ADI Journal on Recent Innovation (AJRI)
Vol 1 No. 1 September 2019

p-ISSN : 2685-9106
e-ISSN : 2686-0384

The Application of RSA and LSB in Securing Message on Images

Bob Subhan Riza[1], M. Y.Mashor[2], Edy Victor Haryanto S[3]

Universitas Potensi Utama[1,3], University Malaysia Perlis[2]

E-mail : bob.potensi@gmail.com, edyvictor@gmail.com

Author Notification
31 August 2019
Final Revised
01 September 2019
Published
03 September 2019

To cite this document :
Riza, B., Mashor, M., & Haryanto, E. (2019). APPLICATION OF RSA AND LSB IN SECURITY OF MESSAGES ON IMAGERY. *ADI Journal on Recent Innovation (AJRI)*, *1*(1), 20-32. https://doi.org/https://doi.org/10.34306/ajri.v1i1.10

DOI:
https://doi.org/10.34306/ajri.v1i1.10

Abstract

In this study is to discuss cryptography and steganography where the function is to insert a message or text into an image with JPG extension, the text to be inserted into the image has been encrypted using the RSA method so that the file is safer to be inserted into images, messages that are inserted into a blue image, this application aims to secure a message that you want to save, this application is made made using Android Studio and can be run on a mobile phone.

Keywords : Security, Cryptography, Steganography, RSA, LSB

I. Introduction

Currently the development of technology has been very good and very fast and almost human activity is inseparable from the role of technology both for daily work at home or work in the office so that humans really need technology. Therefore the security of the technology used must also be increased, especially in terms of data that utilizes technology so that the data that we store in these technological devices can be protected and safe.

Cryptography is a method for securing data where the data that is secured is converted into a form that has no meaning so that others cannot find out the data. The RSA algorithm is one part of cryptography where RSA uses very difficult calculations to produce encrypted ciphertexts from secured data. It takes a long time to find out the meaning of the original data from a ciphertext from RSA encryption algorithm without knowing the correct key pair. Therefore the RSA algorithm is still the safest cryptographic algorithm to date.

Steganography is the development of cryptographic methods in which steganography hides data into the cover object so that its existence is not known by others. LSB (Least Significant Bit) is one of the steganographic methods that insert data on the last bits of the cover object so that changes before and after the insertion process are not visible to the human senses. This is because the change in value of each pixel on the cover object only increases 1 or decreases by 1 value.

p-ISSN : 2685-9106
e-ISSN : 2686-0384

The combination of cryptography and steganography has been done in previous studies, this shows that the combination has a high level of security so that the development of methods and algorithms is also widely carried out. The combination of RSA and LSB is considered very appropriate because RSA cryptography is the safest algorithm to date and LSB steganography is needed to hide the ciphertext results from RSA cryptography into images so that its presence is unknown to others. [3]

Barkah in his research designed an application in the field of steganography in securing images using the F5 method. [4]

II. METHODE

2.1. Cryptography

Cryptography (cryptography) comes from Greek: "cryptos" means "secret" writing "Cryptography is defined as the science and art of maintaining the confidentiality of messages by encoding them into a form that cannot be understood anymore. Cryptography has two concepts The main thing is encryption and decryption Encryption is the process of encoding plaintext into ciphertext, whereas decryption is the process of returning ciphertext to the original plaintext Encryption and decryption require keys as parameters used for transformation.

Cryptography is divided into 2 (two), namely:

1. Classic cryptography (character mode):
   - Cipher Substitution
   - Transposition Cipher
2. Modern cryptography (bit / binary mode):
   - Symmetry key ciphers: stream ciphers, block ciphers
   - Public key cryptography [1.]

2.2. RSA

In 1977, Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman formulated a practical algorithm that implements a public-key cryptographic system called the RSA cryptographic system. The pair of keys used in both processes are the public key (e, n) as the encryption key and the private key as the decryption key where e, d and n are positive integers. The RSA algorithm is a block cipher algorithm (an algorithm that works per block of data) which groups plaintext into blocks before encryption is made to ciphertext [2]

