TELKOMNIKA, Vol.12, No.3, September 2014, pp. 651~656
ISSN: 1693-6930, accredited A by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v12i3.83

The Implementation of Henon Map Algorithm for Digital Image Encryption

Edi Sukirman[1] , Suryadi MT[*2] , M. Agus Mubarak[3]
[1] Jurusan Sistem Informasi, Universitas Gunadarma, Depok 16424, Indonesia
[2] Departemen Matematika, Universitas Indonesia, Depok 16424, Indonesia
[3] Jurusan Teknik Informatika, Universitas Gunadarma, Depok 16424, Indonesia
*Corresponding author, email: yadi.mt@sci.ui.ac.id

Abstract

Security information is a very important aspect that must be noticed. Information not only in the form of text but also in form of data image. Using data encription to send private information have been widely use. But still need to improve the endurance from bruto force attack. One ways to improve it, is by using chaos theory with henom algorithm. Test result gave the alghoritm can encrypt image data from grayscale type to colorfull type. Encryption and descryption time proportional to the size image. Composition and variety coulor doesn't effect the time. this algorithm has key space of 10^{30} *and key sensitivity up to* 10^{-16}. *So, it can be concluded that, the algorithm is very difficult to be cracked by brute force attack.*

Keywords: *encryption algorihtm, chaos, digital image, henon map*

1. Introduction

Now a days using computers to send any kinds of information thorough internet connection are common. By using public path people from around the world can send information even though it has very low safety level.

Information security is an aspect that is very important and urgent to be noticed. Informationon concerning the interests of private, institutional and corporate necessarily have a high value and should be kept confidential. Confidential information must be in great demand for various purposes and must carefully guarded. This information not only in the form of text data, but also in the form of image data that is highly confidential.

By encrypting data so that only the recipient can only decrypt the data is one of solutions that many enggineers do. Some encryption algorithms such as DES, AES, RSA, and others have been widely used to encrypt the image data, but these algorithms still must be improved durability of various attacks, such as brute force attacks [1]. Many research have been done in how to improve the durability of the algorithms used in the encryption process from a brute force attack, provide a good combination of speed, high security, complexity, and computational power, etc [2],[3]. One of them is using the chaos theory. Chaos-based encryption also been extensively studied by researchers because of its superior in safety and complexity [4]. One algorithm which implements the theory of chaos is the Henon map algorithm, this algorithm implements chaos theory by generating random numbers with two initial values. The algorithm implements the chaos theory that has sensitivity to small changes in initial parameter values and has a high level of security from brute force attacks [5]-[11].

Based on the above explanation, this research is about implementing the algorithm on the Henon map for the encryption and decryption of digital images information.

2. Research Method

Chaos theory comes from the theory of systems that exhibit irregular appearance, despite the fact that this theory is used to explain the occurrence of random data. Inventor of chaos theory is a meteorologist, Edward Lorentz, in 1960 when he made a model of weather forecasts.by Iterating weather mathematical model to obtain weather forecasts in the future. The longer time weather forecasts are computed, the longer iteration to be done. By changing

Received March 29 2014; Revised July 24, 2014; Accepted August 10, 2014

slightly the initial value of 0.000127 iteration only, he found that the weather forecast had generated great divergence [12].

Henon equation is a dynamic system that implements a discrete system. Henon equation using a point (x,y) in an equation and mapped to a new point with the equation [9],[13]:

$$x_{n+1} = y_n + 1 - ax_n^2, \quad (1)$$

$$y_{n+1} = bx_n \quad (2)$$

Stages in using Henon equation is divided into two stages, which are key stream and encryption/decryption stage.

In the key stream generation phase is done by using algorithms Henon map, the two keys are required to be algorithms generate series of numbers of pseudo-random real numbers, so that sequence numbers can be used as a key stream, then these numbers must be converted to an integer array with a range between 0 to 255.

