Combination of Rivest-Shamir-Adleman Algorithm and End of File Method for Data Security

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

Email: dian.rachmawati@usu.ac.id

Abstract. Data security is one of the crucial issues in the delivery of information. One of the ways which used to secure the data is by encoding it into something else that is not comprehensible by human beings by using some cryptographic techniques. The Rivest-Shamir-Adleman (RSA) cryptographic algorithm has been proven robust to secure messages. Since this algorithm uses two different keys (i.e., public key and private key) at the time of encryption and decryption, it is classified as an asymmetric cryptography algorithm. Steganography is a method that is used to secure a message by inserting the bits of the message into a larger media such as an image. One of the known steganography methods is End of File (EoF). In this research, the cipher text resulted from the RSA algorithm is compiled into an array form and appended to the end of the image. The result of the EoF is the image which has a line with black gradations under it. This line contains the secret message. This combination of cryptography and steganography in securing the message is expected to increase the security of the message, since the message encryption technique (RSA) is mixed with the data hiding technique (EoF).

1. Introduction
Message security is urgently needed to safeguard the privacy of the owner of the message. There are many methods that can be used to protect the message. Cryptography is a way which is commonly used to provide data security. Cryptography, in general, is a science and art to keep the confidentiality of the information. Cryptography has encryption algorithm, some of them have been classified as symmetric algorithm and the others have been categorized as asymmetric algorithm [1]. Rivest-Shamir-Adleman (RSA) is an asymmetric cryptographic algorithm whose public key component is built with two distinct primes. In order to build an exact key, it requires some mathematical operations because the processed data is in numerical form, and will go through several stages of calculations until a secure key pair is obtained. The RSA algorithm consists of some discrete mathematics calculations, most importantly modulo exponentiation. [2]. The RSA has three stages: key generation, enciphering, and deciphering. The key generation stage begins by generating two random prime numbers (p, q), computing and publishing the public key pair (n, e), and computing the decryption key (d). The enciphering or encryption stage begins by receiving the public key pair and calculating the cipher text from the original message. The deciphering or decryption stage begins by getting the cipher text and calculating the value of the plaintext using the decryption key.

Delivering the cipher text by using RSA algorithm to the recipient may cause suspicion to the unwanted parties since the cipher text which appears random may cause them to think that there is something hidden in it. In order to minimize this suspicion, the cipher text is embedded into a larger
media without noticeable changes. The technique of hiding confidential data in digital media so that the existence of the confidential data is not known by the other person is called steganography. Steganography is done by hiding (or embedding) the confidential data into a media. The media is then sent to the recipient. In order to recover the data, the recipient extracts the hidden (or embedded) data from the media. Steganography has several methods, one of them is the End of File (EoF) method which appends the data to the end of the file. EoF method is adapted from the end of file marker method which used by the windows operating system. The combination of RSA algorithm and EoF is expected to improve data security and reduce the suspicion of third-party about the existence of confidential data. Cryptography and steganography are the fundamental methods which use to protect the data from unauthorized access [3].

2. Methods
2.1. Rivest Shamir Adleman Algorithm
RSA which was built by modular exponential function consists of three main processes, namely: key generation, encryption, and decryption [4].

Step 1. RSA Key Generation
Decryption must generate public and private keys in order to use RSA. Both of these keys require two large primes to make it difficult to be factored. The following RSA key generation algorithm is [5]:

\begin{align*}
(p, q) &\leftarrow \text{large random primes} \\
n &\leftarrow p \cdot q \\
\phi(n) &\leftarrow (p - 1) \cdot (q - 1) \\
e &\leftarrow \text{the odd random numbers in range } 1 < e < \phi(n), \gcd(e, \phi(n)) = 1 \\
d &\leftarrow e^{-1} \mod \phi(n) \\
K_{\text{public}} &= (e, n) \\
K_{\text{private}} &= d
\end{align*}

Step 2. RSA Encryption
The encryption process uses the RSA public key that has been raised before. RSA encryption algorithm uses a modular exponential function as follows:

\begin{align*}
K_{\text{public}} &= (e, n) \\
P &= \text{plain text} \\
C &= P^e \mod n
\end{align*}

