Contemporary Mathematics and Applications
Vol. 2, No. 1, 2020, pp. 109-117.

Encryption and Decryption Application on Images with Hybrid Algorithm Vigenere and RSA

Radifan Darari[1], Edi Winarko[1,*] & Auli Damayanti[1]

[1]Mathematics Department, Faculty of Science and Technology, Universitas Airlangga

[*]Corresponding author: edi_winarko@fst.unair.ac.id

Abstract. Digital image is digital pictures on a two-dimensional plane which consists of pixels, where every pixels has *Red, Green, Blue* (RGB) with varying intensity depending on the image. In this thesis digital image is encrypted using *hybrid* algorithm Vigenere and RSA. Vigenere algorithm is a symmetric key algorithm which is a variety from Caesar algorithm where the similarity is in both of them are based on shifting the index of alphabet letters. RSA algorithm are based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). The encryption process starts with getting the RGB intensity of each pixels from the image, then the RGB values are encrypted using Vigenere algorithm, after that RSA Algorithm encrypt those values, the values of RSA Algorithm encryption are limited so the value can be within the intervals of RGB values and the after limitation the values after being limited become the RGB values in the encrypted image. The decryption process is the inverse of encryption process, which enables the encrypted image to become the initial image before encryption. The program for encrypting and decrypting image are made using Java programming language with Netbeans IDE 8.2 software. The result of this implementation on image file *donbass.jpg* with the length of Vigenere key of 5 those are k1=144, k2=166 , k3=38 , k4=204 , k5=98, and RSA Algorithm keys are n=2201, e=1139, d=59, the results from the encrypted image is a visually very different image from the initial image. While in the decryption process, the encrypted image is able to be decrypted back to the initial image.

Keywords: *digital image, digital picture, RSA algorithm, Vigenere algorithm.*

1 Pendahuluan

Rapid development in the field of information technology over the last 10 years and have reached a wider public use. Directly o not, information technology has become an important part in many areas of life such as Cloud Computing in IT and bioinformatics in biology. The ease offered by information technology enables communication and exchanging information becoming easier. One such thing is a Social Networking Service (SNS), which is generally referred to as social media and is often used as a platform to exchange information. Many SNS providers often offer a feature of which sending messages in the form of images between its users is possible. Thus the SNS developers need a method to ensure the security of the data exchanged within it. Data security is required to ensure the privacy of users, especially if the data is being exchanged in a

computer network that is not necessarily secure. Loss or leakage of user data could be detrimental to the mental health and material of its victim [1]. It certainly raises the risk of undesirable outcomes if a private or sensitive valuable information accessed by third parties that are not desirable.

Information security against unwanted party has been a concern for centuries. Modern communication techniques using computers connected in a network, creates a new threats thus makes it more vulnerable to the threats that are exist [2]. Data can be secured with the use of cryptography to encrypt and decrypt the data. Cryptographic algorithms generally fall into two category which are symmetric key algorithms and asymmetric key [3]. Symmetric key algorithms use the same key between the sender and its recipient. As for asymmetric algorithms use a public key and a secret key to encrypt and decrypt the data [4]. Digital information often use pictures as a medium to communicate. A picture itself is a collection of pixels that have different intensity of color values [5].

One of the many vulnerable information often hacked is an image file. Research on the images security using Vigenere algorithm has been done before by [6], Vigenere algorithm itself is a variation of the Caesar algorithm. Vigenère algorithm uses a series of Caesar algorithms for its encryption and decryption. This method is called shift-cipher in which each plaintext is shifted as much as the existing key just like Caesar Cipher the difference is in its where Vigenère keys are often times plural [7]. Other studies using the RSA algorithm has been done by [8]. RSA Security has so far proved to be secure because there has been no successful trial to effectively break into the RSA algorithm using a classical computer, but with quantum computers and potentially eliminating RSA algorithm security using Shor's algorithm [9]. RSA algorithms security lies in the difficulty of factorizing large prime number n = pq, where p and q are large prime numbers with a classical computer [10].

Improving secureness of messages can be done by hybrid algorithm. Hybrid Algorithm aims to combine the advantages of each algorithm while simultaneously reducing the weaknesses of each algorithm. Research has been done by [11] is called a hybrid of Vigenere and RSA algorithm for 8-bit bitmap file. In general, the advantages of hybrid algorithm are commonly on the computing speed and accuracy of the results [12].

Based on above, it is interesting to apply the Hybrid RSA and Vigenere algorithms to encrypt and decrypt files such as JPG and PNG images. So that it can provide security for digital images.

