Digital Image Security Application With Arnold Cat Map (ACM)

A M H Pardede¹, Dahlan Abdullah², Budhi Santri Kusuma³, Citra Kurniawan⁴, Suwarni⁵, Akbar Iskandar⁶, Lusi Dwi Putri⁷, Cut Ita Erliana⁸, Fitri Irwansyah⁹, A Saleh A⁶, S Sriadhi¹⁰ and H Hartono¹¹

¹College of Informatics Management and Computer Science, St. Mark's University
²Department of Informatics, Universitas Malikussaleh, Aceh, Indonesia
³Department of Electrical Engineering, Universitas Medan Area, Medan, Indonesia
⁴Department of Industrial Engineering, Sekolah Tinggi Teknik Malang, Malang, Indonesia
⁵Department of Management, Universitas Dehasen Bengkulu, Indonesia
⁶Informatics Engineering, STMIK AKBA, Makassar, Indonesia
⁷Department of Civil Engineering, College of Engineering, Universitas Lancang Kuning, Pekanbaru, Indonesia
⁸Department of Industrial Engineering, Universitas Malikussaleh, Aceh, Indonesia
⁹Statistics, Financial, & Social Sciences Research Group, Indonesia
¹⁰Department of Electrical Engineering, Universitas Negeri Medan, Indonesia
¹¹Department of Computer Science, STMIK IBBI, Medan, Indonesia

* dahlan@unimal.ac.id

Abstract. The development of science and technology is advancing. Therefore, the data security needs to be applied. Cryptography is one of the sciences that learn mathematical techniques related to aspects of information security such as secrecy. One of them is known as the Arnold Cat Map (ACM) algorithm on encryption and decryption by iterating digital images to secure an image. Arnold Cat Map (ACM) algorithm is one of the common cryptographic algorithms used to encrypt images. Application designed to secure an image by performing the process of randomizing the image pixel, the randomized image will change the pixel position based on the Arnold Cat Map method, then encryption and then the image encryption results become unknown. The result of the Arnold Cat Map method is that the random pixel position will return to its original position after going through several iterations with reference to the image capacity, where if the image size is different, the iteration will return to the original with different iteration point at time of encryption or decryption system by Arnold Cat Map method.

Introduction

Nowadays, the development of information technology is very important especially in an imaging technology, which is included in image transmission and image iteration. Therefore, many people have developed a security by utilizing imaging technology in the process of randomizing pixels to protect an image. The problem that there are many stealing cases of images done by unauthorized parties due to this sophistication. [1] Proposed super encryption cryptography with IDEA and WAKE algorithm. [2] proposed a combination base64 and hashing variable length for securing data. [3] proposed
combination base64 and EOF Technique for steganography. Another research from [4] using prime number comparison using Sieve of Eratosthenes and Sieve of Sundaram Algorithm to generate prime number that can be used in cryptography. The research of [5] using keylogger for monitoring user activity, and [6] using deterministic dynamic programming algorithm. The usage of cryptography can be applied in website to ensure the web security[7],[8],[9]. Cryptography process must also follow the benchmarking process to ensure the efficiency[10],[11],[12].

Arnold Cat Map Algorithm (ACM) is one of the cryptographic algorithms commonly used to encrypt images [13]. The concept of this algorithm is to rotate the image continuously so that it becomes an invisible and random form so that the image cannot be seen easily but can still be recognized by the system for the same image file.

The purpose of this paper is: (1) to implement Arnold Cat Map (ACM) algorithm on digital image security with Adobe Dreamweaver CS3 programming language, (2) to produce applications that are specific to securing digital images with *Jpg format, (3) to design and implement a security system for digital image encryption algorithms with the Arnold Cat Map (ACM) algorithm, (4) to make it easier for users to secure digital images from unauthorized parties.

Related Works

ACM is a one-to-one mapping which means that each pixel position is translated to another position uniquely [14]. This chaotic function was discovered by Vladimir Arnold in 1960, who used the image of a cat as his experiment. The process that occurred in each ACM iteration is a shear in the y direction, then in the x direction, and all the results (which may be outside the drawing area) were modulated with N to remain in the image area (area preserving).