III. RESULT AND DISCUSSION

In the RSA cryptographic process, input the message as a plaintext is ASCII characters that is 255 characters. The results obtained from the encryption process are ciphertext in the form of decimal values generated from the calculation of the RSA algorithm encryption formula. After the ciphertext is obtained it is converted into a binary form which will then be inserted in each pixel cover object in the form of an RGB image, in this case a blue pixel. Image image used in the format * .jpg with image

p-ISSN : 2685-9106
e-ISSN : 2686-0384

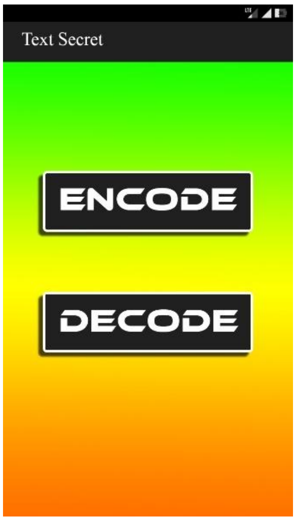

Figure 1. Main Menu Layout

In the main menu layout of the application, the user can choose a menu on the application for further processing by the system. There are 2 main menus, namely the encode menu which will encrypt the message which is then inserted into the image image, and the decode menu which will extract the message from the image that produces the ciphertext and then decrypt it using the RSA algorithm that produces a plaintext in the form of the original message. The following encoding menu layout can be seen in Figure 2 :

Figure 2. Layout Menu Encode

In the encode menu the user can encrypt and insert messages where as an example of this research, the message used is "Great Indonesia". The first step the user must first select the cover object that will be used by clicking on the Image button, the system will open the system gallery that will display images across all user devices. After the cover object is selected, then the next generation of key pairs by entering two primes that are not the same value, in this study used the values of 43 and 47, the following is a manual key generation calculation :

a. Search value n :
   n = p x q
   = 43 x 47
   = 2021
b. Search value Θn :
   Θn = (p-1) x (q-1)
   = (43-1) x (47-1)
   = (42) x (46)
   = 1932
c. Search value e :
   e = 2
   *While Θ*n mod e ≠ 0
   e = e + 1
   End While
   Proses 1 :
   Θn mod e = 1932 mod 3= 0
   e = 3 + 1
   e = 4
   Proses 2 :
   Θn mod e = 1932 mod 4
   = 0
   e = 4 + 1
   e = 5
   Proses 3 :
   Θn mod e = 1932 mod 5
   = 2
   e = 5
d. Search value d :
   U1 = 1
   U2 = 0
   U3 = Θn
   V1 = 0
   V2 = 1
   V3 = e
   While V3 = 0
   Q = Int(U3 / V3)
   N1 = U1 - (Q x V1)
   N2 = U2 - (Q x V2)
   N3 = U3 - (Q x V3)
   U1 = V1
   U2 = V2
   U3 = V3
   V1 = N1
   V2 = N2
   V3 = N3
   End While

Process 1:
Q = Int(U3 /V3)
= Int(1932 /5)
= 386
N1 = U1 - (Q x V1)
= 1 - (386 x 0)

= 1
N2 = U2 - (Q x V2)
= 0 - (386 x 1)
= -386
N3 = U3 - (Q x V3)
= 1932 - (386 x 5)
= 1932 - 1930
= 2
U1 = 0
U2 = 1
U3 = 5
V1 = 1
V2 = -386
V3 = 2

Process 2:

Q = Int(U3 /V3)
= Int(5 / 2)
= 2
N1 = U1 - (Q x V1)
= 0 - (2 x 1)
= -2
N2 = U2 - (Q x V2)
= 1 - (2 x - 386)
= 773
N3 = U3 - (Q x V3)
= 5 - (2 x 2)
= 5 - 4
= 1
U1 = 1
U2 = -386
U3 = 2
V1 = -2
V2 = 773
V3 = 1

Process 3:

Q = Int(U3 /V3)
= Int(2 / 1)
= 2
N1 = U1 - (Q x V1)
= 1 - (-2 x -3)
= 5
N2 = U2 - (Q x V2)
= -386 - (2 x 773)
= -1932
N3 = U3 - (Q x V3)
= 2 - (2 x 1)
= 0
U1 = -2
U2 = 773
U3 = 2
V1 = 5
V2 = -1932
V3 = 0

After the calculation process, the RSA algorithm's key pair is obtained with the value. Then the encryption process is then performed by changing the original messange into the ciphertext with manual calculations as follows :

Ci = Pie mod n
Ci = Cipherteks
Pi = Plainteks
e = Nilai kunci e
n = Nilai kunci n

Enkripsi Pertama :
I = 73
Ci = Pie mod n
= 735 mod 2021
= 2073071593 mod 2021
= 528

Enkripsi Kedua :
n = 110
Ci = Pie mod n
= 1105 mod 2021
= 16105100000 mod 2021
= 1604

