Proceeding of International Conference on Green Technology
Vol.8, No.1, October 2017 Page 33-37
p-ISSN: 2580-7080 | e-ISSN: 2580-7099

Hybrid Algorithm with Super Encryption of Medical Record Image Data

Muhammad Khudzaifah, Muhamad Wais Al Qorny, Hawzah Sa'adati
Departement of Mathematics,UIN Maulana Malik Ibrahim Malang

Article Info

Article history:

Received Jul 12th, 2017
Revised Aug 20th, 2017
Accepted Oct 26th, 2017

Keyword:

Medical Record
Image Data
Encryption
Decryption
Hybrid Algorithm

ABSTRACT

In the technology information, security becomes very important to secure data. One of the most secret data and needs to be secured is medical record data in the form of an image. The method that can be used to secure it is a cryptographic algorithm. There are two cryptographic algorithm that can be used to secure medical record data that is symmetric and asymmetric. Symmetric algorithm fast in the process of encryption and decryption, but less secure in the key, while asymmetry slow in process of encryption and decryption, but safe with the key. To get an efficient result, the used hybrid algorithm, that is symmetric algorithm for process of encryption and decryption, while the key is secured with asymmetric algorithms. In this research, the symmetric algorithm uses super encryption (affine cipher and transformation), while the asymmetric algorithm uses RSA algorithm. The result obtained are the process of encryption and decryption need a short tme and the security of the key more increased.

Corresponding Author:

First Author,
Departement of Mathematics,
UIN Maulana Malik Ibrahim Malang,
Jl. Gajayana No. 50 Malang, Jawa Timur, Indonesia 65144
Email: khudzaifah@uin-Malang.ac.id

1. INTRODUCTION

Security issues an important aspect of the development of imformation technology, one of the as a security to secure data. In the medical world, medical records are very secret and sensitive information. As the development of technology information, the medical record is not only a data but including an image. To maintain the security of medical record in the form of image data, it is necessary to use a secure algorithm, using cryptograpy method.

In cryptograpy there are two very important algorithm, namely the symmetric algorithm and the asymmetric algorithm. The symmetric algorithm is excellent because it is fast in the process of encryption and decryption , but has a weakness in the key, while the asymmetric algorithm has weakness because it is slow in the process of encryption and decryption but excel in the key [1], [7].

Application in the encryption and decryption of medical ricord in the form of image data, symmetric algorithm is very appoprite because the process is fast but weak in the key. While the data from the medical record is very secret. If implemented asymmetric algorithm, then tha data is more secure because the key is strong but slow in the process of encryption and decryption. To overcome these problems, then used a combination of symmetric algorithm and asymmetric algorithm called hybrid algorithm [1].

Tosecure medical record in the form of image data, the encyption and decryption process using super encryption algorithm (affine cipher and transformation), while the weak key is secured using asymmetric algorithm, that is RSA algorithm. Although using symmetric algorithm, but its key security is increasing, so medical record in the form of image data hightly secret can be maintained its security.

Discussion of medical records can be seen in books made by Sjamsuhidajat [9]. For discussion of

number theory can be seen in the book made by Irawan [2]. For a discussion of the matrix can be seen in the book made by Lipschutz [5]. While for the discussion of cryptography, especially on the topic of symmetry algorithms, asymmetry algorithms, and hybrid algorithms can be seen in books compiled by Ariyus [1], Kromodimoeljo [4], Mollin [6], Munir [7], Setyaningsih [8] and stalings [10]. Research on hybrid algorithm has been done by Khudzaifah [3].

2. RESEARCH METHOD

The method used in this research is described in the form of literature research and simulation. The steps in this research is to combine the two algorithms, super encryption (affine cipher and transformation) and RSA, and apply them to the medical record in the form of image data, as well as create the program of super encryption algorithm, image on medical record.

As for the steps in this research is:

1. Create public key and private key of RSA algorithm.
2. Create session key of the affine cipher algorithm.
3. Make plaintext in the form of image data.
4. Encrypt plaintext image data with session key to be ciphertext.
5. Encrypt session keys with public key.
6. Decrypt, encrypted session key, with private key.
7. Decrypt the ciphertext with session key to plaintext.

3. RESULTS AND ANALYSIS

In this chapter the author will first describe the process of encryption and decryption plain text, image using super encryption algorithm (affine cipher and transformation). Then construct a hybrid algorithm (super encryption and RSA) applied to the program of encryption process and decrypt medical record in the form of image data.

3.1. Encryption and Decryption Plaintext Image Data

To perform the process of encryption and decryption need to be made the key fist and then followed by the process of encryption and decryption.

