International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Arnold's Cat Map Algorithm in Digital Image Encryption

Eko Hariyanto[1], Robbi Rahim[2]

[1]Faculty of Computer Science, Universitas Pembangunan Panca Budi, Jl. Jend. GatotSubroto Km. 4,5SeiSikambing, 20122, Medan, Sumatera Utara, Indonesia

[2] Faculty of Computer Science, Universitas Pembangunan Panca Budi, Universitas Prima Indonesia

Abstract: ***Cryptography is a field that has developed very rapidly with the number of algorithms that keep popping up with this type of symmetric and asymmetric which has advantages and disadvantages of each, the algorithm Arnold's Cat Map is one type of cryptographic algorithms to secure the digital image by performing iterations for n in the pixel image and the outcome can not be known without knowing the value of a process of iteration***

Keyword: Cryptography, Arnold's Cat Map, Digital Image Encryption, Image Cryptography

1. Introduction

Computer security is a branch of technology known as information security as applied to computers. Computer security objectives are among others the protection of information against theft or corruption, or the preservation of availability, as outlined in the security policy*[1]*.

Image is one of the important forms of multimedia. Image visually present information and information presented by a richer image than presented textually*[2]*. Digital images are not only stored in the storage such as hard disks, flash drives, CDs, DVDs, and other storage device, but also transmitted via public channels such as the internet. For the image of the private or confidential, storage and transmission of images need to pay attention to security aspects. The image that is private personal documents such as photos can only be seen by the owners or those who are given authority only *[2]*, confidential example is the image of the remote sensing (satellite photo) recording potential of natural resources of a country*[2]*.

Recently an effective security of a system is needed for daily business activities. A secure system can provide a high level of confidence to the user so that it can add value and efficiency to the system itself. Users will feel comfortable and safe when dealing with a system that can secure user data from attackers.

In addition to the image of private and confidential, the security aspect is an important feature in the image paid. Only paid customers who can access the information in the image. A digital video is essentially composed by a series of still image frames are displayed in a very short time. For the industry of multimedia such as Pay TV or video on demand, protection against broadcast video plays an important role, because video broadcasts transmitted by broadcast through the transmission line (which can be intercepted) but only paying customers are able to enjoy live TV, while the illegal subscribers are not can access the video broadcast.

Researchers have developed a lot of cryptographic algorithms for encryption, but most algorithms are intended to encrypt messages in text form. Although conventional encryption algorithms such as DES, AES, Blowfish, Serpent, RC4, RSA, ElGamal, Rabin, can also encrypt images *[3]*, but the algorithm is safe enough to be applied. This is due to the image have different characteristics with textual data. An image generally has a data capacity is very large, so the image encryption requires large computational volume. Some applications that have a need for real-time such as teleconferencing, live video streaming, and others, obviously require very high computing speed that the conventional algorithm is obviously not suitable for encrypting image*[3]*.

Arnold's Cat Map algorithm (ACM) is one of the cryptographic algorithm used to encrypt the image *[4]*The concept of the algorithm is continuously rotate the image so that it becomes a form that is not visible and random so that the image can not be seen by the naked eye but can still be recognized by the system for image file (image) of the same *[4]*.

2. Arnold's Cat Map Algorithm

Chaos is a common technique used in the random number generator*[5]*, it's happening because this technique is faster and easier to use in the process stream object both in terms of storage and process objects Only a few functions (chaotic maps) and some parameters (inital conditions) were quite good used if the process takes quite a long time *[5]*.

Arnold's Cat Mapare chaotic two dimensions that can be used to change the position of the pixel of the image without removing any information from the image*[6]*, pixel image can be assumed by S = {(x, y) | x, y = 0, 1, 2 ... N-1} . 2-dimensional image of Arnold's Cat Map can be written by the following equation:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ n)$$

$$\begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ n)$$

Where p and q are positive integers, the determinant (A) = 1. (x ', y') is the new position of the original pixel position (x, y) when Arnold's Cat Map algorithm performed once. Results after application of Arnold's Cat Map to the number of iterations of iterations R will be a random drawing that contains all the values of the same pixel of the original image. The number of iterations R to complete depending on the parameters p, q and N size of the original image. So Arnold's Cat Map algorithm has parameters p, q, and the number of iterations R, all can be used as a secret key*[6]*.

3. Experiment And Result

The analysis algorithm used in this study is Arnold's Cat Map algorithm, here are the steps how algorithms work Arnold's Cat Map

a) Read the color pixel RGB On Citra
b) Calculate the position X, Y pixel in the image to be encrypted
c) rotation (iteration) RGB pixels to the image to be random and can not be recognized.