ACM iterations of an image will randomize the image, which is the same as encrypting the image. By doing iterations many times, a different random image is obtained. However, after a certain iteration, the original image will return, that is why ACM has a limit/period.

Security is one of the essential things and must be done in order to maintain information so that data cannot be stolen by irresponsible parties. Image picture is one of the most widely used forms of media and many of the images are used by irresponsible parties, so they need to be secured by a cryptographic mechanism. In this study, the author chose the Arnold Cat Map algorithm as an encryption and decryption algorithm.

Research Methodology

The encryption and decryption process in the Arnold Cat Map (ACM) algorithm was done on an image size of 3x3. This size is a non-aspect ratio measurement, so the width and height of the images were the same, and then the pixel is 3 x 3 for the encryption process, so the image will be rotated by 3x3 until all n pixels are completely rotated. The following formula is used for the encryption and decryption process:

a) Encryption formula

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

...........................................................................3.1

b) Decryption formula

\[
\begin{bmatrix}
  x_i \\
  y_i
\end{bmatrix} =
\begin{bmatrix}
  1 & b \\
  c & bc + 1
\end{bmatrix}^{-1}
\begin{bmatrix}
  x_{i+1} \\
  y_{i+1}
\end{bmatrix} \mod(n)
\]

...........................................................................3.2
For the next step, an image has to be taken after knowing the encryption and decryption formulas to take the pixel value of an image [15]. The picture as follow:

Figure 1. Picture with format jpg

Figure 1 is an image that will be encrypted. For the first step, the writer needs to take the RGB values from the image that will be encrypted. The RGB value retrieval process is done using the Matlab software. The value generated largely while for the results of RGB values using Matlab can be seen in the picture below:

Figure 2. Results of RGB values

For preliminary test, the author took the RGB value provided in figure 3.1 as much as 3x3 pixels. The results were follows:

Table 1. Samples of 3x3 pixels

| Pos Pixel | 0   | 1   | 2   |
|-----------|-----|-----|-----|
| 0         | 149 | 151 | 153 |
| 1         | 156 | 155 | 158 |
The encryption and decryption with the Arnold Cat Map algorithm after the pixel values were evaluated.

Result and Discussion

Image security system applications using the Arnold Cat Map algorithm were designed to be able to run in a Windows-based operating system and run using a web browser. When the user wants to iterate the image, the first thing to do is to click the choose file button, the function is used to select an image file that will be randomly pixelated.

![Image with choose file button](ika.jpg)

**Figure 3.** Display of picture with "choose a file" choice

Randomization of the image was started by clicking the button 'iteration'. By pressing the button the process of randomizing the image will immediately be started when the trial is done randomizing the image. The image is the one that will appear to iterate:

![Selection of images](ika.jpg)

**Figure 4.** Selection of images that will be randomized to the pixel
During the 201th iteration, it was seen that the randomization of images looked better and disguised. While iterating up to 300, the pixel position on the image is back to normal. As shown in Figure 5.

![Figure 5. 300th iteration](image)

Randomization continued to occur to the desired results. During randomization, visible pixel displacement can be seen in the image and disguised. Randomization continued until the iteration limit, in multiples of 300 randomization the pixel will return to the original image.

**Conclusion**

From the research, it can be concluded that:

1. The application designed to secure an image by performing the process of image pixel randomization has the advantage that the image size will remain the same and has no effect with all capacities that have been processed using the Arnold Cat Map method.
2. The results of pixel randomization and interaction using the Arnold Cat Map method have not been implemented optimally; in achieving security, the image does not change or damage the image from its original form.
3. The randomized pixel position will return to its original position after going through several iterations by referring to the capacity of the image image, where if the image size is different, then the random iteration of the pixel will return to the original iteration point that varies at the time of encryption and decryption with the method Arnold Cat Map.
4. In the pixel randomization program that has been built is still not perfect, for example on the application of the Arnold Cat Map method modulation on the program cannot be implemented optimally and only strengthens pixel randomization maximally in the image.

