THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Combination Algorithm Arnold Cat Map (ACM) and Rivest Shamir Adleman (RSA) in Security Image

Fitria Nova Hulu
Lecturer, University of Development Panca Budi Medan – North Sumatra, Indonesia
Dr. Erna Budhiarti Nababan
Lecturer, Department of Computer Science, University of Northern Sumatra
Universitas Sumatera Utara –USU, Indonesia
Dr. Suherman
Lecturer in the Department of Electrical Engineering University of Northern Sumatra,
Universitas Sumatera Utara –USU, Indonesia

Abstract:
At present, the security and confidentiality of the data or information is a critical thing and the increasingly widespread use of image data in a variety of fields. Therefore, the security of image data from unauthorized access becomes necessary. There are a variety of techniques to improve the safety of the data or information has been developed, one of which is Cryptography technique or so-called encryption/decryption technique. Cryptography is the science of keeping messages by changing the data or information into a form that is different or can not be recognized. To increase security on the image we can take more than one encryption algorithm, and a second cryptography algorithm to do encryption and decryption can be the way. Cryptographic algorithms commonly used today and proved its strength especially for the digital image is Algorithm with Chaos system. Arnold's Cat Map (ACM) is one of a chaos-based algorithm that can be used to encrypt the image file and to improve security on that image then use new algorithms are algorithms Rivest Shamir Adleman (RSA) algorithm, known as the standard in the field of cryptography. This research aims to optimize the security image jpg format by combining two cryptographic algorithms are algorithms ACM and the RSA algorithm so expect the strength of the encrypted with the algorithms are complicated to be solved.The aims of the comparison MSE showed good results where quality RGB original image with the image of an encrypted does not show error , but the value of PSNR between the original image with the image of the encoded still showed noise where PSNR finally to red (r) = 16.8955, green (g) = -1.9952, blue (b) = -7.1882. Comparison of the time required for each encryption-decryption is approximately 0.1 seconds to 0.4 seconds.

Keywords: *ACM, Chaos, Encription, MSE, PSNR, RSA.*

1. Overview

By rapid growth of communication world, especially in the field of information such as the data, images, audio or video, we need a system that can maintain the confidentiality of such information. Security is a common requirement and Becomes necessary, the confidential nature of an information requires a security mechanism that can deal with the confidentiality of such information.

Encryption is the process of scrambling method or process of securing the information to the make such information can not read without any specialized knowledge. Encryption can use for security purposes, but other techniques still needed to the make communications secure, particularly subject to Ensure the integrity and authentication of a message.

This paper was conducted to analyze a method of encryption decryption algorithm using a combination of Arnold Cat Map (ACM) and Algorithms Rivest Shamir Adleman (RSA) Security glittering image.

2. Rivest Shamir Adleman (RSA)

These algorithms perform factoring very large numbers. Therefore RSA considered safe. the variables used in the RSA algorithm is:

1. p and q are primes (secret)
   n = p * q (secret) (3)
   Φ(n) = (p – 1) (q – 1)(secret) (4)
2. PK (encryption key) (not secret)
3. SK (decryption key) (secret)
4. X (Original Image)(secret)
5. Y (Encrypted Image) (not secret)

RSA is a block cipher where the original text and secret text is an integer between 0 and n-1 for some n. Encryption and decryption is derived from some form of the following, M is the original text block and C is the encrypted text blocks.

$$\mathbf{C = M^{e} modn} \qquad (5)$$

Equation 5 is the equation used to perform the encryption process, while the decryption process performed by the equation 6 below:

$$\mathbf{M = C^{d} modn = (M^{e})^{d} modn = M^{ed} modn}(6)$$

which :
C =Encrypted Image
M = Original Image
e =public exponent, or often called encryption exponent.
d =private exponent, or often called decryption exponent
n =divisor of modulo operation

The sender and receiver must know the values of n and e, and only the recipient who knows the value of d. This is a public key encryption algorithm with a public key of KU = {e, n} and a special key for KR = {d, n}. In order for this algorithm could qualify as a good public key encryption, it must meet the following provisions:
1.The possibility of finding the value of e, d, n such that Med = M mod n for all values of M <n.
2. relatively easy to calculate M^{e}dan $C^{d}$for all values of M <n.
3. Not easy to calculate or determine the value of d that contains the value of e and n.

The first two conditions can be met with ease. While the three new provisions can be met if the value of e and n is large enough.