Enkripsi Ketiga :
d = 100
Ci = Pie mod n
= 1005 mod 2021
= 10000000000 mod 2021
= 1055

Enkripsi Keempat :
o = 111
Ci = Pie mod n
= 1115 mod 2021
= 16850581551 mod 2021
= 927

Enkripsi Kelima :
n = 110
Ci = Pie mod n
= 1105 mod 2021
= 16105100000 mod 2021
= 1604

Enkripsi Keenam :
e = 101
Ci = Pie mod n
= 1015 mod 2021
= 10510100501 mod 2021
= 1156

Enkripsi Ketujuh :
s = 115
Ci = Pie mod n
= 1155 mod 2021
= 20113571875 mod 2021
= 1869

Enkripsi Kedelapan :
i = 105

Ci = Pie mod n
= 1055 mod 2021
= 12762815625 mod 2021
= 546

Enkripsi Kesembilan :
a = 97
Ci = Pie mod n
= 975 mod 2021
= 8587340257 mod 2021
= 102

Enkripsi Kesepuluh :
[space] = 32
Ci = Pie mod n
= 325 mod 2021
= 33554432 mod 2021
= 1790

Enkripsi Kesebelas :
H = 72
Ci = Pie mod n
= 725 mod 2021
= 1934917632 mod 2021
= 106

Enkripsi Ketigabelas :
e = 101
Ci = Pie mod n
= 1015 mod 2021
= 10510100501 mod 2021
= 1156

Enkripsi Keempatbelas :
b = 98
Ci = Pie mod n
= 985 mod 2021
= 9039207968 mod 2021
= 507

Enkripsi Kelimabelas :
a = 97
Ci = Pie mod n
= 975 mod 2021
= 8587340257 mod 2021
= 102

Enkripsi Keenambelas :
t = 116
Ci = Pie mod n
= 1165 mod 2021
= 21003416576 mod 2021
= 270

The encoding process is continued by inserting the RSA encryption algorithm results intothe blue pixel cover object, where the encrypted cipher text is added with the character "|" as a delimiter between words to facilitatethe process of decryption later. The ciphertext after adding

a delimiter is “5 2 8 1 2 4 1 6 0 4 1 2 4 1 0 5 5 1 2 4 9 2 7 1 2 4 1 6 0 4 1 2 4 1 1 5 6 1 2 4 1 8 6 9 1 2 4 5 4 6 1 2 4 1 0 2 1 2 4 1 7 9 0 1 2 4 1 0 6 1 2 4 1 1 5 6 1 2 4 5 0 7 1 2 3 1 0 2 1 2 3 2 7 0” the system will change the cover object to RGB where the system will use the pixel blue value as a medium to insert the ciphertext. Here is an example of insertionin a blue pixel :
After the calculation process, the RSA algorithm’s key pair is obtained with the value. Then the encryption process is then performed by changing the original message into the ciphertext with manual calculations as follows:

44	39	48	47	98	19	19	17
66	67	13	13	38	39	39	22
66	68	65	49	48	48	50	50
90	67	66	13	13	21	21	23
90	12	12	12	11	30	30	31
91	12	13	13	22	22	23	50

Table 3. Pieces of RGB pixel image value

After getting the cover object’s RGB value, the system will separate it into 3 parts and only use one part, the blue pixel segment. The Following results are the separation of image pixel value :

48	47	98	19
13	13	38	39
65	49	48	48
66	13	13	21
12	12	11	30
13	13	22	22

Table 4. Pieces of blue pixel image

The result of the separation of image pixels is then converted into a binary form to do the insertion process in the image. The conversion results can be seen in the following table :

00110000	00101111	01100010	00010011
00001101	00001101	00111000	00111001
00110101	00110001	00110000	00110000
00110110	00001101	00001101	00100001
00001100	00001100	00001011	00011000

p-ISSN : 2685-9106
e-ISSN : 2686-0384

00001101	00001101	00010010	00010010

Table 5. Conversion of image pixel values

The next process is to change the message binary form, for eexample the message is “RSA” and converted to binary to "010100100101001101000001". The following is the result of inserting the message into the cover object.

