA\ (P))) = DA\ (EA\ (EB\ (P))) = EB(P) \quad (7)$$

4. Bob decrypts C3 with his key to get P [5].

2.5 The Combination of Vigenere and One Time Pad Algorithm in Three-Pass Protocol

How the combination of vigenere and one time pad algorithm works in Three-Pass Protocol is shown in figure 1.

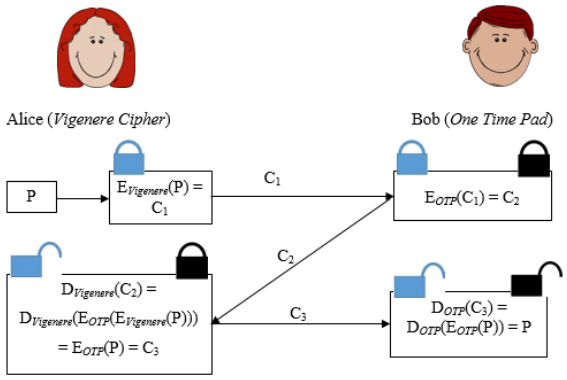

Fig. 1. The Combination of Vigenere and One Time Pad Algorithm in Three-Pass Protocol.

This figure 1 shows that Three-Pass Protocol is a framework that allows the sender to send encrypted messages to the recipient without the need to distribute the sender's key to the receiver [10]. Sender and receiver have their respective key, in this case, Alice uses the key from vigenere cipher, and Bob uses the key from one time pad.

3 Results

3.1 The Calculation Process

The calculation process using the combination of the two algorithms in the three pass protocol scheme is as follows:

For example, sender wants to encrypt plain image which shown in figure 2 by using Vigenere Cipher.

R: 191 G: 158 B: 159	R: 103 G: 3 B: 0	R: 164 G: 115 B: 115
R: 194 G: 154 B: 131	R: 232 G: 195 B: 164	R: 196 G: 160 B: 135
R: 234 G: 224 B: 216	R: 198 G: 153 B: 125	R: 238 G: 227 B: 220

Fig. 2. Plain image and its RGB values.

If sender has keys $K_1 = 234$, $K_2 = 98$, $K_3 = 182$, $K_4 = 46$, $K_5 = 28$

By using this formula $C_i = P_i + K_i \pmod n$, it will generate RGB cipher image for the first row and column as show below:

$C_{11} = (191, 158, 159) + 234 \pmod{256} = (425, 392, 393) \pmod{256} = (169, 136, 137)$

The same calculation method is done up to the last row and column. This first encryption process by sender will produce a cipher image I is shown in figure 3:

R: 169 G: 136 B: 137	R: 201 G: 101 B: 98	R: 90 G: 41 B: 41
R: 240 G: 200 B: 177	R: 4 G: 223 B: 192	R: 174 G: 138 B: 113
R: 76 G: 66 B: 58	R: 124 G: 79 B: 51	R: 28 G: 17 B: 10

Fig. 3. Cipher image I and its RGB values.

The cipher image I will send to the receiver and the receiver do the encryption process again by using One Time Pad algorithm. The formula that will use is $C_i = P_i + K_i \bmod n$. If receiver has keys $K_1 = 029$; $K_2 = 000$; $K_3 = 242$; $K_4 = 236$, $K_5 = 183$, $K_6 = 124$, $K_7 = 237$, $K_8 = 126$, $K_9 = 149$. Then the encryption process for the first row and column as show below:

$C_{21} = C_{11} + K_1 \pmod n = (169, 136, 137) + 029 \pmod{256} = (198, 165, 166) \pmod{256} = (198, 165, 166)$

The same calculation method is done up to the last row and column. This second encryption process by receiver will produce a cipher image II is shown in figure 4:

R: 198 G: 165 B: 166	R: 201 G: 101 B: 98	R: 2 G: 27 B: 27
R: 220 G: 180 B: 157	R: 187 G: 150 B: 119	R: 42 G: 6 B: 237
R: 57 G: 47 B: 39	R: 250 G: 205 B: 177	R: 177 G: 166 B: 159

Fig. 4. Cipher image II and its RGB values.

The cipher image II will send back to the sender, and the sender does the first decryption process by using this formula $P_i = C_i - K_i \bmod n$. If $C_{3i} < 0$ then $C_{3i} = C_{3i} + 256$. Then the decryption process for the first row and column as shown below:

$C_{31} = C_{21} - K_1 \pmod n = (198, 165, 166) - 234 \pmod{256} = (-36, -69, -68) \pmod{256} = (220, 187, 188)$

The same calculation method is done up to the last row and column. This first decryption process by the sender will produce a cipher image III is shown in figure 5:

R: 220 G: 187 B: 188	R: 103 G: 3 B: 0	R: 150 G: 101 B: 101
R: 174 G: 134 B: 111	R: 159 G: 122 B: 91	R: 64 G: 28 B: 3
R: 215 G: 205 B: 197	R: 68 G: 23 B: 251	R: 131 G: 120 B: 113

Fig. 5. Cipher image III and its RGB values.

