Image Encryption using Combination of Chaotic System and Rivers Shamir Adleman (RSA)

Pahrul Irfan
Islamic University of Indonesia
Jln. Kaliurang km.14.5,
Yogyakarta

Yudi Prayudi
Islamic University of Indonesia
Jln. Kaliurang km.14.5,
Yogyakarta

Imam Riadi
Ahmad Dahlan University
Jln. Prof.Dr.Soepomo,
Janturan, Yogyakarta

ABSTRACT
Security and confidentiality of data or information at the present time has become an important concern. Advanced methods for secure transmission, storage, and retrieval of digital images are increasingly needed for a number of military, medical, homeland security, and other applications. Various kinds of techniques for increase security data or information already is developed, one common way is by cryptographic techniques. Cryptography is science to maintain the security of the message by changing data or information into a different form, so the message cannot be recognized.

To compensate for increasing computing speeds increases, it takes more than one encryption algorithm to improve security of digital images. One way is by using algorithms to double cryptography do encryption and decryption. Cryptographic algorithm often used today and the proven strength specially the digital image is Algorithm with Chaos system. To improve security at the image then we use Additional algorithms namely Rivers algorithm Shamir Adleman (RSA) which known as the standard of cryptography algorithms.

This research aims to optimize security bitmap image format by combining the two algorithms namely Chaos-based algorithms and RSA algorithm into one application. Experiments conducted show that the proposed algorithm possesses robust security features such as fairly uniform distribution, high sensitivity to both keys and plain images, almost ideal entropy, and the ability to highly de-correlate adjacent pixels in the cipher images. Furthermore, it has a large key space, and transform image to pure text file which greatly increases its security for image encryption applications.

General Terms
Security

Keywords
Chaos, cipher text, bitmap, image encryption, RSA.

1. INTRODUCTION
Developments in information technology have made storage and transmission of digital media such as images and video becomes more easily and efficiently. Issues arising This convenience is the presence of a security hole for people who are not responsible to do theft of data, whether stored in a hard drive or transmitted from internet.

One type of files that are widely used and generally contain important information is digital image. Currently image has been used in almost all areas such as security plans, medical sciences, engineering sciences machinery, architectural buildings, works of art, advertising, education and so forth.

The image that is stored or transmitted in the form plain image susceptible to eavesdropping or theft, so the important information contained in the image can be accessible by someone who are not responsible. The example of the importance of securing the image is in the image building model design or design products made by a company. If the image can be accessed by unauthorized person, of course, the company will receive both in terms of financial losses or the other. Therefore it safeguards against the image of an important concern for protect the information contained.

The development of methods used in data encryption very rapidly, both Symmetrical (encryption use one key) or Asymmetric (Encryption using two keys). Symmetrical cryptographic among others, DES, 3DES, IDEA, AC5, RC4, AES, Chaos. As for the cryptographic algorithms that are Asymmetrical namely RSA, Deffie-Hellman, DSA, ElGamal [12].

Popular encryption algorithm used in image is the Chaos - based encryption. Chaos System used varies, like Logistic Map, Baker Map, Arnold Cat Map, and others. Logistic Map is one of Chaos is an encryption system that is simple but produce complex calculations, requiring short processing time, do not have a period and has sensitivity to initial input value [10]. Because some excess algorithm Chaos in image encryption, the authors tried to apply the algorithm Chaos Logistic system uses to perform encryption Map the RGB pixel image, and added to the algorithm Arnold Cat Map that is used to perform randomization the pixel position of the image, which is expected to be obtained cipher image which has scrambled pixel perfect and not can be recognized.

Cipher image generated from a single cryptographic algorithm is not strong enough to withstand the attack cryptanalyst, this is due to an increase in computation speed more quickly. to be able to increase the strength of the cipher image, we needs to be encrypt image using a combination of two encryption algorithms that produced the cipher strength of the encryption process can be guaranteed, and can hold the attack from cryptanalyst.

Rivers Shamir Adleman (RSA) is the Most popular cryptography algorithm. Virtually all standard cryptographic protocols using the RSA algorithm, including SSL / TLS (for securing http) and SSH (secure shell) [13]. Security algorithms RSA lies in the difficulty of factoring large numbers into a number of factors - the prime factor which is used as a private key to unlock cipher text [9]. Due to the excess of the RSA algorithm is a standard for cryptography algorithms both on text encryption or other data types, the authors try to implement these algorithms on digital image.