Based on the above process design scheme writer IPO (Input Process Output) from the analysis are discussed, below is a schematic diagram

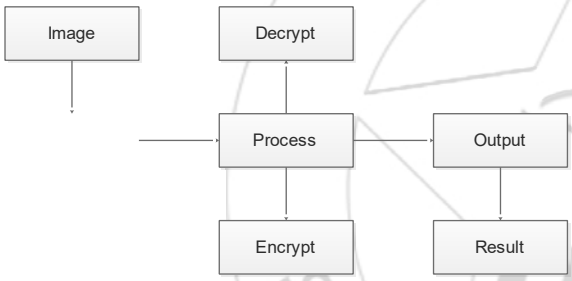

Figure 1: Input Process Output System Arnold's Cat Map

The process of encryption and decryption algorithms Arnold's Cat Map performed at an image size of 200 x 223, this measure is a measure of non aspect ratio sehing Width and Height is not the same, then the image drawn pixel by 4 x 4 to the encryption process, so the image will be rotated by 4x4 until the entire pixel n rotated entirely, for the encryption and decryption process is used the following formula

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ cc & b+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod(n)$$

The above formula is the formula of encryption, decryption for the following formula

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} \bmod(n)$$

The above formula is the formula of decryption, after the formula determines the encryption and decryption, then the next step is the author took a shot to take the pixel values of an image, the following picture

Figure 2: Author Picture

Figure 2 is an image that will be the author of encryption, the first step the authors took the RGB value of the image values to be encrypted, making processes RGB values is done using matlab software, the resulting value very much, here are sample results obtained RGB

Tabel 1: RGB Value

104	134	144	139	150	163	162	155	161
88	124	140	139	152	167	159	146	135
84	123	141	140	154	169	157	138	136
81	120	135	124	133	152	162	164	150
78	121	141	132	135	149	159	162	156
76	123	148	139	136	143	149	154	153
79	123	148	141	137	139	138	139	138
83	120	141	137	136	136	130	128	125
82	116	134	131	132	133	129	129	127
77	111	130	127	128	131	134	142	138
70	107	129	126	124	130	141	156	146

As an initial test authors take the RGB values of the values listed in Table 3.1 as 3x3 pixels, and the results of its value

Table 2: Sample 3X3 Pixel

Pos Pixel	0	1	2
0	104	134	144
1	88	124	140
2	84	123	141

After obtaining the pixel value, next perform encryption and decryption algorithms Arnold's Cat Map, the following processEncryption and decryption process includes pixel shuffle and shuffle to the pixel according to the equation formula is as follows:

$$\begin{bmatrix} 1 & 134 \\ 84 & 134+84+1 \end{bmatrix} x \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \bmod 3 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 134 \\ 84 & 134+84+1 \end{bmatrix} x \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 84 & 219 \end{bmatrix} = \begin{bmatrix} 0 \\ 303 \end{bmatrix} \bmod 3 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 134 \\ 84 & 134+84+1 \end{bmatrix} x \begin{bmatrix} 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 168 & 438 \end{bmatrix} = \begin{bmatrix} 0 \\ 606 \end{bmatrix} \bmod 3 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 134 \\ 84 & 134+84+1 \end{bmatrix} x \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 134 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 135 \\ 0 \end{bmatrix} \bmod 3 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 134 \\ 84 & 134+84+1 \end{bmatrix} x \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 134 \\ 84 & 303 \end{bmatrix} = \begin{bmatrix} 135 \\ 387 \end{bmatrix} \bmod 3 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 134 \\ 84 & 134+84+1 \end{bmatrix} x \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 & 134 \\ 168 & 438 \end{bmatrix} = \begin{bmatrix} 135 \\ 606 \end{bmatrix} \bmod 3 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 134 \\ 84 & 134+84+1 \end{bmatrix} x \begin{bmatrix} 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 & 268 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 536 \\ 0 \end{bmatrix} \bmod 3 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 134 \\ 84 & 134+84+1 \end{bmatrix} x \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 & 268 \\ 84 & 303 \end{bmatrix} = \begin{bmatrix} 536 \\ 387 \end{bmatrix} \bmod 3 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 134 \\ 84 & 134+84+1 \end{bmatrix} x \begin{bmatrix} 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 2 & 268 \\ 168 & 438 \end{bmatrix} = \begin{bmatrix} 536 \\ 606 \end{bmatrix} \bmod 3 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$$

The above process is an iterative process - first, for the iteration process is dynamic based on the number of pixels and the wishes of the user, the author uses only one iteration just to prove Arnold's Cat Map algorithm, and the results pixels after doing iteration as follows:

Table 3: Result*Arnold Cat Map*

Pos Pixel	0	1	2
0	84	134	104
1	88	124	140
2	144	123	141

Encryption and decryption algorithms Arnold's Cat Map totally different, because the process of iterating through n will restore the image changes into the form of the initial results, the following are some of the results of iterations of the algorithm Cat Folders writer Arnold trials with a prototype system that the author made

