International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Digital Image Cryptography Using Combination of Arnold's Cat Map and Bernoulli Map Based on Chaos Theory

Rama Dian Syah[1], Ruddy J Suhatril[2]
[1]Department of Technology and Engineering, Software Information System, University of Gunadarma, Indonesia
[2]Department of Technology and Engineering, University of Gunadarma, Indonesia

Abstract— *Data security is a very important requirement in information technology. Irresponsible parties can access data transmitted over the internet so that it can be detrimental to the data owner. Data security system is needed when data will be sent to other parties. Cryptography is a technique for data security with concept of making data unreadable by everyone. There are various kinds of techniques and algorithm to encode data. The cryptographic method in this study is by implementing chaos theory using Arnold's Cat Map and Bernoulli Map algorithms. The two algorithms are combined and produce encryption techniques to increase the security of the data sent by the sender to the recipient without being known by others. The algorithm is applied to process of encryption and decryption in grayscale and RGB digital images. The results of this study indicate that image file can be encrypted properly. The time of the encryption and decryption process depends on the size of the image. Histogram shows the difference between original image and encrypted image. Low PSNR values in encrypted image indicate good image quality. The distribution of pixels that spread on the encrypted image explains the low correlation of pixels.*

Keywords— *Arnold's Cat Map, Bernoulli Map, Chaos, Cryptography*.

I. INTRODUCTION

The development of information technology today has helped humans to process information retrieval and information delivery. This convenience can pose many threats to the security of data and information. Data security that supports privacy is one of these protections.

Examples of hacking cases that threaten security have occurred in Hollywood artist named Adele according to CNN Indonesia News. This news explains the hacking of personal photos starting from email burglary. Adele's personal photos that have never been released to the public are spread on social media by hackers.

From the case it can be seen that the image can contain information that is privacy and confidential. Images have more information that text. An Image data security technique is needed to limit access to information by irresponsible parties.

Encryption is a technique to increase security on a data, where the data will be scrambled. The encryption data will be difficult to decrypting without knowing the specific code or password.

Encryption can be applied to an image. Image encryption is a method for maintaining image privacy information from unauthorized access [1]. Image encryption can be done at fast time with high level of security [2].

Image encryption based on chaos theory is an encryption technique that has speed, security, and good computing [3]. Chaos is applied to image encryption in form of functions. The chaos function is a function that is random and sensitive to the initial value [4]. One function that applies the chaos function is Bernoulli map.

Image Encryption with Bernoulli map is combined with Arnold's cat map to improve encryption security. The concept of encryption is to shuffle the position of pixels by Arnold's cat map then keystream are generated using Bernoulli map functions and the value of pixels are manipulated by operation XOR to produce an encrypted image.

The results of the encryption and decryption process can be analysed including time analysis, histogram analysis, image quality analysis, and correlation analysis.

II. LITERATURE REVIEW

A. Chaos Theory

Chaos theory is a branch of mathematics that is related to non-linier dynamic systems [5]. Chaos theory is a movement that is randomly depends on the initial conditions. A very small change in the initial value will produce a different row of values.

Chaos on cryptography is used in the form of function. Repetition in the chaos function will generate keystream based on the initial value. The resulting image of encryption will be different according to the changes in initial values so that the possibility of a force attack continuously searching for secret key will be difficult.

B. Bernoulli map

Bernoulli map proposed in the research by Hossam and Ayman is a development algorithm of logistic map and is a chaos function used in cryptography [6]. Random behavior generated from this function can provide good combination of speed, complexity, and high security. The Bernoulli map function is defined as equation [6]:

$$X_{n+1} = r \times X_n \ mod\ 1$$

The value of X_n and the value of r are the secret keys. Both of these values are decimal numbers. The value range $X_n \in [0, 1]$ with the initial value starting from 0.1. The value range $r \in [1, \infty]$ [6]. Bernoulli map function will produce keystream.

