Implementation of Rivest Shamir Adleman Cryptographic Algorithms and Techniques of Steganography First of File for Message Security

Dian Rachmawati*, Yeni Rosalin Munthe*

1 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, yenrosm@gmail.com

Abstract. Accessing data by an unauthorized person often happens these days. Addressing this case, the techniques of cryptography and steganography was necessary. The science of cryptography use randomizes/disguise the data, whereas the science of steganography to hide data in a way. The cryptographic algorithms to be used is the Rivest Shamir Adleman (RSA) which utilizes two prime numbers to generate a public key and private key. To further enhance the security of message, the algorithm has combined with the First of File (FoF) as steganography techniques. The technique First of File (FoF) works by inserting a message at the beginning of the file image horizontally to produce a stego image that will extract to get the previous ciphertext. Then the ciphertext decrypted to be returned to the original message. By using FoF, in the cover image with large pixel size, the insertion process with FoF is entirely invisible, so the stego image and original image cannot be distinguished, whereas in small pixels there is a black line above the image. A combination of RSA and the FoF will increase data security because when a message has scrambled into a ciphertext and the ciphertext will be inserted into the image file.

1. Introduction

The primary purpose of data security is to secure data/information from abuse by irresponsible parties. With data security, actions such as sabotage and unauthorized data exchange can be prevented. But data security has not been a top priority for most people at the moment. It frequently found incidents related to data security disorders. Therefore, to overcome these circumstances can be used some science from data security majors such as cryptography and steganography.

Overall the concept of cryptography is to scramble or disguise the meaning of a message but not hide it so it can still be seen and can cause suspicion. The technique of steganography has developed to avoid suspicion. In general, steganography is an art or science that is used to hide secret messages in any way that other than the intended person, others will not be aware of the existence of the secret message. Secret hidden data can also be image, audio, text, or video. Steganography demonstrates an option method to conceal the presence of information in the cover picture. The mystery message is recovered negligible by approved individual [1]. There are a lot of steganography techniques for hiding secret
information in a cover object. Some methods are more complicated than others, but all of them have respective strong and weak points [2].

The use of a cryptographic method or even a steganography method can no longer guarantee the security of a message. This is due to the rapid development of cryptanalysis science. In this research used the combination of cryptography and steganography method, so the use of a combination of these two methods is expected to make the message security becomes more powerful. In this research, the cryptographic algorithm used is Rivest Shamir Adleman (RSA) and steganography method used is First of File (FoF).

2. Method

2.1. Rivest Shamir Adleman

RSA (from Rivest-Shamir-Adleman) is a public-key cryptosystem based on exponentiation in finite fields over integers modulo N where N is a composite integer of two significant factors (i.e., a semi-prime) [3]. It has based on the mathematical operation that is very easy to compute in one direction, calculating the product of two large primes. On the other hand, the different course is tough to do, factoring the modulus equal to the production of two of large primes[4].

RSA cryptographic public key algorithm is illustrated by a sender and receiver with Alice as the sender and Bob as the recipient of the message [5].

**Step 1. Generating RSA keys**

(1) Bob generates two large primes p and q at random, where p ≠ q.
(2) Calculated the value of p and q to produce n = p x q and searched for its totient value $\phi(n) = (p-1) (q-1)$. The n number of RSA is called the modulus.
(3) Then Bob specifies a random integer for the encryption key (e) where $1<e<\phi(n)$ and the value is relatively primed with $\phi(n)$. GCD(e, $\phi(n)$ = 1). RSA is called enciphering exponent.
(4) With the Euclidean algorithm, Bob gets the decryption key (d) where $e \times d \equiv 1 \pmod{\phi(n)}$ with $1<d<\phi(n)$. The encryption value d in RSA is called deciphering exponent.

Bob publishes (n, e) as the public key and stores the d, p, q, and (n) values as private keys.