Step 3. RSA Decryption
To restore the cipher text into plain text, the RSA decryption also a form of a modular exponential function N by using the private key. The following algorithm RSA decryption are:

\begin{align*}
K_{\text{private}} &= d \\
C &= \text{cipher text} \\
P &= C^d \mod n
\end{align*}

2.2. End Of File
End-of-File (EoF) is a method or technique of steganography that hides a message by appending it to the end of the file horizontally. This technique can be used to insert the message into the needed size. The size of the files that have been inserted are equal with the size of the file before it is inserted into the message plus the size of the message that is inserted into the file. In this technique, the message is appended at the end of the file with the given identifier as the distinctive mark at the beginning of the message and the identifier of the end of the data.

In order not to cause any suspicions, it has to be arranged in some ways so that the inserted message does not change the size and shape of the image at the time is displayed, because the image-forming element is the pixel that has a value of Red, Green, and Blue [6]. The example of an image will be shown in Table 1, and already inserted by cipher text using steganography End of File method. Cipher text value is marked with a red number.
Table 1. The RGB value of an image before and after End of File process.

|   | R : 23 | R : 35 | R : 16 | R : 23 | R : 35 | R : 16 |
|---|--------|--------|--------|--------|--------|--------|
| G | 17     | G : 50 | G : 23 | G : 17 | G : 50 | G : 23 |
| B | 87     | B : 97 | B : 56 | B : 87 | B : 97 | B : 56 |

|   | R : 70 | R : 88 | R : 48 | R : 70 | R : 88 | R : 48 |
|---|--------|--------|--------|--------|--------|--------|
| G | 42     | G : 89 | G : 72 | G : 42 | G : 89 | G : 72 |
| B | 48     | B : 39 | B : 35 | B : 48 | B : 39 | B : 35 |

|   | R : 13 | R : 15 | R : 19 | R : 13 | R : 15 | R : 19 |
|---|--------|--------|--------|--------|--------|--------|
| G | 44     | G : 80 | G : 23 | G : 44 | G : 80 | G : 23 |
| B | 47     | B : 18 | B : 36 | B : 47 | B : 18 | B : 36 |

3. Results and Discussion

In some case, the stenography is still not secure enough to hide the data. Therefore the merger by cryptographic methods is needed [7]. For example End Of File is a steganography method which is easy to recognize because the secret massage was hidden in the bottom of the cover object. Therefore in this research, it uses a cryptography algorithm such as RSA to encode the message first, before it was embedded to the cover object. The combination of RSA method and the End of File method can be illustrated in the Figure 1.

![Figure 1](image_url)

**Figure 1.** The combination of RSA algorithm and End of File in the security message.

In the image above are explained that the sender of the encrypted message with the RSA algorithm and perform the insertion with End of File algorithm, while the recipients doing the extraction process by using the End of File algorithm and decrypt the message by RSA algorithm.

The example of message security process is: if we have a message “Dian USU Medan”, then the first step is to change the message into the ASCII to 68 105 97 110 32 85 83 85 32 77 101 100 97 110. And then make a key generation process by using the RSA method. The first step is to take the two pieces of prime numbers, such as p = 11 and q = 13. Next step is to do a multiplication p and q so that we could retrieve n = 143 and φ (n) = 120 from the obtained formula of e and d are e=7 d=103. By using the encryption formula then it will gain the cipher text 29 118 59 33 98 123 8 123 98 77 62 100 59 33. The result of the cipher text then inserted into the cover image as illustrated in Table 2.
Table 2. Insertion Process in Cover Image.