The cipher image III will send back to receiver, and the receiver do the second decryption process by using this formula $P_i = C_i - K_i \bmod n$. If $P_i < 0$ then $P_i = P_i + 256$. Then the decryption process for the first row and column as shown below:

$P_1 = C_{31} - K_1 \pmod n = (220, 187, 188) - 029 \pmod{256} = (191, 158, 159) \pmod{256} = (191, 158, 159)$

The same calculation method is done up to the last row and column. This last decryption process by the receiver will produce a cipher image IV is shown in figure 6:

R: 191 G: 158 B: 159	R: 103 G: 3 B: 0	R: 164 G: 115 B: 115
R: 194 G: 154 B: 131	R: 232 G: 195 B: 164	R: 196 G: 160 B: 135
R: 234 G: 224 B: 216	R: 198 G: 153 B: 125	R: 238 G: 227 B: 220

Fig. 6. Cipher image IV and its RGB values.

3.2 Data Integrity Testing

Data integrity is one of the parameters used to test the implementation of the Three-Pass Protocol scheme with a combination of two classical cryptographic algorithms. Testing is done by using GetPixel in C # language to see the RGB pixel values in the image. Based on the results of system testing in the whole process of encryption and decryption of a plain image with a combination of Vigenere Cipher and One Time Pad algorithms in the Three-Pass Protocol scheme described earlier, it is seen that the RGB plain image pixel value before being encrypted is equal to the RGB pixel value of image which results from decryption of One Time Pad. The RGB plain image pixel value before being encrypted equals after being decrypted with the One Time Pad algorithm (cipher image IV). This proves that the combination of Vigenere Cipher and One Time pad algorithms in the Three-Pass Protocol scheme meets the parameters of data integrity.

3.3 Testing Algorithm against Process Time

The relation of the program execution time to the size of an image can be seen in figure 7:

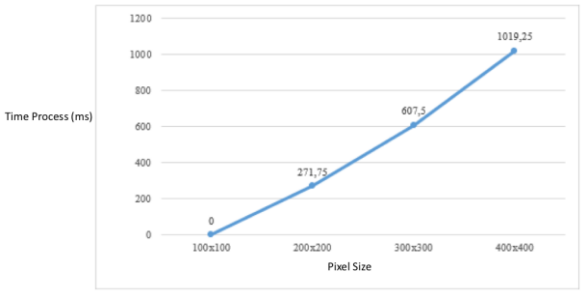

Fig. 7. Graph Testing Algorithm against Process Time.

Based on the figure 7 can be seen the relationship of processing time is linearly straight to the size of the image which means that the larger the image size, the longer it will take time to execute the program.

4 Conclusions

The conclusions that can be drawn from this research are Three-Pass Protocol Implementation with the combination of Vigenere Cipher algorithm and One Time Pad algorithm can secure the image file successfully because of the cipher image looks different with the original image. Both of sender and receiver can use their key and algorithm, without doing key exchange. Based on test results with GetPixel, encryption and decryption process in image file security using a combination of Vigenere Cipher algorithm and One Time Pad on Three-Pass Protocol fulfill the data integrity parameter. Based on the graph of the relationship between the processing time encryption and image decryption with pixel size indicates that the processing time is directly proportional to the size of the image. The larger the image pixel size, the greater the time of encryption and decryption process.

We gratefully acknowledge that this research is funded by Fund Dissemination IPTEKS Research Results for Lecturers / Researchers Universitas Sumatera Utara.

References

1. Patel K, Utareja S, Gupta H. *Information Hiding Using Least Significant Bit Steganography and Blowfish Algorithm* International Journal of Computer Applications **63** (13) 24 – 28. (2013)
2. D Rachmawati *et al, IOP Conf. Ser.: Mater. Sci. Eng.* **308** 012003 (2018)
3. Dian Rachmawati *et al. IOP Conf. Ser.: Mater. Sci. Eng.* **300** 012040 (2018)
4. Mollin, R.A. *An Introduction to Cryptography: Discrete Mathematics and Its Application.* Kenneth H. Rosen. 2nd Edition. Taylor & Francis Group, (LLC: New York. 2007)
5. Paar, C. & Pelzl, J. *Understanding Cryptography A Textbook for Students and Practitioners.* (Springer: New York. 2010)
6. Kester, Q. A cryptosystem based on Vigenere cipher with varying key. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* 1(10): 108-113. (2012)
7. Mollin, R.A. *RSA and PUBLIC–KEY CRYPTOGRAPHY: Discrete Mathematics and Its Application. Kenneth H. Rosen.* Taylor & Francis Group, (LLC: New York. 2003)
8. Yumnam Kirani Singh, *Generalization of Vigenere Cipher*, ARPN Journal of Engineering and Applied Sciences VOL. **7**, NO. 1 (2012)
9. Amin Subandi et al, *Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification*, Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 5, 1-5 (2017)
10. D Rachmawati *et alI. OP Conf. Ser.: Mater. Sci. Eng.* **308** 012003 (2018)