Encryption Algorithm

1. Select an integer a and b.
2. Create a plaintext image data and change it to a number on the square matrix P.
3. Calculate the matrix $C_1 \equiv Pa + b \pmod{m}$.
4. Transformation (permutation) of matrix C_1 with rotation from key b to ciphertext C_2.
5. Obtained ciphertext C_2.

Decryption Algorithm

1. Find the inverse of $a \pmod{m}$ or a^{-1}.
2. Transformation (permutation) ciphertext C_2 with rotation from key b to matrix C_1.
3. Calculate the matrix $P \equiv a^{-1}(C_1 - b) \pmod{m}$.
4. Change the number in the square matrix P in the image data.
5. Retrieved plaintext image data.

3.2. Hybrid Algorithm Construction (Super Encryption and RSA)

To perform the encryption and decryption process needs to be made the key first and then followed by the process of encryption and decryption. In order to easily understand the illustration is made as follows:

1. Patient generates public key and private key of RSA algorithm. After the public key is obtained, the patient sends the key to the doctor.
2. Doctors generate session keys from the affine cipher algorithm. Then the physician makes the plaintext image and converted into a number in the square matrix P. The doctor encrypts the square matrix P uses the super encryption algorithm to generate the ciphertext and encrypts the session key using the RSA algorithm with the public key. After obtaining the encrypted session key, then sent to the patient.
3. The patient decrypts the key of the doctor using the RSA algorithm with the private key. After obtaining the session key the patient decrypts the ciphertext using the super encryption algorithm to generate the square matrix P.The number in the square matrix P is then converted to image data form. The end result obtained makes plaintext the image of the doctor to patient.

Mathematically explained as follows:

1. The patient chooses large prime number p and q (p should not be equal to q).
2. Patients compute n and $\phi(n)$ with $n = pq$ and $\phi(n) = (p-1)(q-1)$.
3. The patient takes the integer e such that it is relatively primed with $\phi(n)$ or fpb$\big(e, \phi(n)\big) = 1$.
4. Patient count d with $d = \frac{1+k\phi(n)}{e}$. Thus there is integers k that gives integers d.
5. The patient gets the public key and private key (e, n) and (d, n). Then the patient sends the public key (e, n) to the doctor.
6. Doctors choose two integers a and b.
7. The doctor makes the plaintext image data and converted into a number in the square matrix P.
8. The doctor encrypts P using the super encryption algorithm $C_1 \equiv Pa + b \pmod m$ (affine cipher) and proceeds the transformation (permutation) matrix C_1 with turnaround to C_2.
9. Doctors encrypt session keys (a and b) using RSA algorithms with public key (e, n) that is $a_c \equiv a^e \pmod n$ and $b_c \equiv b^e \pmod n$. After the encrypted session key is encrypted that is a_c and b_c then the doctor sends ciphertext C_2 and encrypted session key a_c and b_c to the patient.
10. After obtaining ciphertext C_2 and encrypted session key a_c and b_c from a doctor then the patient does the decryption process.
11. The patient decrypts the encrypted session key a_c and b_c to obtain the original session key (a and b) using the RSA algorithm with the private key (d, n) that is $a \equiv {a_c}^e \pmod n$ and $b \equiv {b_c}^e \pmod n$. Then obtained the original session key is a and b.
12. Before decrypting the patient looks for the inverse value of a or a^{-1}) in order to perform the decryption. After getting a^{-1} the patient decrypts the ciphertext C_2 using the super encryption algorithm that is the transformation (permutation) first ciphertext C_2 with turnover to C_1 and followed by $P \equiv a^{-1}(C_1 - b) \pmod m$. Having obtained the square matrix P change the number in the square matrix P into the image data. The patient's final result obtained medical record data from the doctor.

3.3. Results of Encryption and Decryption of Plaintext Image

To obtain image data from the doctor, the patient needs to generate the public key from the RSA first. Once the public key is obtained, the key is sent to the doctor so that the key security will be sent to the patient safe patient. To obtain a public key select any prime p and q, in this example we selected $p = 47$ and $q = 71$, as in Figure 1.