In this paper proposed doubles encryption algorithm for digital image using the Chaos algorithm and RSA algorithm. Election Chaos algorithm because it can produce random numbers that are sensitive to initial conditions, requires a short processing time and do not have looping period, where as RSA been selected because is a standard algorithm for encryption protocol. So from the merger of the two algorithms are is expected to improve the security of the cipher text from cryptanalyst attack and can answer challenge development of faster computing.

2. BASIC THEORIES

2.1 Logistic Map

Logistic map is the simplest chaotic systems form an iterative equation as follows [8]:

$$x_i + 1 = rx_i(1 - x_i) \qquad (1)$$

where r ∈ [3.57 ... 4] is the map parameter and $i = 1, 2, . . . , n$ is the number of iterations. The total number of iterations is equal to the number of pixel in image. Starting from a certain initial condition x_0, after n iterations the map will generates the chaotic sequence.

2.2 Arnold Cat Map

Arnold Cat Map (ACM) is a two-dimensional chaotic map after discovered by Vladimir Arnold in 1960 [14]. ACM transform the coordinates (x, y) in the image of size N × N to the new coordinates (x ', y'). The equation of ACM is :

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod(N) \qquad (2)$$

where (x_i, y_i) is position of the pixel in the image, $(x_i + 1, y_i + 1)$ is new pixel position after iteration i. Parameters b and c are any positive integer. ACM is iterated as m times and each iteration produces a random image. Values of $b, c,$ and m can be considered as the secret keys. The scramble image can be reconstructed into the original image using the same key (b, c, and m). The inverse equation of ACM is :

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}^{-1} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} mod(N) \qquad (3)$$

2.3 Rivers Shamir Adleman (RSA)

In 1978, a paper was published by R. Rivest, A. Shamir, and L. Adleman. This cryptosystem, which has come to be known as the most popular cryptographic algorithms [9]. These algorithms do factoring very large numbers which make it safe. Today, RSA is used in cryptographic applications from banking, and e-mail security to e-commerce on the Internet [10]. For RSA key pair generation, used algorithm as follows [12]:

- Choose two large distinct primes p and q and then form the public modulus n = pq.
- Choose public exponent e to be co-prime to $(p-1)(q-1)$, with $1 < e < (p-1)(q-1)$.
- The pair (n, e) is the public key.
- The private key is the unique integer $1 < d < (p-1)(q-1)$ such that $ed = 1 \bmod (p-1)(q-1)$.
- Encryption and decryption using equation below:

$$C = M^e \bmod n \; (Encryption) \qquad (4)$$
$$M = C^d \bmod n \; (Decryption) \qquad (5)$$

3. PROPOSED ALGORITHM

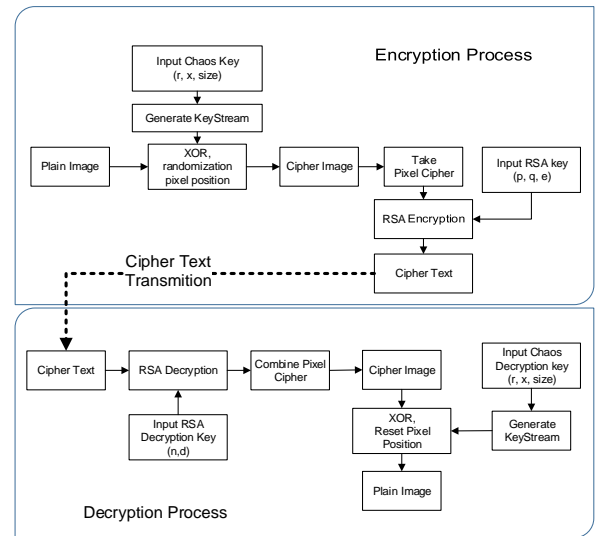The draft will be used in this study illustrated in Figure 1

Fig 1: Schematic Design in Doubles Encryption

From the Fig. 1 we can see that if a cryptanalyst managed to break the key of the RSA algorithm, then the next step to get the original image is to solve the second encryption algorithms which is Chaos-based algorithm. This will make the strength of the cipher can be assured

3.1 Encryption Algorithms

Multiple encryption algorithms are proposed as follow:

- Select the image to be encrypted (Plain images).
- Input an initial value which is variable x0,
- Generate an encryption key (eq. 1).
- Make the process of encryption by using the scheme XOR for each - each color component image with a key that was created earlier.
- Randomization pixel position (eq. 2). The results of the first step is cipher image.
- Extract the whole bit pixel of cipher image, then perform second encryption using RSA algorithms.
- For RSA algorithm first step is the inclusion of three variables, namely the value of p, q and e which is a key shaper to do encryption.
- Then proceed with the encryption process the whole bit pixel image that has been previously extracted (eq 4). Results of this whole process is in a cipher text of pixel values.