The process is done by absolut sequence numbers (Xn), each of these numbers multiplied by 1000. Mathematically the integer conversion functions can be written as follows: the process is done by absolut sequence numbers (Xn), each of these numbers multiplied by 1000. Mathematically the integer conversion functions can be written as follows:

$$E_n = \|X_n \times 1000\|$$

$$F_n = \lfloor E_n \rfloor$$

Then the rounding down (floor) resulting integer (Fn). Having obtained the integer series, the series is mapped to the range [0, 255]. Mathematically, the mapping function can be written as follows $K_n = F_n \mod 256$

Encrptyon stage is the stage where the original image or plain image (Pn) is converted into cipher image (Cn) by XOR the pixels of plain image (Pn) of the keystream (Kn) which has been raised. Mathematically this encryption function can be written as follows:

$$C_n = P_n \oplus K_n \quad (3)$$

where :

C_n : Cipher image (encryption image).
P_n : Plain image (previous image).
K_n : Keystream.

The decryption phase has the same process with encryption stage, it's just using a cipher encrypted image (C_n) as the input image. To decrypt the original image from the cipher image (C_n), by XOR operation for the pixel-pixel image cipher (C_n) of the keystream (K_n) which has been raised. The process can be described by the algorithm shown in Figure 1.

```
Algorithm Henon map
Initial state : orginal image (P)
Final state : encrypted image (C)
Input Key A, B
Input Image P(1..mxn)
Initial value x(0), y(0)
Loop i = 0 to (mxn)-1
        x(i+1) = y(i)+1-a*x(i)*x(i)
        y(i+1) = b*x(i)
        E(i+1) = |x(i+1)|*10000
        F(i+1) = floor(E(i+1))
        K(i+1) = mod(F(i+1), 256)
        C(i+1) = P(i+1)⊕ K(i+1)
Next loop
Output Image C(1..mxn)
```

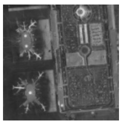
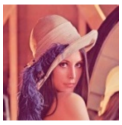
Figure 1. Image Encryption Algorithm

3. Results and Analysis

Implementation of the application is done on a computer with hardware specs: Intel ® Core ™ processor B940 (2.0GHz, 2MB L3 cache), DDR3 RAM (2GB), VGA Intel ® HD Graphics, 320 GB HDD, monitor, keyboard and mouse.

In the test phase, the encryption and decryption process use a numbers of images. Images data used in this study can be seen in Table 1.

Table 1. Image Data Testing

File Name	Original Image	Image Type	File Size	Image Size
Clock. bmp		Gray scale (8 bits/ pixel)	192 kb	256 x 256
Aerial. bmp		Gray scale (8 bits/ pixel)	768 kb	512 x 512
Airport. bmp		Gray scale (8 bits/ pixel)	300 kb	1024 x 1024
Girl.bmp		Color (24 bits/ pixel)	192 kb	256 x 256
Lena. bmp		Color (24 bits/ pixel)	768 kb	512 x 512
SteelSea. bmp		Color (24 bits/ pixel)	300 kb	1024 x 1024

3.1. Analysis of Key Space

Key space is the total number of different keys that can be used for encryption and decryption. To deal with a brute force attack, cryptographic algorithms should have a large key space, then the longer the time it takes to break the lock of the algorithm. Key parameters used in the encryption algorithm are two, namely key A and key B, each data in double type. Double-precision computing for precision according to standard 64-bit IEEE floating-point is 10^{-15}. So the number of possible values of each key is 10^{-15}, then the possible combinations of two keys key is R (A, B) = $10^{-15} \times 10^{-15} = \mathit{10^{30}}$

Time required to try all combinations of keys (exhaustive key search) [14] can be seen in Table 2.