**Step 2. Enciphering Stage**

Alice has a message or plaintext (m) where m < n, and GCD (m, n) = 1. Alice gets Bob’s public key (n, e) from the database and encrypts m into ciphertext with computation $c \equiv m^e \pmod{n}$. Then Alice sends ciphertext (c) to Bob.

**Step 3. Deciphering Stage**

When Bob gets the ciphertext (c) from Alice, then Bob will use the private key d to convert the ciphertext to plaintext. $M \equiv c^d \pmod{n}$.

2.2. First of File (FoF)

First of File is a method or steganography technique to hide or insert messages at the beginning of the file horizontally. This technique can be used to add messages to the short length or long length. The file size which the message has inserted is larger than the original file. Images created from the pixel, pixel generated by using these three colors red, green and blue have called RGB [6]. An example of the RGB value of an image before and after the message inserted with the FoF method has shown in table 1.
3. Results and Discussions
The combined use of cryptography (RSA) and steganography (FoF) in this study are shown in Figure 1 below:

![Diagram showing the combination of RSA and FoF](image)

**Figure 1. Combination of RSA and FoF**

Figure 1 has shown the combination of RSA and FoF process which is sender do encryption by using public key and embedded operation, and the receiver does extraction and decryption by using private key.

The process of RSA shown by the calculation below: the key will be generated by taking 2 primes for example p and q are P = 23, Q = 13, N = p \cdot q , N = 299, \phi(n) = (p - 1) \cdot (q - 1) , \phi(n) = 264. Find e value with formula 1 < e < \phi(n), gcd (e, \phi(n)) = 1, e = prime number. Let e = 137, Looking for
value d with the formula \( d = e^{-1} \mod \phi(n) \), \( d = 185 \). RSA algorithm is used to encrypt messages. The character will be changed first to the decimal form according to the ASCII table, after which the characters will be encrypted per each character. For example, there is a message = Dian Rachmawati. This message will be converted to integer number based on ASCII table. The message numbers are 068 105 097 110 032 082 097 099 104 109 097 119 097 116 105. By using the formula \( c \equiv m^e \mod n \). The message will be changed to 22 27 158 210 54 257 158 86 156 44 158 58 158 116 27. This integer numbers will be embedded to cover image by using FoF as shown by table 2.

### Table 2. RGB value of an image after the message Dian Rachmawati inserted

| R=22 | R=210 | R=158 | R=44 | R=158 | R=0 | R=0 | R=0 | R=0 | R=0 | R=0 | R=0 |
|------|-------|-------|------|-------|-----|-----|-----|-----|-----|-----|-----|
| G=27 | G=54  | G=86  | G=158| G=116 | G=0 | G=0 | G=0 | G=0 | G=0 | G=0 | G=0 |
| B=158| B=257 | B=156 | B=58 | B=27  | B=0 | B=0 | B=0 | B=0 | B=0 | B=0 | B=0 |

| R=52 | R=42  | R=48  | R=61 | R=80  | R=97 | R=52 | R=52 | R=52 | R=52 | R=52 | R=52 |
|------|-------|-------|------|-------|-----|-----|-----|-----|-----|-----|-----|
| G=89 | G=79  | G=82  | G=93 | G=111 | G=120| G=89 | G=89 | G=89 | G=89 | G=89 | G=89 |
| B=118| B=106 | B=107 | B=116| B=132 | B=134| B=118| B=118| B=118| B=118| B=118| B=118|

| R=58 | R=49  | R=46  | R=50 | R=54  | R=75 | R=58 | R=58 | R=58 | R=58 | R=50 | R=54 |
|------|-------|-------|------|-------|-----|-----|-----|-----|-----|-----|-----|
| G=86 | G=77  | G=78  | G=86 | G=98  | G=111| G=86 | G=86 | G=86 | G=86 | G=86 | G=98 |
| B=107| B=98  | B=101 | B=110| B=125 | B=133| B=107| B=107| B=107| B=110| B=110| B=125|

| R=69 | R=60  | R=62  | R=56 | R=52  | R=73 | R=69 | R=73 | R=62 | R=56 | R=56 | R=52 |
|------|-------|-------|------|-------|-----|-----|-----|-----|-----|-----|-----|
| G=65 | G=87  | G=91  | G=87 | G=89  | G=102| G=65 | G=102| G=91 | G=87 | G=78 | G=89 |
| B=32 | B=106 | B=109 | B=107| B=116 | B=32 | B=116| B=116| B=109| B=107| B=101| B=107|