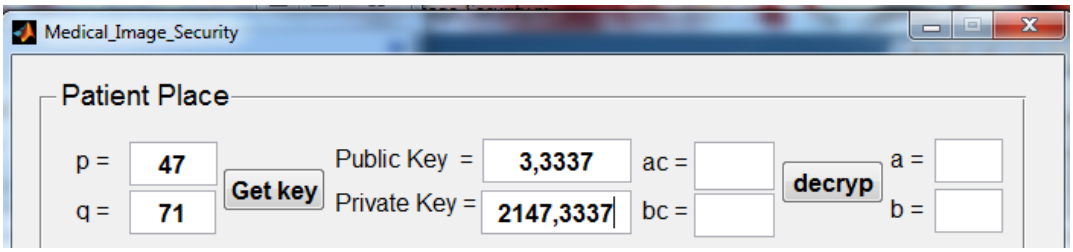

Figure 1. Display program to generate public key

After the public key is sent to the doctor, the physician encrypts the image data using a super encryption algorithm (affine cipher and transformation) and encrypts the session key with a public key. To encrypt the image data then take the image file first and then select any number a and b. After the key and image data obtained next is the data encryption process and encrypted the results obtained as in Figure 2.

 p-ISSN: 2580-7080 | e-ISSN: 2580-7099

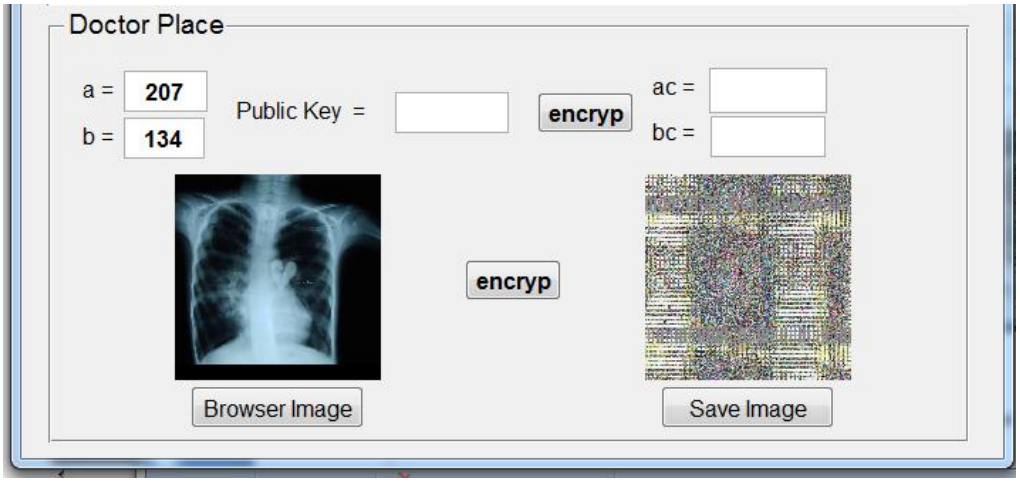

Figure 2. Image data encryption process

After encrypting the image data further encrypts the key to be safe when sent to the patient. To encrypt the session key then using the public key encrypted session key as shown in Figure 3.

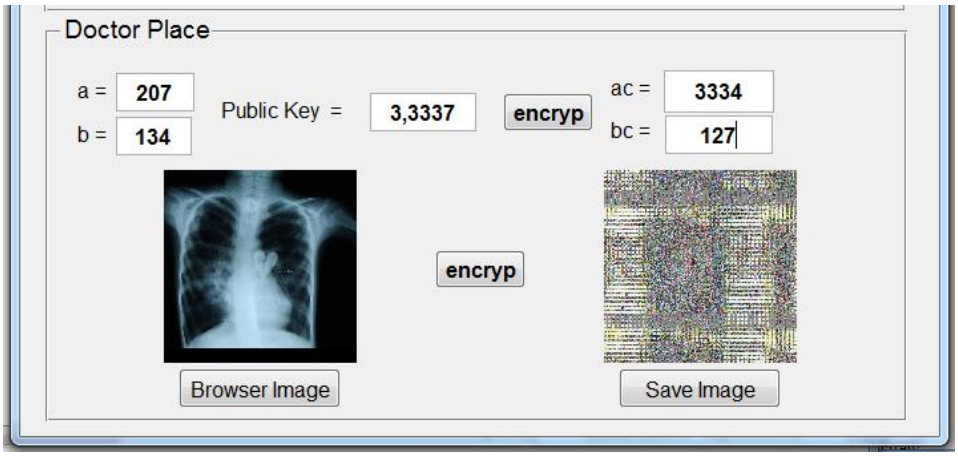

Figure 3. The session key results are encrypted

After image data and encrypted session key is sent to the patient. before the patient decrypts the data, then it must decrypt the encrypted session key first. To obtain the session key the private key is used and the session key is obtained as shown in Figure 4.