Table 2. Time Required to Try exhaustive Key Search

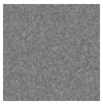
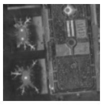
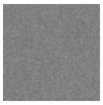
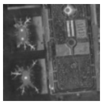
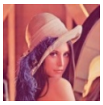
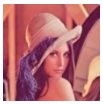
Key Space	Experiments/sec	Time needed	
		Second	Years
10^{30}	10^{6}	10^{24}	$3{,}215 \times 10^{16}$
	10^{12}	10^{18}	32150205761
	10^{18}	10^{12}	32150,20576
	10^{24}	10^{6}	0,032150206

Data in Table 2 shows that it takes approximately 3.215 × 10^{16} years to try all combinations of keys with a computer that can do 1 million experiments per second. So it is known that it takes substantial time to solve two key combination that led to a brute force attack is not efficient.

3.2. Image Similarity Analysis

Testing is done by comparing the image of the beginning of the encrypted image and decrypted image on a number of test images. The results are shown in Table 3.

Table 3. Result Test Similarity Image

Image name	Original Image	Encryption image	Descryption image
Clock.bmp 256 x 256	 192 kb	 192 kb	 192 kb
Aerial.bmp 512 x 512	 768 kb	 768 kb	 768 kb
Airport.bmp 1024 x 1024	 3000 kb	 3000 kb	 3000 kb
Girl.bmp 256 x 256	 192 kb	 192 kb	 192 kb
Lena.bmp 512 x 512	 768 kb	 768 kb	 768 kb
Steel Sea.bmp 1024 x 1024	 3000 kb	 3000 kb	 3000 kb

Tabel 3 shows that the file size and dimensions of the original image,encrypted image and decrypted image is essentially the same as the encryption and decryption process in this study only change the values of the pixels of the image using XOR operations for key bits with image pixels.

3.3. Analysis of Parameter Sensitivity Key

The test is performed by comparing the image of the decryption on a number of test images that have been encrypted with a key value of 1.4 and a value of 0.3 B key with a very small change of value on one or two key pieces. Results of testing done by the decryption process uses a different key value, key A with a value 1.4 + 10^{-16}, whose results appear in Table 4.

Table 4. Key Sentitivity Test Result

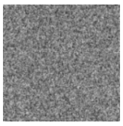
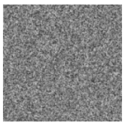
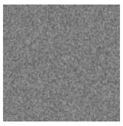
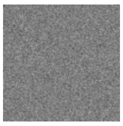
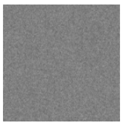
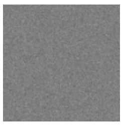
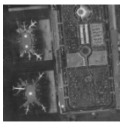
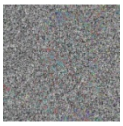
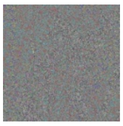
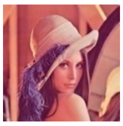
Image names	Encryption image Key A= 1.4 Key B = 0.3	Descryption image key A = 1.4 + 10^{-16} key B = 0.3	Descryption image Key A = 1.4 = 1.4 + 10^{-17} key B = 0.3
Clock.bmp			
Aerial.bmp			
Airport.bmp			
Girl.bmp			
Lena.bmp			
Steel Sea.bmp			

Table 4, shows the process of decryption of the encrypted image with little different in one of the key, encryption algorithm has key sensitivity that reaches 10^{-16}.

3.4. Analysis Process Encryption and Decryption Time

The test is performed by calculating the process time of encryption and decryption on a number of test images. The test results shown in Table 5.