Extracting process do by collecting the RGB values from the First of File which is contained numbers 22 27 158 210 54 257 158 86 156 44 158 58 158 116 27. By using private key d and formula \( m \equiv c^d \mod n \). The message will be back to 68 105 097 110 032 082 097 99 104 109 097 119 097 116 105 and has converted to ASCII table as a string Dian Rachmawati. The combination of RSA and FoF can protect the message and also hide it from an intruder.

The experimental result by using message Dian Rachmawati Program Studi Ilmu Komputer Universitas Sumatera Utara. The time that it takes to do encryption is 7.54 seconds, and embedding is 0.67 seconds. The time that it takes to do extraction is 0.43 seconds and decryption is 8.2 seconds. The experimental result by using message Dian Rachmawati. The time that it takes to do encryption is 4.13 seconds, and embedding is 0.65 seconds. The time that it takes to do extraction is 0.41 seconds and decryption is 4.7 seconds.

Other experiments are using various types of pixel image as a cover image to hide string Dian Rachmawati Program Studi Ilmu Komputer Universitas Sumatera Utara. The results have shown in Table 3.
| No. | Pixel   | Cover Image | Stego Image |
|-----|---------|-------------|-------------|
| 1   | 1800 x 1350 | ![Image 1](1800x1350) 7311 KB | ![Image 2](1800x1350) 9761 KB |
| 2   | 900 x 650   | ![Image 3](900x650) 1873 Kb | ![Image 4](900x650) 2437 Kb |
| 3   | 300 x 255   | ![Image 5](300x255) 214 Kb | ![Image 6](300x255) 284 Kb |
| 4   | 75 x 56     | ![Image 7](75x56) 14 Kb | ![Image 8](75x56) 19 Kb |
4. Conclusions
The conclusion of this research is the combination of RSA and FoF able to secure the message by encrypting and hiding, so it is not to arouse suspicion for those who see the image. The combination of both algorithms is also able to restore the message into its original form. In the cover image with large pixel size, the insertion process with FoF is entirely invisible, so the stego image and original image cannot be distinguished, whereas in small pixels there is a black line above the image (the place which the message hide). The time required for encryption and decryption is directly proportional to the length of the message.

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

References
[1] M. Jain, R. C. Choudhary and A. Kumar, Secure medical image steganography with RSA cryptography using decision tree, 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, 2016, pp. 291-295. doi: 10.1109/IC3I.2016.7917977
[2] M. Saritha, V. M. Khadabadi and M. Sushravya, Image and text steganography with cryptography using MATLAB, 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, Odisha, India, 2016, pp. 584-587. doi: 10.1109/SCOPES.2016.7955506
[3] M. Kiviharju, On the fog of RSA key lengths: Verifying public key cryptography strength recommendations, 2017 International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 2017, pp. 1-8. doi: 10.1109/ICMCIS.2017.7956481
[4] K. Somsuk, The improving decryption process of RSA by choosing new private key, 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, 2016, pp. 1-4. doi: 10.1109/ICITEED.2016.7863242
[5] Mollin, R. A. 2002. RSA and Public-Key Cryptography. 2nd Edition. Chapman & Hall/CRC: Florida.
[6] D Rachmawati, A Amalia, and J Surya, Combination of huffman coding compression algorithm and least significant bit method for image hiding, Journal of Physics: Conference Series 801 (2017), no. 1, 012059.