C. Arnold's Cat Map

Arnold's Cat Map is a chaotic function with the concept of shuffling the position or coordinates of pixels by not changing

Rama Dian Syah and Ruddy J. Suhatril, "Digital Image Cryptography Using Combination of Arnold's Cat Map and Bernoulli Map based on Chaos Theory," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 2, pp. 258-262, 2019.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

pixel values. ACM will shuffle the pixel coordinates in the original image to the new pixel coordinates in the encrypted image [8]. The Arnold's Cat Map equation for the encryption process is defined as equation [1]:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod\,(N)$$

The values of p and q are positive integers. These values are the secret keys of ACM. To return the original pixel position or coordinates using the ACM decryption equation which is defined as equation [1]:

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} \frac{pq+1}{pq+1-pq} & \frac{-p}{pq+1-pq} \\ \frac{-q}{pq+1-pq} & \frac{1}{pq+1-pq} \end{bmatrix} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} mod(N)$$

The ACM equation for decryption process is invers equation of the encryption process.

D. XOR operation

XOR operation on cryptography is used to manipulate pixel value of original image into pixel value of encrypted image. Pixel value of original image is carried out by the XOR operation with the keystream generated by the Bernoulli map function. The XOR operation in the encryption process is defined as equation [7]:

$$I_C = I_P \oplus I_K$$

I_c is the pixel of encrypted image, I_p is the pixel of original image and I_k is the keystream that are generated by Bernoulli map function. The XOR operation in the decryption process is defined as equation [7]:

$$I_P = I_C \oplus I_K$$

XOR operation equation in decryption process is the opposite of XOR operation equation in encryption process.

III. PROPOSED METHOD

This research is conducted in 5 steps of research: (1) encryption; (2) decryption; (3) time analysis; (4) histogram analysis; (5) image quality analysis; (6) correlation analysis. The step of research is shown if Figure 1.

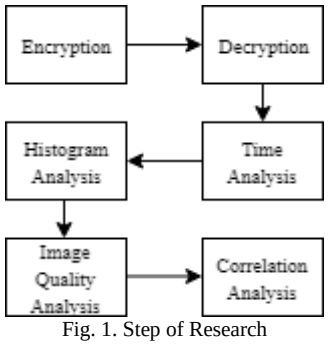


Fig. 1. Step of Research

The process of encryption and decryption is carried out on digital images with square dimensions with grayscale and RGB color types. The results of the encryption and decryption will be analyzed.

A. Encryption Flow Diagram

The encryption process using combination algorithm between Arnold's cat map and Bernoulli map. The encryption process is shown in Figure 2.

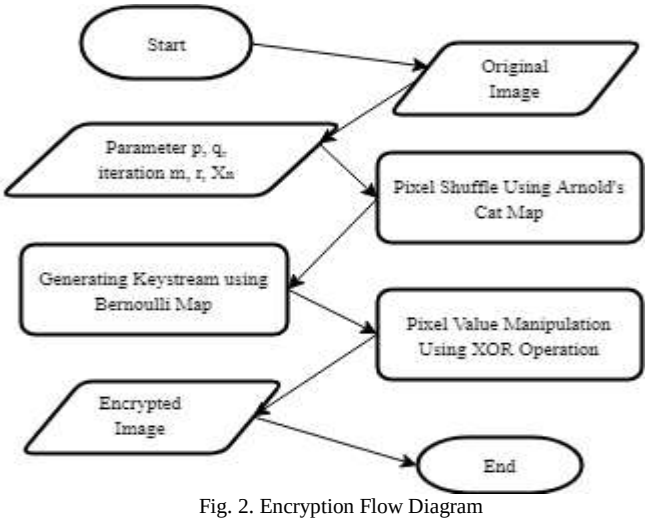


Fig. 2. Encryption Flow Diagram

B. Decryption Flow Diagram

The decryption process is the opposite of encryption process. The decryption process is shown in Figure 3.