Table 5. Time Test Result for Encryption and Decryption Process

Image name	Image type	File size	Image dimensions (pixel)	Encryption time proces (second)	Descryption time proces (second)
Clock.bmp	Grayscale (8 bits/ pixel)	192 kb	256 x 256	2.684	2.638
Aerial.bmp	Grayscale (8 bits/ pixel)	768 kb	512 x 512	40.867	40.613
Airport.bmp	Grayscale (8 bits/ pixel)	300 kb	1024 x 1024	866.170	816.802
Girl.bmp	Color (24 bits/pixel)	192 kb	256 x 256	2.653	2.649
Lena.bmp	Color (24 bits/pixel)	768 kb	512 x 512	40.725	40.587
Steel Sea.bmp	Color (24 bits/pixel)	300 kb	1024 x 1024	884.054	848.692

Test result data in Table 5, shows that the encryption and decryption processing time proportional to the size of the image dimensions, the greater the dimensions of an image of the longer time required to encrypt the image. Table 5 also shows that the composition and diversity of colors that make up the image did not significantly affect time image encryption and decryption process.

4. Conclusion

Henon map algorithm implementation on the process of encryption and decryption of digital image has been successfully carried out on the application and tested on several images. The experimental results show that the algorithm Henon map can encrypt and decrypt image with exactly the same as the original image, and can be deduced from this study that :

a. Encryption and decryption processing time proportional to the size of the image dimensions, the greater the dimensions of an image of the longer time required to encrypt the image because the bigger the dimensions of the image, the bigger pixels of the image to be processed and vice versa.
b. Composition and diversity of colors of image did not significantly affect the time of encryption and decryption processes. t the image which has the composition and diversity of high color with the image that has the composition and diversity of low color has time encryption process is relatively the same.
c. Encryption algorithm has key space for 10^{30} and key sensitivity that reaches 10^{-16}, so the algorithm is very difficult to be cracked by brute force attack.

Thus the digital image encryption algorithm is very difficult to be solved with brute force attacks.

References

[1] Pareek NK., Patidar V., Sud KK. Image encryption using chaotic logistic map. *Journal of Image and Vision Computing.* 2006; 24: 926-934.

[2] Patidar V., Pareek NK., Sud KK. A new subtitution-diffusion based image cipher using chaotic standard and *logistic maps*. *Journal of Commun Nonlinear Sci Numer Simulat.*, 2009; 14: 3056-3075.

[3] Menezes, Alfred J., Paul C van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press. 1996.

[4] Zhang W., Wong K., Yu H., Zhu Z. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. *Journal of Commun Nonlinear Sci Numer Simulat.* 2013; 18: 2066-2080.

[5] Kocarev L., Lian S. *Chaos-based cyrptography*. Berlin Heidelberg: Springer-Verlag. 2011.

[6] Gao H., Zhang Y., Liang S., Li D. A new chaotic algorithm for image encryption. *Journal of Chaos, Solutons and Fractals.* 2006; 29: 393-399.

[7] Suryadi MT. *New Chaotic Algorithm for Video Encryption.* 4th The International Symposium on Chaos Revolution in Science, Technology and Society 2013, Jakarta, 28-29, August. 2013.

[8] Munir, Rinaldi., Algoritma Enkripsi Selektif Citra Digital Dalam Ranah Frekuensi Berbasis Permutasi Chaos. *Jurnal Rekayasa Elektrika*. 2012; 10(2): 69-75.

[9] Abu Zaid, Osama M., El-Fishawy, Nawal A., Nigm, EM. Cryptosystem Algorithm Based on Chaotic System for Encrypting Colored Image. *International Journal of Computer Science Issues.* 2013; 10(4): 215-224.

[10] Zhang Y. Plaintext Related Image Encryption Scheme Using Chaotic Map. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2014; 12(1): 635-643.

[11] Zhang Y, Xia JL, Cai P, Chen B. Plaintext related two-level secret key image encryption scheme. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(6): 1254-1262.

[12] Devaney RL. *An introduction to chaotic dynamical systems* (2nd ed.). New York: Addison-Wesley Publishing company, Inc. 1989.

[13] Sonis M. Once more on Hénon map: Analysis of bifurcations. *Chaos, Solitons & Fractals*. 1996; 7(12): 2215–2234.

[14] Stallings W. *Computer and Network Security : Principle and Practice* (5th ed.). New York: Prentice hall. 2011.