2 Digital Image

Digital image is a data containing pixels. Each pixels refers to the color intensity or gray level for black and white image on each point of an image, so that each pixel is a small

dot of containging color. In short is that a digital image is a set of pixels arrays in a square shape [13].

2.1 Pixel

Pixel is an abbreviation of (picture elements). Each pixels has varieties of color intensity. Pixel is the smallest element of an image, so that a collection of pixels forms an image. For black and white image of each pixel has a value corresponding to the gray level of an image of a particular location in the image. In general there are 256 levels of gray in the image. As for the color image for each pixel has three values corresponding to the level of RGB (red, green, blue) to form a color. With each color has 256 levels for each RGB component [13].

2.2 Resolution

The more points that are taken from an image, the more detail an image produced. The density of pixels in an image is called as resolution. The higher the resolution, the more information there is on the image. If the image remains the same size and resolution is increased, the image will be sharp and detailed. Another way is with increasing its resolution the image size can also be increase to get the same sharpness and detail [13].

2.3 Digital Image Classification

There two classification of digital images:

a. Binary Image
   Only complains binary image using one bit for each pixel. Because one bit only exists in two states on or off, then each pixel of a binary image must be of one of two colors white and black.
b. Color Image
   Color images have color variations as much as 16,777,216 colors, and are obtained from the RGB values where each component has 256 levels of color [13].

3 Vigenere Algorithm

Vigenere algorithm is a method of encrypting alphabetic text by using a series consisting of Caesar ciphers based on the letters of a keyword, so often time using a Vigenere table or tabula recta as a quick way to encrypt and decrypt the Vigenere algorithm. The algorithm itself is a simple substitution polyalphabetic [14].

3.1 Vigenere Algorithm Process

The key consists of a series of letters that make up keywords. We encode each letter A, B, ..., Z with the numbers 0, 1, ..., 25, consistenly, the encryption process is done by adding each index of the plaintext letter with its corresponding key. The encryption process of Vigenere algorithm written mathematically as follows:

$$C_i = E(P_i) = (P_i + k_j) mod\ 26 \quad (1)$$

where C is the ciphertext, k is the key, E is an encryption function, and P is plaintext, i is the index of the messages and j is the length of the key.

Vigenere algorithm decryption process by keyword k (in this case k is the same keyword used for encryption and decryption), this can be written as follows:

$$P_i = D(C_i) = (C_i - k_j) mod\ 26 \quad (2)$$

where C is the Ciphertext, k is the key, D is a decryption function, and P stands for Plaintext.

3.2 Vigenere Implementation on Image

Cryptographic process in the image is done by encoding the RGB index, whereas the Vigenere algorithm we encode letters of the alphabet, in this case its necessary for a modification. In the process of encrypting and decrypting in Vigenere algorithm we used modulo 26, this refers to the number of alphabet letters A through Z as many as 26 characters, which is then encoded into an integer from 0-25 in accordance with the sequence of letters as in equation (1). In the case of encrypting and decrypting images, due to the intensity of the pixels have a value of 0-255, the Vigenere formula of equation (1) and (2) should be replaced by using modulo 256 to be applied to the image. Mathematically it can be written as follows:

$$C_{(i,j)} = E(P_{(i,j)}) = (P_{(i,j)} + k_s) mod\ 256 \quad (3)$$
$$P_{(i,j)} = D(C_{(i,j)}) = (C_{(i,j)} - k_s) mod\ 256 \quad (4)$$

where C is the ciphertext, k is the key, E is an encryption function, D is a decryption function, P is a plaintext, i is the index of the messages, and j is the length of the key.

4 RSA Cryptography Algorithm

The RSA algorithm is an asymmetric key algorithm created by three researchers from MIT (Massachusetts Institute of Technology) in 1976, namely: Ron (R) ivest, Adi (S) Hamir, and Leonard (A) dleman [15].