2.1. Mean Square Error (MSE) andPeak Signal to Noise Ratio (PSNR)

MSE is the average squared error between the original image with the image that has been processed, which mathematically can be formulated as follows:

$$MSE = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left| \left(f(x,y) - g(x,y) \right)^{2} \right| \qquad (7)$$

Which :
MSE = The Value of Mean Square Error of the Image
M = Image Length (in Pixel)
N =Image Width (in Pixel)
(x,y) = coordinates of each pixel

2.2. Testing Methods

The programming language used is the programming language MATLAB. Data for encryption and decryption process is an image file with format "jpg" or "jpeg (Joint Photographic Experts Group), which was originally sized 249x249 pixel later writers changed to a size of 100x100 pixels were taken with a camera phone. The author takes the example of a simple image to materials analysis.

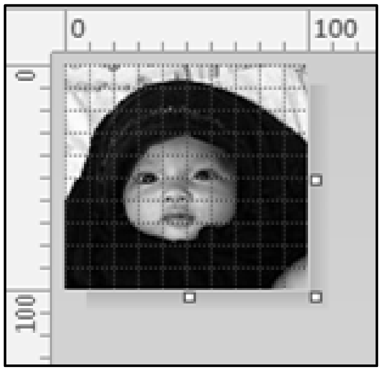


Figure 1: First Image File "Ahla.jpg" size of 100 x 100 pixels

2.3. Process Encryption and Decryption by using ACMAlgorithm

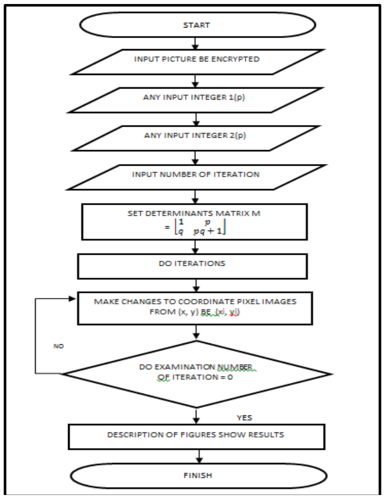

START
INPUT PICTURE BE ENCRYPTED
ANY INPUT INTEGER 1(p)
ANY INPUT INTEGER 2(p)
INPUT NUMBER OF ITERATION
SET DETERMINANTS MATRIX M
$= \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}$
DO ITERATIONS
MAKE CHANGES TO COORDINATE PIXEL IMAGES FROM (x, y) BE (xi, yi)
NO
DO EXAMINATION NUMBER OF ITERATION = 0
YES
DESCRIPTION OF FIGURES SHOW RESULTS
FINISH

Figure 2: Flowchart of the encryption process by Arnold Cat Map Algorithm

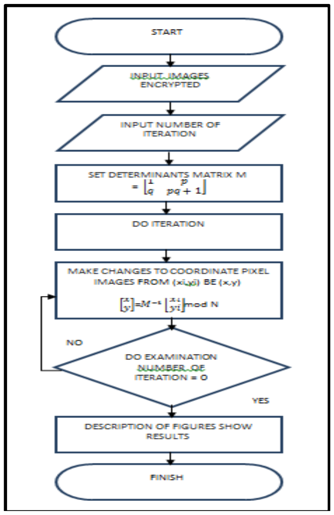

START
INPUT IMAGES ENCRYPTED
INPUT NUMBER OF ITERATION
SET DETERMINANTS MATRIX M
$= \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}$
DO ITERATION
MAKE CHANGES TO COORDINATE PIXEL IMAGES FROM (xi,yi) BE (x,y)
$\begin{bmatrix} x \\ y \end{bmatrix} = M^{-1} \begin{bmatrix} xi \\ yi \end{bmatrix} \bmod N$
NO
DO EXAMINATION NUMBER OF ITERATION = 0
YES
DESCRIPTION OF FIGURES SHOW RESULTS
FINISH

Figure 3: Flowchart of Decryption Process by Arnold Cat on Map (ACM)Algorithm

3 Analysis of Test Results

In this section, will explain the results of research using methods Algorithm Arnold Cat Map (ACM) and Algorithms Rivest Shamir Adleman (RSA) in providing security to the image.

3.1. Encryption and Decryption Process With the combination of Arnold's Cat Map (ACM) Algorithm and Rivest Shamir Adleman (RSA)Algorithm

Encryption and decryption that is done using ACM algorithm to the original image "Ahla.jpg" will use the key in the form of primes, which p = 5 and q = 7

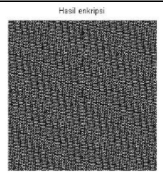
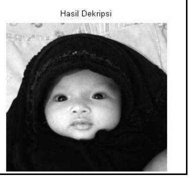
Original Image	Encrypted Image	Decrypted Image
		

Table 1: Encryption and Decryption by ACM Algorithm

The process of testing on a sample image of the image to be encrypted and decrypted using the Rivest Shamir Adleman (RSA), in which the testing process will first use the key form of two primes, i.e., p = 2 and q = 3 with a value of n = 6, d = 1 and e = 5 so that we obtain the public key = (5,6) and the Private key = (1,6)