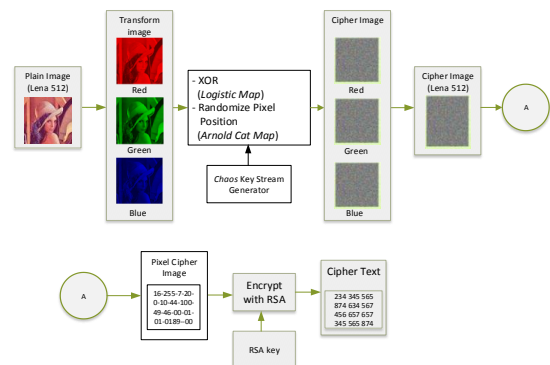Encryption process illustrated in Figure 2 :

Fig 2: Encryption Process

3.2 Decryption Algorithms

Image decryption algorithm is as follows:

- Select the cipher text.
- Enter the private key (n, d) to perform the decryption operation algorithm using RSA (eq. 5).
- From the second step of image pixel values obtained are not Encrypted which then will be reunited be cipher image.
- Next step is enter Chaos decryption key that has been previously used for encryption and generate Chaotic random key (eq. 1).
- Perform XOR operations and the process returns to the starting position pixel position using (eq. 3) then produced plain image or the original image.
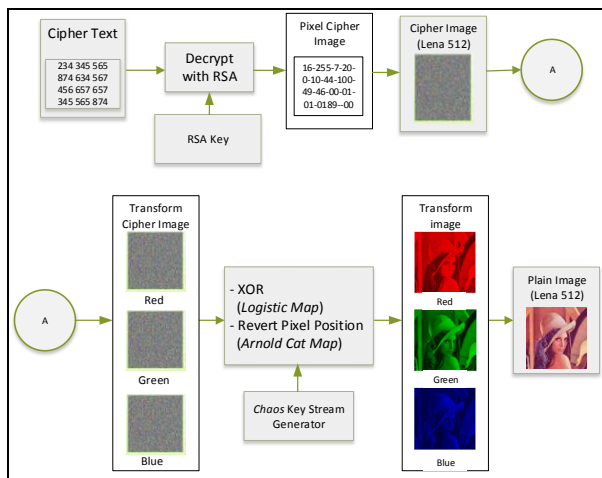
Encryption process illustrated in Figure 3 :

Fig 3: Decryption Process

4. EXPERIMENT RESULTS

Experiments in this study using Visual Studio 2012 software. The test image used is selected from grayscale and color images. Two test images used is 'mandril' with dimensions of 512x512 pixels and file size 768 KB shown in Figure 2 (a) and image 'Cameraman' with dimensions of 256x256 pixels and a size of 37 KB shown in Figure 2 (b). Both are standard image used in research on image processing. Keys are used in experiments is: x_0= 0.05678912, a = 78, b = 91, m = 2, p = 11, q = 17 and e = 7.

In this study, the time of encryption / decryption needed is not measured because of the many factors that causing changes such as process time optimization programming, hardware used, and forth.

4.1 Encryption and Decryption Results

Encryption Results used in the form of algorithm is cipher text, but to clarify the process that occurs, then the authors show the results of encryption on each algorithm. Chaos-based encryption algorithm will generate cipher image the form shown in Figure 4 (c) and 4 (d). The image of the encryption has been seen cannot be recognized. while the second encryption using the RSA algorithm will generate the cipher text as shown in the Figure 4 (e) and 4 (f). And decryption results are shown in Figure 4 (g) and 4 (h).
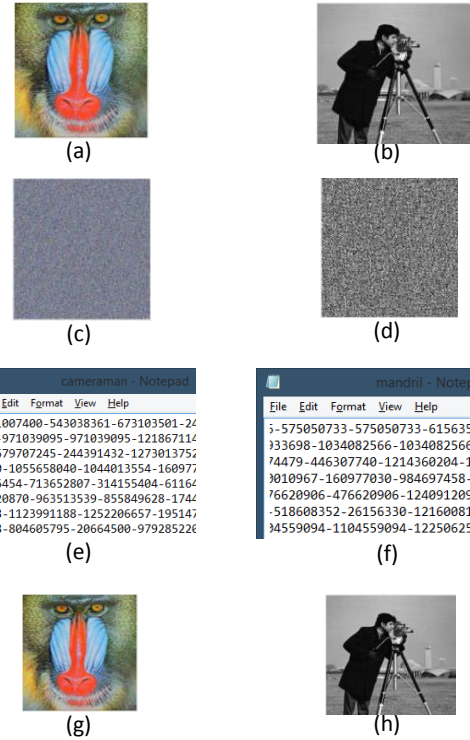