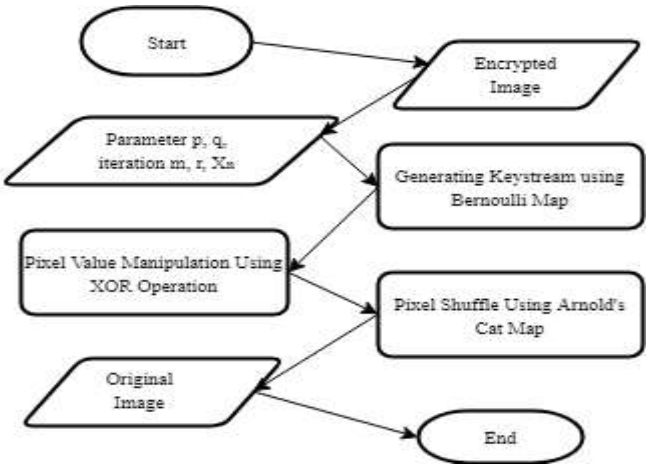


Fig. 3. Decryption Flow Diagram

IV. RESULTS AND DISCUSSION

The data test are grayscale image and RGB image with square image. The display of data test is shown in Table 1.

TABLE 1. Data Test

Data Test	Grayscale Image	Name	Color Type	Size (Pixel)
Data 1		Watch .png	*Gray scale*	256×256
Data 2				360×360
Data 3				512×512
Data 4				720×720
Data 5				1024×1024
Data 6		Monarch .png	*True color*	256×256
Data 7				360×360
Data 8				512×512
Data 9				720×720
Data10				1024×1024

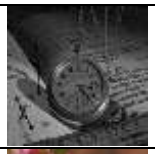
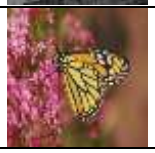
The data test is encrypted and decrypted with parameter p = 2, q = 3, *iteration* m = 4, X_n = 0.1, and r = 2.3. The results of

Rama Dian Syah and Ruddy J. Suhatril, "Digital Image Cryptography Using Combination of Arnold's Cat Map and Bernoulli Map based on Chaos Theory," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 2, pp. 258-262, 2019.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

the encryption and decryption process is shown in Table 2.

TABLE 2. Result of Encryption and Decryption Process

Data Test	Original Image	Encrypted Image	Decrypted Image
Data 1			
Data 2			
Data 3			
Data 4			
Data 5			
Data 6			
Data 7			
Data 8			
Data 9			
Data 10			

A. *Time Analysis*

The purpose of time analysis is to calculate the length of time of encryption and decryption process using data test in figure 1. The graph for the encryption process time using grayscale and RGB data test is shown in Figure 4 and 5.