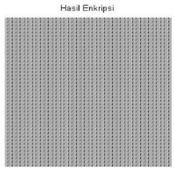
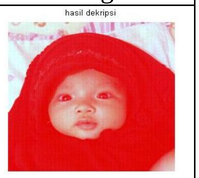
Original Image	Encrypted Image	Decrypted Image
		

Table 2: Encryption and Decryption Process with RSA Algorithm

From Table 3 are shown in a test results encryption and decryption of the original image, where the testing process also input the prime numbers p and q. Results first encryption using ACMalgorithms shows the original image is no longer recognizable, but because of it's periodic characteristics, ACM algorithm is able to reproduce the image of the original, so the encryption by using ACM algorithm not safe, because through a simple hack value of p and q can be found through surgery brute force. Therefore testers perform a second encryption using the RSA algorithm which aims to enhance the security of the image where the algorithm Rivest Shamir Adleman (RSA) algorithm, known as the standard in cryptography.

Decryption is the reverse of the encryption itself, which after the end of the RSA encryption that caused the original image pattern becomes increasingly visible, then the first decryption is done by using the RSA algorithm again, the results of the first decryption algorithm to be decrypted again with ACM to obtain the original image.

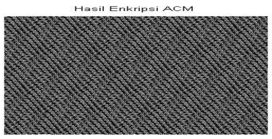
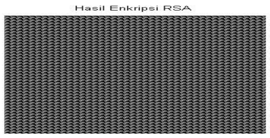
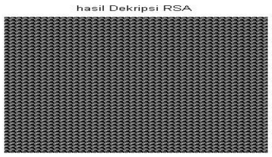
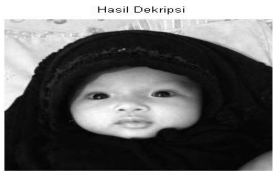
Original Image	
Encrypted by ACM	
Encrypted by RSA	
Decrypted by RSA	
Decrypted by ACM	

Table 3: Encryption and Decryption Process with Combination of Arnold Cat Map (ACM)Algorithm and Rivest Shamir Adleman (RSA)Algorithm

4.1. Histogram Analisys

A histogram is a graphical representation of the color distribution of digital image or describe the distribution of pixel intensity values of an image or specific part in the image.

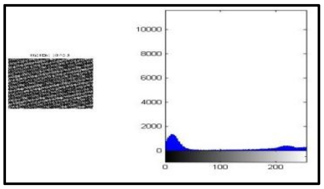


Figure 8:Encrypted by ACM Image's Histogram

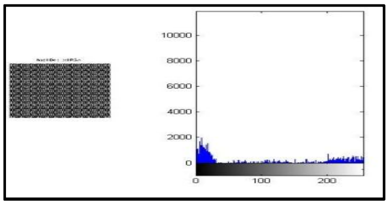


Figure 9:Encrypted by RSA Image's Histogram

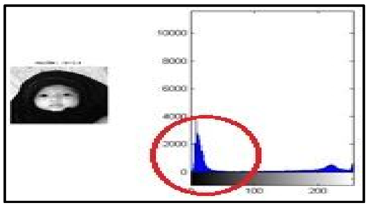


Figure 11:Decrypted by RSA Image's Histogram

Histogram at the ACM show that histogram original image changes shape and lower than previously where the histogram graph shows a comparison between BV (brightness value) while the histogram at the RSA is also not much different from the ACM where the peak histogram which is the pixel intensity has decreased, however RSA decryption result at histogram shows that the value back to its original position, but the contrast range move and change of the original image, it is due to the noise of the image produced on the decryption process. In combination ACM and RSA histogram, histogram generated according as the initial image at the time of encryption and decryption process, the problem of the noise at the time of decryption with the RSA algorithm can be overcome by a combination of the two algorithms.