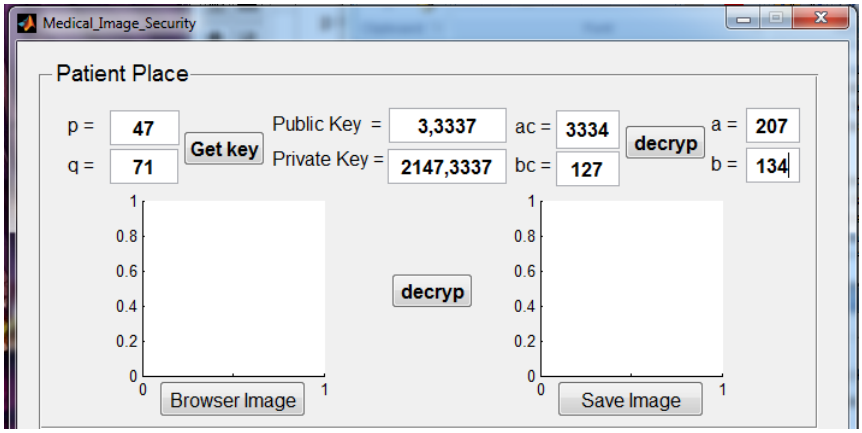

Figure 4. Decryption process encrypted session key generates session key

For the last process is to decrypt the image data. Previously the patient took the image data sent by the doctor then then the data decryption process and obtained the original image data as in Figure 5.

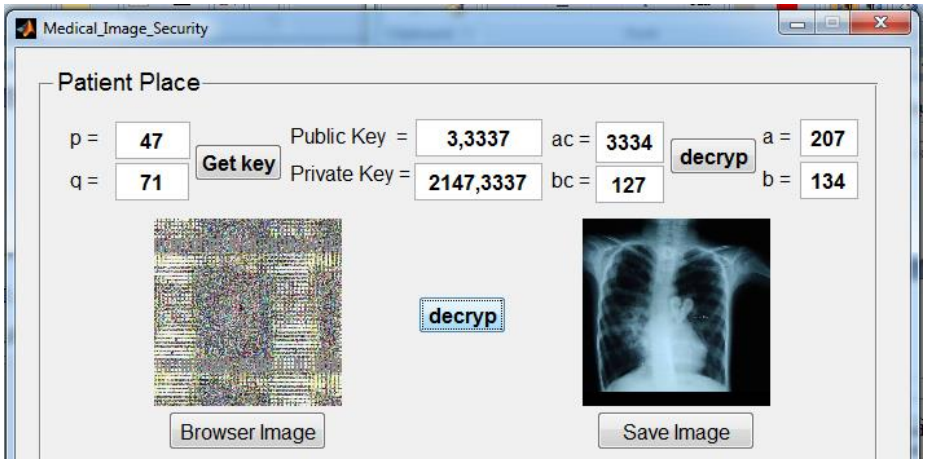

Figure 5. The final result of the image data decryption process

4. CONCLUSION

From the results and analysis above can be concluded that to secure the medical record in the form of image data can use cryptography method. To strengthen the security, then used hybrid algorithm that the result of plaintext and the session key become encrypted. By using super encryption algorithm (affine cipher and transformation) generated a very random image cipher. When the cipher and encrypted key are sent then it can only be decrypted with the private key to find out the session key used to decrypt the cipher.

REFERENCES

[1] Ariyus D. Pengantar Ilmu Kriptografi. Jogjakarta: Andi, 2008.

[2] Irawan WH, Hijriyah N, & Habibi AR. Pengantar Teori Bilangan. Malang: UIN-MALIKI Press, 2014.

[3] Khudzaifah M. Aplikasi QuasiGroup Dalam Pembentukan Kunci Rahasia Pada Algoritma Hibrida (RSA-QuasiGroup Chiper), Cauchy, vol. 3, no. 2, pp. 55-58, 2014.

[4] Kromodimoeljo S. Teori dan Aplikasi Kriptografi. Jakarta: SPK IT Consuling, 2010.

[5] Lipschutz S & Lipson ML. SCHAUM'S outlines Linear Algebra Fourth Edition. New York: McGraw-Hill Companies, Inc, 2009.

[6] Mollin RA. An Introduction to Cryptography Second Edition. London: CRC, 2007.

[7] Munir R. Sistem Kriptografi Kunci-Publik. Diktat Kuliah. Bandung: Departemen Teknik Informatika Institut Teknologi Bandung, 2004.

[8] Setyanigsih E. Kriptografi dan Implementasinya Menggunakan Matlab. Jogjakarta: Andi Publisher, 2015.

[9] Sjamsuhidajat AS. Manual Rekam Medis. Jakarta: Konsil Kedokteran Indonesia, 2006.

[10] Stallings W. Cryptography and Network Security Fourt Edition Principles and Practices. New Jersey: Prentice Hall, 2005.