4.1 RSA Algorithm Process

According to [15]**, t**he RSA algorithm is based on Euler's theorem

$$(m^e)^d \equiv m(mod\ n) \quad (5)$$

which means that m powers to e and followed by powers of d returns to the earlier m. So that the encryption and decryption process is formulated as follows:

$$E_e(m) = c = m^e (mod\ n) \quad (6)$$
$$D_d(m) = m = c^d (mod\ n) \quad (7)$$

4.2 Implementation of RSA algorithm in Image

The encryption process is done by encoding the RGB components of each pixels in the image. In the RSA algorithm encryption values will range from 0 to n because the results are modulo n. While the intensity of the RGB value is between 0 to 255. Then it's necessary to limit on the value of the encryption [8].

a. Encryption Process
   Once the value is encrypted with the RSA algorithm. Encrypted value is limited by the formula

$$y_i = 256.k_i + r_i \quad (8)$$

   where r_i is added to the image and k_i become a key matrix elements K. While k_i obtained using formula $k_i = \left\lfloor \frac{y_i}{256} \right\rfloor$ and r_i from formula $r_i = y_i\ mod\ 256$.

b. Decryption Process
   Decryption process begins by taking the RGB values of the encrypted image r_i. Then Forming a new value y_i using the key matrix K, by formula (8). Then the value is decrypted to be y_i, with formula $x_i = y_i^e\ mod\ n$.

5 Implementing Image Encryption and Decryption with *Hybrid* Algorithm Vigenere and RSA

Studying from literature relating to the implementation of cryptography, Vigenere algorithm and RSA algorithm on an image.

1. Applying the process of encrypting image files with Vigenere algorithm and RSA algorithm with the following steps:
   a. Encryption process
      i. Inserting images with (n x m) pixels.
      ii. Taking the RGB values at each pixels.
      iii. Vigenère algorithm encryption with the key: $x(s), s = 1,2, \dots, z$. Depending on the length of the key, where x_1 the key to encrypt the RGB components of the pixels 1, x_2 to encrypt the RGB components of the pixel 2 and so on, if the key index has reached its length but the pixel is still not exhausted it will be repeated again from the beginning. With the formula:

$$R'(i,j) = R(i,j) + x(s)\ mod\ 256$$
$$G'(i,j) = G(i,j) + x(s)\ mod\ 256$$

$$B'(i,j) = B(i,j) + x(s)\ mod\ 256$$

iv. RSA key generation algorithm.
   1. Choose two random prime numbers, for example, and.pq
   2. Calculate $n = pq$.
   3. Calculate $\phi(n) = (p-1)(q-1)$.
   4. Select the public key e which are relatively prime with $\phi(n)$.
   5. Specifies the private d key that satisfies $e * d = 1\ mod\ \phi(n)$.

v. Encrypting on each RGB value by RSA algorithm, with the formula:

$$R''(i,j) = (R'(i,j)^e)\ mod\ n$$
$$G''(i,j) = (G'(i,j)^e\ )mod\ n$$
$$B''(i,j) = (B'(i,j)^e\ )mod\ n$$

vi. Limiting the value of the RSA encryption using formula:

$$R''(i,j) = 256.K_1(i,j) + \ r(i,j)$$
$$G''(i,j) = 256.K_2(i,j) + \ g(i,j)$$
$$B''(i,j) = 256.K_3(i,j) + \ b(i,j)$$

where K_1, K_2, K_3 is the key element of the matrix.

vii. The encrypted image obtained by entering $r, g, and\ b$ as the RGB value.

b. Decryption process.

i. Inserting an image that will be decrypted with (n x m) pixels.

ii. Taking the RGB values at each pixels.

iii. Forming a new value using key matrix formula,

$$R''(i,j) = 256.K_1(i,j) + \ r(i,j)$$
$$G''(i,j) = 256.K_2(i,j) + \ g(i,j)$$
$$B''(i,j) = 256.K_3(i,j) + \ b(i,j)$$

iv. Decrypting is the new value with the RSA algorithm, formula,

$$R'(i,j) = (R''(i,j)^d\ )mod\ n$$
$$G'(i,j) = (G''(i,j)^d)\ mod\ n$$
$$B'(i,j) = (B''(i,j)^d\ )mod\ n$$

v. Decrypting with a Vigenere keys $x(s)$, each key is used to decrypt the RGB values from the previous process with the formula.

$$R(i,j) = R'(i,j) - x(s)\ mod\ 256$$
$$G(i,j) = G'(i,j) - x(s)\ mod\ 256$$
$$B(i,j) = B'(i,j) - x(s)\ mod\ 256$$

vi. RGB values are added in the new image with the size (n x m) pixels, the same decrypted image thus the original image is obtained

2. Creating a program from procedures that have been described.
3. Testing program to the implementation of the algorithm.

6 Result and Discussion

The encryption process is done first by randomize key, the key length is five keys then randomized to get $k_1 = 144, k_2 = 166\ , k_3 = 38\ , k_4 = 204\ , k_5 = 98$ as the Vigenere

keys while the algorithm RSA keys are.$p = 71, q = 31, n = 2201, \phi(n) = 2100, e = 1139, d = 59$, then inputting the initial image file as shown in Figure 1.