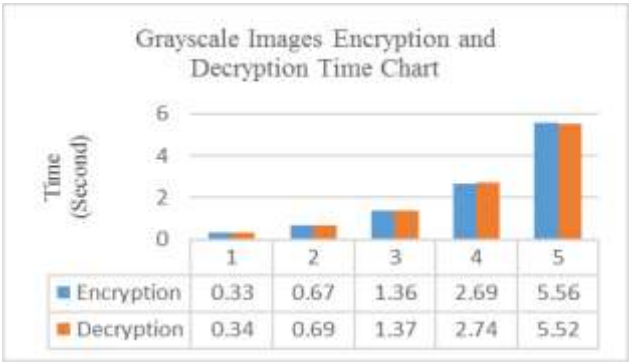


Fig. 4. Grayscale Images Encryption and Decryption Time Chart

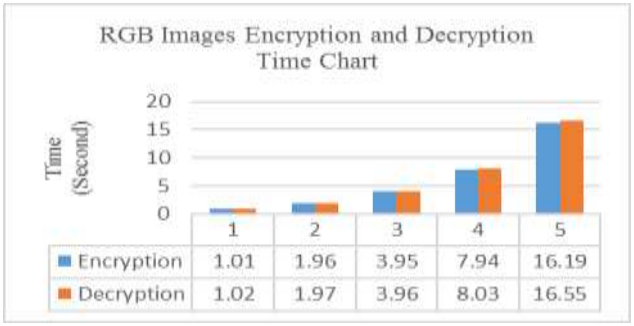


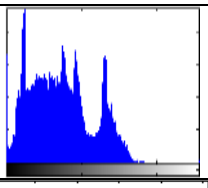
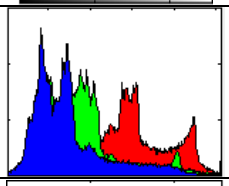
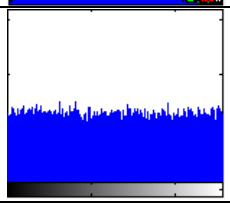
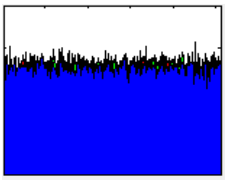
Fig. 5. RGB Images Encryption and Decryption Time Chart

The time process for RGB images is longer than grayscale images. Encryption process in color images is done in 3 color channels.

B. *Histogram Analysis*

The histogram of the image is the frequency intensity of pixel values in image [9]. The histogram on the image can show the level security of the image encryption system. The difference between the histogram on encrypted image and original image shows that the encryption algorithm has a good level of security [10]. The histogram between original image and encrypted image is shown in Table 3.

TABLE 3. Histogram

Image Type	Nama dan Tampilan Citra	Histogram
Original Image	 Watch.png	
	 Monarch.png	
Encrypted Image	 Encrypted Watch.png	
	 Encrypted Monarch.png	

The histogram of the encryption image is different from the original image because the algorithm shuffling and manipulating value of the pixels.

C. *Image Quality Analysis*

Image quality in this research is measured using PSNR (Peak Signal Noise to Ratio) between original image and encrypted image. The PSNR is defined as equation [11]:

$$PSNR = 10\ Log_{10}\left(\frac{a^2\ max}{MSE}\right)$$

MSE (Mean Square Error) is needed to find the PSNR value. The MSE is difined as equation:

$$MSE = \frac{1}{MN}\sum_{X=1}^{M}\sum_{y=1}^{N}(a_{xy} - b_{xy})^2$$

The values of x and y are image coordinates, M and N values are dimension of image. Value of A is pixel of encrypted image and value of B is pixel of original image. The values of MSE and PSNR between original image and encrypted image is shown in Table 4.

TABLE 4. Image Quality

Original Image	Encrypted Image	Size (Pixel)	PSNR (dB)
Watch.png	Encrypted Watch.png	256 × 256	-37.13
		360 × 360	-40.06
		512 × 512	-43.12
		720 × 720	-46.06
		1024×1024	-49.09
Monarch.png	Encrypted Monarch.png	256 × 256	8.54
		360 × 360	8.56
		512 × 512	8.60
		720 × 720	8.64
		1024×1024	8.66

Rama Dian Syah and Ruddy J. Suhatril, "Digital Image Cryptography Using Combination of Arnold's Cat Map and Bernoulli Map based on Chaos Theory," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 2, pp. 258-262, 2019.

D. Image Correlation Analysis

Correlation in the image is the relationship between adjacent pixels in the original image and encrypted image. Image correlation is very useful for measuring the quality of image encryption [12]. The quality of good image encryption is encrypted by algorithm that can randomize the relationship of pixel in original image and decrypted image [13]. The coefficient correlation is defined as equation [14]:

$$cc = \frac{cov(x,y)}{\sigma x \times \sigma y}$$

Where:

$$\sigma x = \sqrt{var(x)}$$

$$\sigma y = \sqrt{var(y)}$$

$$var(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 E(x) = \frac{1}{N}\sum^{N} x_i$$

$$cov(x,y) = \frac{1}{N}(x_i - E(x))(y_i - E(y))$$

The value of *cc* is the correlation coefficient. The values of *x* and *y* are adjacent pixels. The value of *N* is the number of pixels used and the value of *E* is the average value.