4.2. AnalysisMean Square Error (MSE) andPeak Signal to Noise Ratio (PSNR)

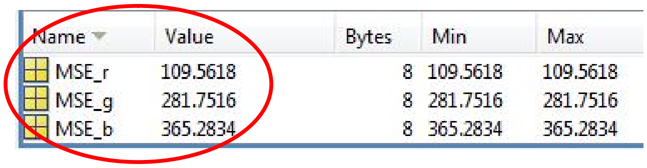
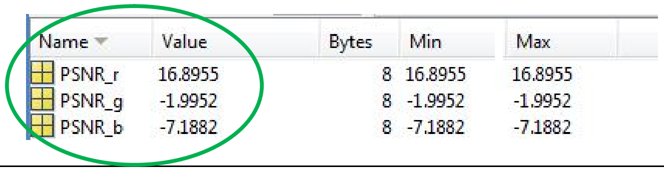
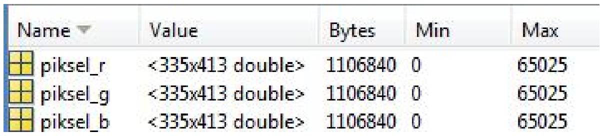
MSE	 Name Value Bytes Min Max MSE_r 109.5618 8 109.5618 109.5618 MSE_g 281.7516 8 281.7516 281.7516 MSE_b 365.2834 8 365.2834 365.2834
PSNR	 Name Value Bytes Min Max PSNR_r 16.8955 8 16.8955 16.8955 PSNR_g -1.9952 8 -1.9952 -1.9952 PSNR_b -7.1882 8 -7.1882 -7.1882
Pixel	 Name Value Bytes Min Max piksel_r <335x413 double> 1106840 0 65025 piksel_g <335x413 double> 1106840 0 65025 piksel_b <335x413 double> 1106840 0 65025

Table 4: Comparison of MSE and PSNR of Original image against Encrypted image by combination of ACM and RSA Algorithm

Table 4 shows the MSE and PSNR to quality RGB image, the acquisition of MSE and PSNR value resulting from a comparison of the original image to the image encrypted with a combination of ACM and the RSA algorithm. MSE value to the quality of the respective RGB image quality that is good enough where the value of red (r) = 109.5618, green (g) = 281.7516, blue (b) = 365.2834.
PSNR values in Table 4 for each quality RGB has shown better results. This is because the image of the encrypted experienced double encryption process: first by using an algorithm ACM and the second by using the RSA algorithm cannot be denied that the image of the decryption with these two algorithms still have noise, however, to generate value PSNR much better then the filter must still be done, because the value falls below 30 dB PSNR indicates relatively low quality, which the distortion due to the insertion clearly visible. But the quality of stego-image high is at a value of 40 dB and above.

5. Conclusion

The conclusions that can draw from this study are:

1. The process of encryption and decryption by using the combination of Arnold Cat Map (ACM) algorithms and the Rivest Shamir Adleman (RSA) algorithms successfully carried out, wherein the encrypted image looks like a random image and is no longer recognizable.
2. Analysis of the histogram shows the pixels in the image encrypted sensitive to small changes in the key so that the picture not successfully decrypted, so the algorithm is safe from hacker attacks.
3. Comparison of MSE shows good results where the quality of the original image RGB with the encrypted image does not show error, but the value of PSNR between the original image with the encoded image still shows a noise marked with a minus value, where the value of PSNR finally to red (r) = 16.8955, green (g) = -1.9952, blue (b) = -7.1882.
4. Comparison of time required for each encryption decryption-selling no longer is about 0.1 seconds to 0.4 seconds.

6. References

i. Li, X. W., Kim, D. H., Cho, S. J., Kim, S.T. 2013, Integral Imaging Based 3-D Image Encryption Algorithm Combined with Cellular Automata. Department of information and communications, Engineering Pukyong National University Daeyeon 3-Dong, Pusan 599-1, Korea.

ii. Lin, Ch-H., Chen, T-H., dan Wu, Ch-S. 2013, A batch image encryption scheme based on chaining random grids. Sharif University of Technology, ScientiaIranica D (2013) 20 (3), 670–681.

iii. Lumbangaol, RiniWati. 2013, Aplikasi Pengamanan Gambar Dengan Algoritma Rivest-Shamir Adleman (RSA).Jurnal STMIK Budidarma.

iv. Menezes, A. 1997.Handbook of Applied Cryptography. USA: CRC Press, Inc.

v. Munir, Rinaldi. 2012, Algoritma Enkripsi Citra Digital Berbasis Chaos dengan Pengga bungan TeknikPermutasidan Teknik Substitusi Menggunakan Arnold Cat Map dan Logistic Map.ISSN 2089-8673 Jurnal Nasional Pendidikan TeknikInformatika (JANAPATI) Volume 1, Nomor 3, December 2012

vi. Rhee, Man Young, 1994, Crytography and Secure Communications. Korea: McGraw-Hill Book Co.

vii. Schneier, B. 1996, Applied Cryptography 2nd Edition, Wiley & Sons.

viii. Sharma, M., Kowar, M.K. 2010, Image Encryption Technique Using Chaotic Schemes: A Review, International Journal of Engineering, Science, and Technology Vol 2 (6) 2010.

ix. Singh, Laiphrakpam Dolendro. Singh, Khumanthem Manglem. 2015, Image Encryption using Elliptic Curve Cryptography, Procedia Computer Science 54 (2015) 472 – 481 Science Direct