Figure 1 Initial Image

6.1 Encryption Process

Once the images are encrypted with both algorithm, the patterns of the object from the initial image has changed a lot, so it is quite difficult to identify the original picture. Image encryption result can be seen in Figure 2.

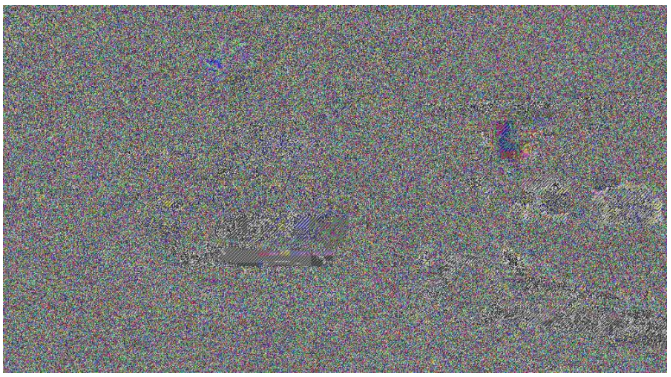

Figure 2 Encrypted Image

6.2 Decryption Process

Decryption process performed by inserting an encrypted image as shown in Figure 2. In the decryption process, RSA algorithm run first then Vigenere algorithm. The results of the decryption process of the encrypted image can be seen in Figure 3.

Figure 3 Decrypted Image

7 Conclusion

Implementation of the program on the image with Vigenere Algorithm keys $k_1 = 144, k_2 = 166, k_3 = 38, k_4 = 204, k_5 = 98$ and RSA algorithm $p = 71, q = 31, n = 2201, \phi(n) = 2100, e = 1139, d = 59$. From the encryption process, the encrypted image is very different from the initial image. While the decryption process, the encrypted image can be decrypted to the initial image.

8 References

[1] Leeson, P.T., dan Coyne, C.J. 2005. *The Economics of Computer Hacking*. USA: Journal of Law, Economics and Policy.

[2] Tillborg, H.C.A. van. 2018. Fundamentals of Cryptology. Dordrecht: Kluwer Academic Publishers..

[3] Barakat, M., Eder, C., Hanke, T. 2018. An Introduction to Cryptography. University of Kaiselautern: Germany.

[4] Mousa, A., Hamad, A. 2006. Evaluation of the RC4 Algorithm for Data Encryption. International Journal of Computer Science and Applications.

[5] Khizrai, M.S.Q., Bodkhe, S.T. 2014. Image Encryption using Different Techniques for High Security Transmission over a Network. International Journal of Engineering Research and General Science Volume 2, Issue 4.

[6] Rihartanto., Susanto, A., Khotimah, T., Sumadi, M.T., Warsito, J. 2018. Image encryption using vigenere cipher with bit circular shift. International Journal of Engineering and Technology, Vol. **7**, pp. 62-64.

[7] Trappe, W., Washington, L.C. 2006. *Introduction to Cryptography with Coding Theory*. New Jersey: Pearson Prentice Hall.

[8] Zhao, G., Yang, X., Zhou, B., Wei, W. 2010. *Rsa-Based Digital Image Encryption Algorithm In Wireless Sensor Networks*. 2010 2nd International Conference on Signal Processing Systems (ICSPS).

[9] Bernstein, D. J., Heninger, N., Lou, P., Valenta, L. 2017. *Post-quantum RSA*. Post-Quantum Cryptography: 8th International Workshop. Utrecht : The Netherlands.
[10] Milanov, E. 2009. *The RSA Algorithm*. Pp. 1-11.
[11] O Ting, T & Yang, Xin-She & Cheng, Shi & Huang, Kaizhu. 2015. *Hybrid Metaheuristic Algorithms: Past, Present, and Future.* 10.1007/978-3-319-13826-8_4.
[12] Yang, X. S., 2008. *Firefly Algorithm For Multimodal Optimization.* Stochastic Algorithms : Foundation and Application, 5th Springer, London, UK.
[13] Sachs, J. 2003. *Digital Image Basics.* Digital Light & Color.
[14] Martin, K. 2017. *Everyday Cryptography Fundamental Principles and Applications 2nd edition*. Oxford University Press, Oxford.
[15] Munir, Rinaldi. 2006. Kriptografi. Bandung: Informatika.