Correlation is calculated on two adjacent pixels between pixels *f(x,y)* with pixels horizontally *f(x,y+1)*, pixels *f(x,y)* with pixels vertically *f(x+1,y)* and pixels *f(x,y)* with pixels diagonally *f(x+1,y+1)* in the original image and encrypted image [1]. The image used for correlation analysis is image with size of 256 × 256. The result of correlation calculation is shown in Table 5.

TABLE 5. Image Correlation

Image	Correlation		
	Horizontal	Vertical	Diagonal
Watch.png	0.84538	0.83561	0.82811
Encrypted Watch.png	-0.00356	0.00033	0.00128
Monarch.png	0.76712	0.84147	0.73675
Encrypted Monarch.png	-0.00023	-0.00255	0.00086

The distribution correlation of adjacent pixels can be seen in images. Pixel distribution can be seen in grayscale and RGB image, which is show the spread of pixels in the original image and encrypted image. Pixel distribution is shown in Table 6 and 7.

The distribution pixel around 45° line indicates strong relationship of pixel adjacent correlation, whereas the distribution spread around the image indicates weak relationship of pixel adjacent correlation.

V. CONCLUSION

In this research of analysis on digital image cryptography using combination of Arnold's cat map and Bernoulli map is done. The technique of encryption has processing time based on image size. Differences in the histogram indicate the original image can be encrypted successfully. The low PSNR value and weak adjacent correlation pixel indicate this technique of encryption has high security.

TABLE 6. Image Pixel Distribution 'Watch' and 'Encrypted Watch'

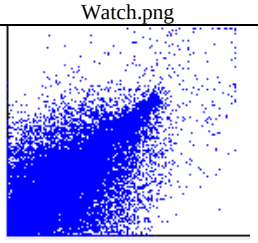
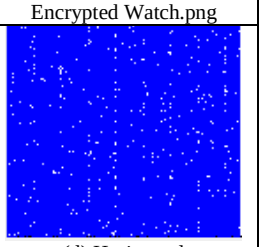
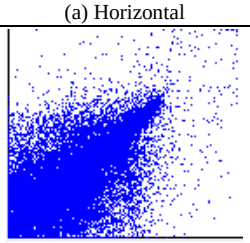
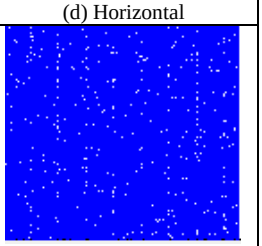
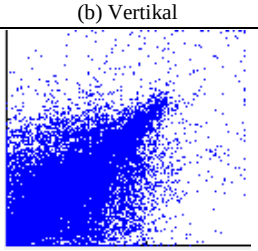
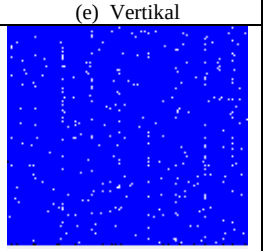
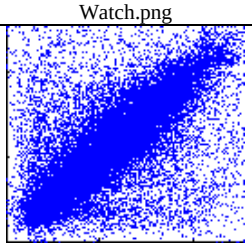
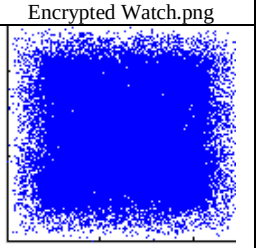
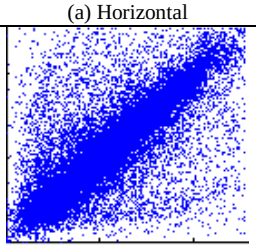
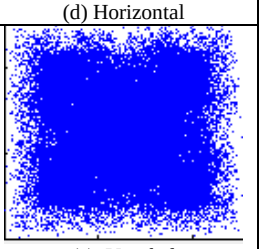
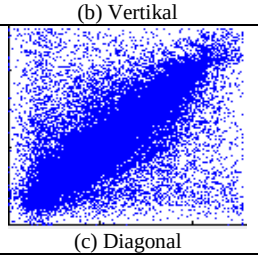
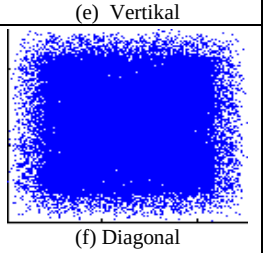
Watch.png	Encrypted Watch.png
 (a) Horizontal	 (d) Horizontal
 (b) Vertikal	 (e) Vertikal
 (c) Diagonal	 (f) Diagonal