Fig 4 **(a) Plain image 'Mandril'; (b) Plain image 'Cameraman'; (c) Cipher image 'mandril'; (d) Cipher image 'cameraman'; (e) Cipher text 'mandril'; (f) Cipher text 'cameraman'; (g) decryption result 'mandril'; (h) decryption results 'cameraman '**

4.2 Performance Analysis

Measurement the speed efficiency from the proposed scheme using C# compiler on a computer of Core i5 CPU 2.5 GHz and 2 GB of RAM. The operating system used is Windows 8.1. The proposed algorithm are tested on the image size = 512x512 pixel and 256x256 pixel, key used x_0= 0.05678912, a = 78, b = 91, m = 2, p = 11, q = 17 and e = 7.

Table 1 shows the test result of the encryption speed proposed scheme and table 2 shows the comparasion speed from other encryption method.

Table 1. Performance Analysis

Test Image	Size	Key	Speed (ms)
Mandril	512 x 512	x_0= 0.05678912, a = 78, b = 91, m = 2 p = 11, q = 17, e = 7	1063
Cameraman	256 x 256		312

Table 2. Comparison test of the encryption speed of image size 512x512 in pixels.

Encryption scheme	Speed (s)
Ref. [4]	0,093
Ref. [1]	0,046
Ref. [6]	0,046
Proposed algorithm	1,063

Table 2 shows that the proposed algorithm takes a long time to complete an encryption process compared to other methods. This is because the encryption process will transform plain image into a base text cipher. On the other methods do not perform transformations on the generated ciher.

5. Security Analysis

Security analysis from the results of the encryption is done in two stages, on each encryption algorithms. It is intended to look at the stages that must be passed by a cryptanalyst if they want to break the cipher text. Security analysis on chaos-based encryption algorithm is done by analyzing histogram cipher image, key sensitivity of the algorithms, and statistical analysis using the correlation parameters and entropy. Whereas in the next stage is analysis in cipher text by looking at the key space available if carried out and analyze the cipher strength of a brute force attack. Security analysis show in Figure 5.
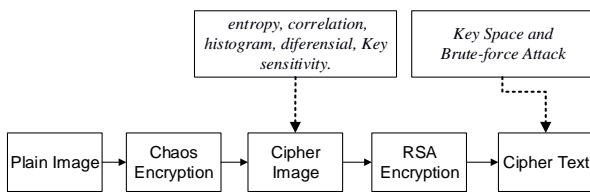

Fig 5: Schematic Security Analysis

5.1 Security Analysis Cipher Image

5.1.1 *Entropy*
Ideal entropy value was 7.99902 (≈8). Therefore encryption system designed safe from entropy attack [5]. Entropy of a message can be calculated using the formula [4]:

$$H_e = -\sum_{k=0}^{G-1} P(k) \log_2(P(k)) \qquad (5)$$

where G is the total number of symbols k (p(k)) is the probability of occurrence of symbol k and log denote the base 2 logarithm so that the entropy is expressed in bits. Let us suppose that the source produces 2^8 symbols with equal probability. The result from this calculation show in Table 3.

Table 3. Entropy and Correlation

Test Image	Size	*Entropy Value*
Mandril	512 x 512	7,7706
Cameraman	256 x 256	7,9771

From the Table 1 that the average entropy value from cipher images is 7.8735 (≈8). This means that the information contained in the images have been scrambled perfectly and safe from entropy attack

5.1.2 *Image Correlation*
An ideal encryption algorithm should produce the cipher images with no such correlation in the adjacent pixels (correlation ≈ 0) [4]. To calculate the correlation coefficient between plain image and cipher image we use the following equation:

$$r = \frac{n\sum(xy) - \sum x \sum y}{\sqrt{[n\sum(x^2) - (\sum(x)^2)][n\sum(y^2) - (\sum(y)^2)]}} \qquad (6)$$

Where n is the number of pixels and x is the pixel value from plain image and y is the pixel from cipher image. The result from this calculation show in Table 4.