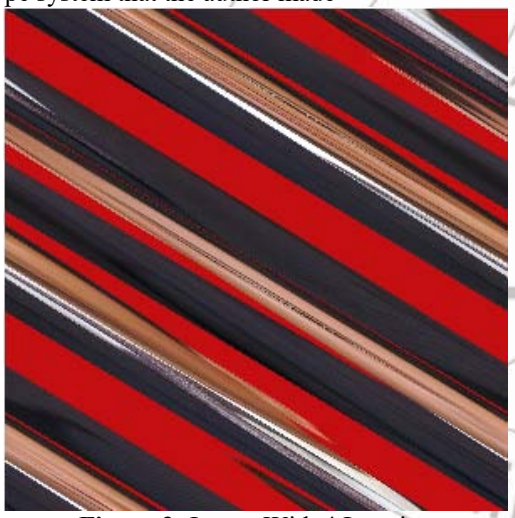

Figure 3: Image With 4 Iteration

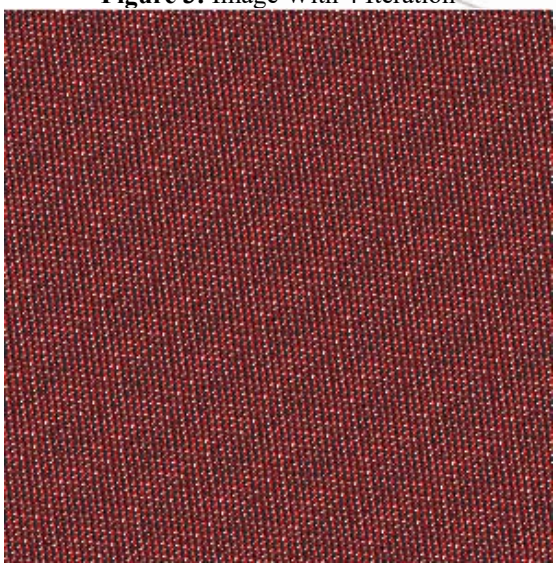

Figure 4: Image With 28 Iteration

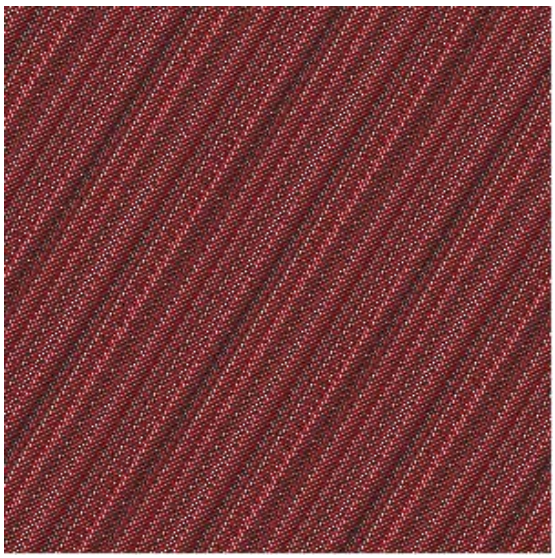

Figure 5: Image With 96 Iteration

Figure 3 to 5 are the result of the iterative process that the author did, the results of the sample image looks the iteration process with Arnold's Cat Map algorithm can randomize the image properly without reducing the value of the pixel in the image

4. Conclusion

Algorithms Arnold's Cat Map is Encryption is good enough to secure a digital image, especially in the security pixel mostly algorithm cryptography secures files or specific to text, berdeda with other algorithms Arnold's Cat Map could safeguard the image of a well without reducing the value or information of a digital image that is secured and this is one of the advantages of this algorithm is the author of the analysis of this study

References

[1] S. Kromodimoeljo, Teori & Aplikasi kriptografi, Medan, Indonesia: SPK Consulting, 2009.
[2] R. Munir, Pengolahan Citra Digital, Jakarta, Indonesia: Informatika , 2004.
[3] N. A. Abbas, "Image encryption based on Independent Component Analysis and Arnold's Cat Map," Egyptian Informatics Journal, pp. 139-146, 2016.
[4] R. Purba, A. Halim and I. Syahputra, "Enkripsi Citra Digital Menggunakan Arnold's Cat Map Dan Nonlinear Chaotic Algorithm," JSM STMIK Mikroskil, vol. XV, no. 2, pp. 61-71, 2014.
[5] E. AVAROĞLU , "Pseudo Random Number Generator Based on Arnold's Cat Map and Statistical Analysis," Turkey, 2011.
[6] P. Gupta, S. Singh and I. Mangal, "Image Encryption Based On Arnold Cat Map and S-Box," IJARCSSE, vol. IV, no. 8, pp. 807-812, 2014.