00110000	00101111	01100010	00010011
00001100	00001100	00111001	00111000
00110100	00110001	00110000	00110001
00110110	00001100	00001101	00100001
00001100	00001101	00001010	00011000
00001100	00001100	00010010	00010011

Table 6. Results for inserting messages in blue pixels

After the process is complete, the system will store the cover object in storage and the system will display a dialog that "The message was successful in Encode”

Gambar 3. *Layout* Menu Decode

In the decode menu layout, the system will extract the cover object that has been inserted image by changing the image into the RGB form. The image is converted into the RGB form and then the value of each pixel is taken, thefollowing is the value of the pixel image:

44	39	48	47	98	19	19	17
66	67	12	12	57	56	39	22

 p-ISSN : 2685-9106
e-ISSN : 2686-0384

66	68	52	49	48	49	50	50
90	67	54	12	13	33	21	23
90	12	12	13	10	24	30	31
91	12	12	12	18	19	23	50

Table 7. RGB image values

After getting the RGB image value, the system will take the blue pixel value that has been pasted in the encoding process, the blue pixel value can be seen as follows :

48	47	98	19
12	12	57	56
52	49	48	49
54	12	13	33
12	13	10	24
12	12	18	19

Table 8. Blue pixel values

The blue pixel value is then converted to a binary number so that the last bits of the pixel can be taken as a secret message. Here are the results of the conversion of blue pixel values into binary forms:

00110000	00101111	01100010	00010011
00001100	00001100	00111001	00111000
00110100	00110001	00110000	00110001
00110110	00001100	00001101	00100001
00001100	00001101	00001010	00011000
00001100	00001100	00010010	00010011

Table 9. Results of blue pixel conversio

After being converted, every last bit of pixel is taken and put together to form a message Following is the process of taking the last bit of pixel:

00110000	00101111	01100010	00010011

p-ISSN : 2685-9106
e-ISSN : 2686-0384

00001100	00001100	00111001	00111000
00110100	00110001	00110000	00110001
00110110	00001100	00001101	00100001
00001100	00001101	00001010	00011000
00001100	00001100	00010010	00010011

Table 10. The process of extracting pixel bits

Then the binary message will be obtained as follows "010100100101001101000001" which if converted will produce the message "RSA". Furthermore, the system will perform the decryption process by changing the encrypted ciphertext into a plaintext again by using the key pairs and values which were first raised in the previous encryption process. For example there is a ciphertext which is "5 2 8 1 2 4 1 6 0 4 1 2 4 1 0 5 5 1 2 4 9 2 7 1 2 4 1 6 0 4 1 2 4 1 1 5 6 1 2 4 1 8 6 9 1 2 4 5 4 6 1 2 4 1 0 2 1 2 4 1 7 9 0 1 2 4 1 0 6 1 2 4 1 1 5 6 1 2 4 5 0 7 1 2 4 1 0 2 1 2 4 2 7 0 ", The decryption process will be carried out with keys n and d, namely 2021 and 773. First the ciphertext is separated from the character marker" **|** "to get the results of the character, then after the separation, the ciphertext "
Pi = Cid mod n
Pi = Plainteks
Ci = Cipherteks
d = Nilai d
n = Nilai n

Then the result of the calculation is that Pi, which is an ASCII decimal value, is converted to ASCII characters so that the plaintext can be read again.

Dekripsi Pertama :
Ci = 528
Pi = Cid mod n
= 528773 mod 2021
= 3,9447739231444509389840801901531e+2104 mod 2021
= 73 = **I**

Dekripsi Kedua :
Ci = 1604
Pi = Cid mod n
= 1604773 mod 2021
= 4,1973320925821901822743614620265e+2477 mod 2021
= 110 = n

Dekripsi Ketiga :
Ci = 1055
Pi = Cid mod n
= 1055773 mod 2021
= 9,4221778343004045568524043277723e+2336 mod 2021
= 100 = d

Dekripsi Keempat :
Ci = 927
Pi = Cid mod n
= 927773 mod 2021

p-ISSN : 2685-9106
e-ISSN : 2686-0384

= 3,5697228047878728461382284266697e+2293 mod 2021
= 111 = o

Dekripsi Kelima :
Ci = 1604
Pi = Cid mod n
= 1604773 mod 2021
= 4,1973320925821901822743614620265e+2477 mod 2021
= 110 = n

Dekripsi Keenam :
Ci = 1156
Pi = Cid mod n
= 1156773 mod 2021
= 4,6388010556934147413077372755344e+2367 mod 2021
= 101 = e

Dekripsi Ketujuh :
Ci = 1869
Pi = Cid mod n
= 1869773 mod 2021
= 8,9947679931588830717146802446832e+2528 mod 2021
= 115 = s