Table 4. Image Correlation

Test Image	Size	*Correlation Value*
Mandril	512 x 512	0,0091281
Cameraman	256 x 256	0,004590

The correlation between adjacent pixels is almost close to zero. However, the two adjacent pixels in the plain image are highly correlated. This indicates that the proposed scheme possesses high security against statistical attacks.

5.1.3 *Histogram*
An ideal image encryption scheme should generate a cipher image with the different histogram from plain images. We calculated and analyzed histograms of encrypted images for the proposed algorithm, as well as their corresponding original images that have widely different content. The histogram result shown in Figs. 6. As shown in Fig. 6. The histograms of the cipher images, are significantly different from original images, and bear no statistical resemblance to the plain image.
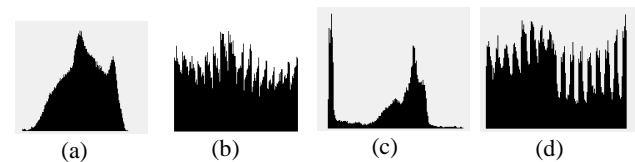

(a) (b) (c) (d)

Fig 6: (a) histogram Plain image 'Mandril'; (b) histogram Plain image 'Cameraman'; (c) histogram cipher image 'Mandril'; (d) histogram cipher image 'Cameraman';

Histogram from cipher image does not provide any clue to employ any statistical attack on the proposed image encryption procedure.

5.1.4 *Differential Attack*
To resist the differential attack, a minor change in the plain image should cause a significant change in the cipher image. To test quantitatively the influence of a one- pixel change on the cipher image. With the implementation of an encryption algorithm to an image, a change takes place in pixel values as compared to the values before encryption. Higher the change in pixel values, the more effective will be the image encryption and hence the quality of encryption.

To measures differential between plain image and cipher image, common method used, number of pixels change rate (NPCR) [13] and Encryption Quality [5], they can be defined as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \, x \, H} \, x \, 100\% \qquad (7)$$

$$EQ = \frac{\sum_{L=0}^{255} |H_L(C) - H_L(P)|}{2} \qquad (8)$$

Where in NPCR f is the pixel value on image matrix, (i,j) is position of pixel and m, n is height, width of image. Quality of encryption may be expressed in terms of the total deviation (changes) in pixel values between the original image and the encrypted one. Result from this experiment shown in Table 5.

Table 5. NPCR and Encryption Quality
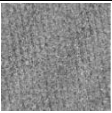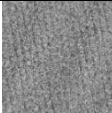
Test Image	Size	*NPCR*	*EQ*
Cameraman	256 x 256	99,69 %	41.134
Mandril	512 x 512	99,54 %	35.694

The NPCR measures the different pixel numbers between two images, and the EQ measures the different between pixel value from two image. The calculation results (NPCR and EQ) from plain images are shown in Table 5. From Table 5, we found that all of the NPCR are over 99.5% and EQ shows the magnitude of the variation in the plain pixel image after the encryption is done, This indicates that the encryption algorithm used has made the cipher image is much different from the plain image.

5.1.5 Key Sensitivity

A good image encryption procedure should be sensitive with respect to both the secret key and plain image. The change of a single bit in either the secret key or plain image should produce a completely different encrypted image. Key sensitivity is very important in a cryptographic system. In the chaos-based encryption small changes in the decryption key result huge change in the results of decryption. Testing the effects of changes Key meant to see if the decryption results using the wrong key. This test aims to see cipher image strength if performed experiments decryption use different keys. Table 6 show tests performed on change initial value (x_0). Initial value x_0 is used 0.05678912 different

Table 6. Key Sensitivity

Test Image	Decryption Results	
	Different: 0.0000001 $x_0 = 0.05678911$	**Different: 0.000001** $x_0 = 0.05678922$

The results are shown in Table 3. We found that the decrypted result are very different when using a small different key.

5.2 Security Analysis Cipher Text

5.2.1 Key Space

Key space is total number of different keys that can be used in the encryption process. For a secure image encryption, the key space should be large enough to make brute force attacks infeasible [3]. The proposed algorithm has a large key space, which is estimated as follows: Key parameters used in the algorithms used are a, b, m, x_0, r, n and e. Key a, b and m are used in Arnold Cat Map algorithm. While the value of x_0 and r used on Logistic Map algorithm to generate chaos and key *n* and *e* is the encryption key for the RSA algorithm. Values of a, b and m is a positive integer value so it is likely the key length used is $2^{32} = 4.3$ x 10^9 as well as the key n and e using a positive integer. For x_0 and r are double-precision or using standard floating-point IEEE $2^{53} = 10^{15}$ [10]. So it is likely that the key space is:

$$H(p, q, m, x_0, r, n, e) \approx (4.3 \text{ x } 10^9)^5 \text{ x } (10^{15})^2 \approx 21.5 \text{ x } 10^{75}$$

$$\approx (2^{32})^5 \text{ x } (2^{53})^2 \approx 2^{266}$$

Key space of the proposed algorithm is large enough to resist the brute-force attack. Table 7 shows the comparasion key space from other encryption method.