TABLE 7. Image Pixel Distribution 'Monarch' and 'Encrypted Monarch'

Watch.png	Encrypted Watch.png
 (a) Horizontal	 (d) Horizontal
 (b) Vertikal	 (e) Vertikal
 (c) Diagonal	 (f) Diagonal

REFERENCES

[1] R. Munir. "Analisis Keamanan Algoritma Enkripsi Citra Digital Menggunakan Kombinasi Dua Chaos Map dan Penerapan Teknik Selektif," *Journal Ilmiah Teknologi Informasi*, vol. 10, issue 2, pp. 89-95, 2012.

[2] M.T. Suryadi, E. Nurpeti and D. Widya. "Performance of Chaos-Based Encryption Algorithm for Digital Image." *Telecommunication Computing Electronics and Control*, vol. 12, issue 3, pp. 675-682, 2014.
[3] W. Zhang, K. Wong, H. Yu and Z. Zhu. "An Image Encryption Scheme Using Reverse 2-Dimensional Chaotic Map and Dependent Diffusion," *Journal of Communication in Nonlinear Science Numerical Simulation*, vol. 18, issue 8, pp. 2066-2080, 2013.
[4] R. Purba, A. Halim and I. Syahputra. "Enkripsi Citra Digital Menggunakan Algorimta Arnold's Cat Map dan Nonlinier Chaotic Algorithm." *Journal Sifo Mikroskil*, vol. 15, issue 2, pp. 61-71, 2014.
[5] G. Boeing. "Visual Analysis of Nonlinear Dynamical Systems: Chaos, Fractals, Self-Similarity and Limits of Predictions." *Systems*, vol. 4, issue 37, pp. 1-18, 2016.
[6] E. Ahmed. "Image Encryption Using Development of Chaotic Logistic Map Based on Feedback Stream Cipher," in *Proceedings Tele-Info*, pp. 274-283, 2014.
[7] K. Gupta and S. Silakari. "New Approach for Fast Color Image Encryption Using Chaotic Map." *Journal of Information Security*, vol. 2, issue 4, pp. 139-150, 2011.
[8] B.A. Wijaksono. "Steganografi Pada Citra Digital Dengan Metode Cat Map dan Outguess." *Satuan Tulisan Riset dan Inovasi Teknologi*, vol. 1, issue 3, pp. 317-324, 2017.
[9] H. Kaur and N. Sohi. "A Study for Applications of Histogram in Image Enhancement." *The International Journal of Engineering and Science*, vol. 6, issue 6, pp. 59-63, 2017.
[10] A. Jolfei and A. Mighadri. "An Image Encryption Approach Using Chaos and Stream Chiper." *Journal of Theoritical and Applied Information Technology*, vol. 19, issue 2, pp. 117-125, 2010.
[11] D.M. Setiadi, E.H. Rachmawanto, and C.A. Sari."Implementasi One Time Pad Kritografi pada Gambar Grayscale dan Gambar Berwarna," *in Proceedings Seminar Ilmu Nasional Multi Disiplin Ilmu*, pp. 50-56, 2017.
[12] I.F. Elashry. "Hemomorphic Image Encryption." *Journal of Electronic Imaging*, vol.18, issue 3, pp. 033002, 2009.
[13] S.H. Kamali, R. Shakerian, M. Hedayati and M. Rahmani. "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption." *In Proceedings ICIE*, pp. 141-145, 2010.
[14] S.Somaraj and M.A. Hussain. "Performance and Security Analysis for Image Encryption Using Key Image." *Indian Journal of Science and Technology*, vol.8, issue 35, pp. 1-4, 2015.