Dekripsi Kedelapan :
Ci = 546
Pi = Cid mod n
= 546773 mod 2021
= 7,0780367100126994994633255938O6e+2115 mod 2021
= 105 = i

Dekripsi Kesembilan :
Ci = 102
Pi = Cid mod n
= 102773 mod 2021
= 4,4456244464174792567180261019521e+1552 mod 2021
= 97 = a

Dekripsi Kesepuluh :
Ci = 1790
Pi = Cid mod n
= 1790773 mod 2021
= 7,1731821553698319681336017738364e+1341 mod 2021
32 = [space]

Dekripsi Kesebelas :
Ci = 106
Pi = Cid mod n
= 106773 mod 2021
= 3,6427876007855229645751636756921e+1565 mod 2021
= 72 = H

Dekripsi Keduabelas :
Ci = 1156
Pi = Cid mod n
= 1156773 mod 2021

p-ISSN : 2685-9106
e-ISSN : 2686-0384

= 4,6388010556934147413077372755344e+2367 mod 2021
= 101 = e

Dekripsi Ketigabelas :
Ci = 507
Pi = Cid mod n
= 507773 mod 2021
= 9,3573433346090832334487836909454e+2090 mod 2021
= 98 = b

Dekripsi Keempatbelas :
Ci = 102
Pi = Cid mod n
= 102773 mod 2021
= 4,4456244464174792567180261019521e+1552 mod 2021
= 97 = a

Dekripsi Kelimabelas :
Ci = 270
Pi = Cid mod n
= 270773 mod 2021
= 2,7809276801454902544239942650756e+1879 mod 2021
= 116 = t

The results of the decryption process above produced a text which means "Great Indonesia". From the results of manual calculations and those produced by the system, there are no significant differences. Therefore RSA and LSB cryptography on the red pixel was successfully processed by the system.

V. ACKNOWLEDGMENT

From the encryption, decryption, embedded, and extraction processes that are running well, the researchers concluded that:

1. The combination of cryptographic RSA algorithm techniques and LSB method steganography techniques is able to maintain the confidentiality of messages because the presence of messages is difficult to know thanks to the LSB method that inserts messages into image images. And also the difficulty of knowing the original message without having an RSA key pair.
2. Insertion of messages successfully on image images with * .jpg format and at 3888x2592 resolution.

VI. ADVICE

In this research, it still has shortcomings under weaknesses that can be developed for subsequent research. Suggestions for future research are as follows:

1. Does not show RSA encryption results in the form of ciphertext making it difficult to compare calculations manually.
2. Researchers can develop programs using Android bass programming
3. Prime numbers still need to be entered manually, in the next research, random primers can be added.

p-ISSN : 2685-9106
e-ISSN : 2686-0384

REFERENCES

[1] Rakhmat, B., & Fairuzabadi, M. (2010). Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenère Dan Rc4. *Jurnal Dinamika Informatika*, *5*(2), 1-17.

[2] Alvianto, A. R., & Darmaji, D. (2015). Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android. *Jurnal Sains dan Seni ITS*, *4*(1), A1-A6.

[3] Arif, M. H., & Fanani, A. Z. (2016). Kriptografi Hill Cipher dan Least Significant Bit untuk Keamanan Pesan pada Citra. *CSRID (Computer Science Research and Its Development Journal)*, *8*(1), 60-72.

[4] Akbar, M. B., & Haryanto, E. V. (2018). Aplikasi Steganografi dengan Menggunakan Metode F5. *JUSITI: Jurnal Sistem Informasi dan Teknologi Informasi*, *4*(2), 165-176.

[5] Rambe, M. R., Haryanto, E. V., & Setiawan, A. (2018). Aplikasi Pengamanan Data dan Disisipkan Pada Gambar dengan Algoritma RSA Dan Modified LSB Berbasis Android. *Konferensi Nasional Sistem Informasi (KNSI) 2018*.

[6] Haryanto, E. V., & Utama, U. P. (2012). Jaringan Komputer. Penerbit Andi.

[7] Haryanto, E. V. (2015). Penerapan Metode Adaptif Dalam Penyembunyian Pesan Pada Citra. Proceedings Konferensi Nasional Sistem dan Informatika

[8] Haryanto, E. V. (2015). Perbandingan Metode Robinson 5 Level Dan Prewit Dalam Mendeteksi Tepi Citra Digital. *Proceedings Konferensi Nasional Sistem dan Informatika (KNS&I)*. (KNS&I).