Table 7. Key space size of the proposed algorithm and other algorithms Encryption scheme.

Encryption scheme	Key Space
Ref. [4]	2^{349}
Ref. [2]	2^{128}
Ref. [6]	2^{256}
Proposed algorithm	2^{266}

5.2.2 Brute force attacks

Brute force attacks carried out by trying every possible key used to decrypt cipher. This type of attack usually takes a very long time even though most of them can unlock the existing cipher. To improve the cipher strength that is safe from this attack, the key used for encryption should be large enough. The larger key used for encryption, the longer the process will be done by cryptanalyst to crack and open the cipher text. If we look at the existing key length, then the brute force attack would require a very long time to be able to unlock the cipher text. So it can be concluded that the cipher text generated is safe from Brute force attack.

6. CONCLUSIONS

In this paper, the proposed algorithm is a combination of encryption algorithm for image using Chaotic System and RSA. Initially, the result is a change in the form of plain image to text base cipher. Experimental results and Security analysis indicate that the scheme is secure, one of the reason is, if a cryptanalyst managed to break the key of the RSA algorithm, then the next step to get the original image is to solve the second encryption algorithms which is Chaos-based algorithm. This will make the strength of the cipher can be assured and the simplicity of the proposed scheme makes it easy to implement in software. For future work, we will try to develop algorithms that can perform encryption on all image sizes and all types of images.

7. REFERENCES

[1] Amin, M., Abd El-Latif, A. A. (2010). Efficient modified RC5 based on chaos adapted to image encryption. Journal of Electronic Imaging, 19(1). doi:10.1117/1.3360179

[2] 13. Amin, M., Faragallah, O. S., & Abd El-Latif, A. A. (2010). A chaotic block cipher algorithm for image cryptosystems. Communications in Nonlinear Science and Numerical Simulation, 15, 3484–3497.

[3] Awad, A. dan Saadane, A. 2010. New Chaotic Permutation Methods for Image Encryption. IAENG International Journal of Computer Science

[4] El-latif, A. A. A., Li, L., Zhang, T., Wang, N., Song, X., & Niu, X. (2012). Digital Image Encryption Scheme Based on Multiple, 67–88. doi:10.1007/s11220-012-0071-z

[5] El-Fishawy, N., & Abu Zaid, O. M. (2007). Quality of encryption measurement of bitmap images with RC6, MRC6, and rijndael block cipher algorithms. *International Journal of Network Security*, *5*(3), 241–251.

[6] Faragallah, O. S. (2011). An efficient block encryption cipher based on chaotic maps for secure multimedia applications. Information Security Journal: A Global Perspective, 20(3), 135–147.

[7] Gaur, E. A., & Gupta, E. M. (2014). Review : Image Encryption Using Chaos Based algorithms, *4*(3), 904–907.

[8] Jolfaei A, Mirghadri A. (2011). Image Encryption Using Chaos and Block Cipher. Computer and Information Science. 4:1.

[9] Stallings, William. (2004). Cryptography and Network Security : Principles and Practice. Prentice-Hall, New Jersey

[10] Stinson, R, D. 2002. Cryptography Theory and Practice 2nd Edition. CRC Press Inc. Boca Raton, London

[11] Tang, Z., & Zhang, X. (2011). Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies, *6*(2), 202–206. doi:10.4304/jmm.6.2.202-206

[12] Taki, A. E., Deen, E., & Gobran, S. N. (2014). Digital Image Encryption Based on RSA Algorithm, *9*(1), 69–73.

[13] Wang, X., Zhang, Y., & Bao, X. (2015). A Colour Image Encryption Scheme Using Permutation-Substitution Based on Chaos, 3877–3897. doi:10.3390/e17063877

[14] Younes, M A B , Jantan A. (2008). "Image Encryption Using Block-Based Transformation Algorithm". IAENG International Journal of Computer Science. 35:1