**References**

[1] D. Abdullah et al., “Super-Encryption Cryptography with IDEA and WAKE Algorithm,” *J. Phys.: Conf. Ser.*, vol. 1019, no. 1, p. 012039, 2018.
[2] M. Mesran et al., “Combination Base64 and Hashing Variable Length for Securing Data,” *J. Phys.: Conf. Ser.*, vol. 1028, no. 1, p. 012056, 2018.
[3] R. Rahim et al., “Combination Base64 Algorithm and EOF Technique for Steganography,” *J. Phys.: Conf. Ser.*, vol. 1007, no. 1, p. 012003, 2018.
[4] D. Abdullah, R. Rahim, D. Apdilah, S. Efendi, T. Tulus, and S. Suwilo, “Prime Numbers Comparison using Sieve of Eratosthenes and Sieve of Sundaram Algorithm,” *J. Phys.: Conf. Ser.*, vol. 978, no. 1, p. 012123, 2018.
[5] R. Rahim, H. Nurdiyanto, A. S. A, D. Abdullah, D. Hartama, and D. Napitupulu, “Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm,” *J. Phys.: Conf. Ser.*, vol. 954, no. 1, p. 012008, 2018.
[6] D. Abdullah, R. Rahim, D. Hartama, A. Abdisyah, Z. Zulmiardi, and S. Efendi, “Application of Web Based Book Calculation using Deterministic Dynamic Programming Algorithm,” J. Phys.: Conf. Ser., vol. 1019, no. 1, p. 012040, 2018.

[7] R. Sitompul, A. Alesyanti, H. Hartono, and A. S. Ahmar, “Revitalization Model The Role of Tigo Tungku Sajarangan in Fostering Character of Children in Minangkabau Family and Its Socialization Through Website,” International Journal of Engineering & Technology, vol. 7, no. 2, pp. 53–57, Mar. 2018.

[8] A. Alesyanti, R. Ramlan, H. Hartono, and R. Rahim, “Ethical decision support system based on hermeneutic view focus on social justice,” International Journal of Engineering & Technology, vol. 7, no. 2.9, pp. 74–77, 2018.

[9] R. Sitompul, A. Alesyanti, H. Hartono, and R. Rahim, “Factors Cause Understanding level of Low Soft Skill for Political Party Members and its Socialization Through Website,” International Journal of Engineering & Technology, vol. 7, no. 2.14, pp. 286–288, 2018.

[10] D. Abdullah, Tulus, S. Suwilo, S. Efendi, and Hartono, “DEA Optimization with Neural Network in Benchmarking Process,” IOP Conference Series: Materials Science and Engineering, vol. 288, p. 012041, Jan. 2018.

[11] D. Abdullah, Tulus, S. Suwilo, S. Efendi, Hartono, and C. I. Erlina, “A Slack Based Measures for Improving the Efficiency Performance of Departments in Universitas Malikussaleh,” International Journal of Engineering & Technology, vol. 7, no. 2, pp. 491–494, Apr. 2018.

[12] D. Abdullah, Tulus, S. Suwilo, S. Efendi, M. Zarlis, and H. Mawengkang, “A Research Framework for Data Envelopment Analysis with Upper Bound on Output to Measure Efficiency Performance of Higher Learning Institution in Aceh Province,” International Journal on Advanced Science, Engineering and Information Technology, vol. 8, no. 2, 2018.

[13] Purba, R 2014 Enkripsi citra digital menggunakan arnold's cat map dan nonlinear chaotic algorithm Jurnal Sifo Mikroskil Vol 15 No , 61-71.

[14] Haifeng Yu, Phillip B. Gibbons, Michael Kaminsky, Toward an optimal social network defense against Sybil attacks. Proceedings of the twenty-sixth annual ACM symposium on Principles of distributed computing, August 12-15 2007, Portland, Oregon, USA

[15] Doni Ariyus.2006. Kriptografi Keamanan Data Dan Komunikasi. Penerbit Graha Ilmu. Yogyakarta