| R  | G  | B  | R  | G  | B  | R  | G  | B  | R  | G  | B  | R  | G  | B  |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 13 | 72 | 18 | 10 | 54 | 27 | 16 | 120| 87 | 120| 89 | 89 | 111| 111|
| 56 | 96 | 18 | 72 | 78 | 72 | 134| 134| 110| 110| 110| 110| 110| 110|
| 48 | 48 | 48 | 61 | 61 | 61 | 93 | 93 | 93 | 93 | 93 | 93 | 93 | 93 |
| 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 |
| B  | B  | B  | B  | B  | B  | B  | B  | B  | B  | B  | B  | B  | B  |
| 182| 182| 182| 182| 182| 182| 182| 182| 182| 182| 182| 182| 182| 182|
| 49 | 49 | 49 | 49 | 49 | 49 | 49 | 49 | 49 | 49 | 49 | 49 | 49 | 49 |
| 78 | 78 | 78 | 78 | 78 | 78 | 78 | 78 | 78 | 78 | 78 | 78 | 78 | 78 |
| R  | R  | R  | R  | R  | R  | R  | R  | R  | R  | R  | R  | R  | R  |
| 56 | 56 | 56 | 56 | 56 | 56 | 56 | 56 | 56 | 56 | 56 | 56 | 56 | 56 |
| 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 |
| 80 | 80 | 80 | 80 | 80 | 80 | 80 | 80 | 80 | 80 | 80 | 80 | 80 | 80 |

After the insertion, the recipient do an extraction on stego image by taking the RGB value at the very bottom of the file. So the cipher text is obtained as follows: 29 118 59 33 98 123 8 123 98 77 62 100 59 33. By using the decryption process, the original message, i.e., Dian USU Medan, is then recovered. From the result of these calculations, it can be seen that the combination of RSA algorithm and End of File can restore message into the original form.

The message “Dian Amalia Eliviani Ilmu Komputer USU Medan” takes 6.43 seconds during an encryption, 0.56 second during the insertion, 0.41 seconds during the extraction and 7.1 seconds during the decryption. Meanwhile, the message “Ilmu Komputer USU” takes 4.23 seconds for the encryption, 0.54 second for the insertion, 0.39 second for the extraction, and 4.34 seconds for the decryption. In Table 3, it is shown that the usage of the value of pixel size for keeping the message.

Table 3. An Experiment by using various pixel size.

| No. | Pixel | Cover Image | Stego Image |
|-----|-------|-------------|-------------|
| 1   | 1800 x 1300 | [Image] | [Image] |
|     | 7280 KB | 9561 KB |
| 2   | 900 x 600   | [Image] | [Image] |
|     | 1779 Kb | 2237 Kb |
4. Conclusion
The use of RSA algorithms to encrypt messages can obfuscate the messages into the form that are not understood by third parties since the resulting cipher text appears random. The combination of RSA and EoF algorithms in this study is able to encode and hide messages into the image media by not significantly changing the quality of the cover image, so the inserted image does not look much different from the original image. In the EoF method, the one that distinguishes the original image from the inserted image is the line below the image. The larger the size of the cover image, the smaller the black line under the image appears to be. The extraction and decryption of data by this algorithm can return the data to the original size. The longer the message, the longer time it takes to perform the encryption and decryption of that message.

Acknowledgments
The authors gratefully acknowledge that the present research is supported by Fund Dissemination IPTEKS Research Results for Lecturers / Researchers University Sumatera Utara.

References
[1] George D and Bonifus P L 2013 *International Conference on Advanced Computing and Communication Systems* p 1-4. doi: 10.1109/ICACCS.2013.6938727
[2] Saxena and Kapoor B 2014 *IEEE International Advance Computing Conference (IACC)* p 850-854. doi: 10.1109/IAdCC.2014.6779433
[3] Kothari L, Thakkar R and Khara S 2017 *International Conference on Computer, Communications and Electronics (Comptelix)* p 448-452. doi: 10.1109/COMPTELIX.2017.8004011
[4] Paar C and Pelzl J 2010 *Understanding Cryptography* (Berlin: Springer-Verlag)
[5] Mollin R A 2002 *RSA and Public-Key Cryptography*. 2nd Edition (Florida: Chapman & Hall/CRC)
[6] Rachmawati D et al 2017 *J. Phys.: Conf. Ser.* 801 012059 doi : https://doi.org/10.1088/1742-6596/801/1/012059
[7] Duluta A, Mocanu S, Pietraru R, Merezeanu D and Saru D 2017 *21st International Conference on Control Systems and Computer Science (CSCS)* p 453-458. doi: 10.1109/CSCS.2017.70