

RESEARCH ARTICLE | JULY 29 2024


Implementation of Hill Cipher Algorithm and Arnold Cat Map (ACM) algorithm on Iris digital image security


Muhammad Khudzaifah ; Muhammad Luqman Hakim


AIP Conf. Proc. 3083, 020002 (2024)


<https://doi.org/10.1063/5.0224888>





 Nanotechnology & Materials Science

 Optics & Photonics

 Impedance Analysis

 Scanning Probe Microscopy

 Sensors

 Failure Analysis & Semiconductors

Implementation of Hill Cipher algorithm and Arnold Cat Map (ACM) Algorithm on Iris Digital Image Security

Muhammad Khudzaifah^{1,a)} and Muhammad Luqman Hakim²

¹*UIN Maulana Malik Ibrahim Malang, Indonesia*

²*PT. GoTo Gojek Tokopedia, Jakarta, Indonesia*

a)Corresponding author: khudzaifah@uin-malang.ac.id

Abstract. The advancement of technology, particularly in smartphones, has prompted the need for the development of an authentication process. Among the various options available is the utilization of iris recognition in the authentication process, which can enhance security since the structure of the iris is unique and distinct from one individual to another. For authentication to be secure, data encryption and decryption processes are necessary. This research uses a combination of two algorithms, namely the Hill Cipher algorithm and Arnold Cat Map (ACM) algorithm. The purpose of this study was to obtain the results of accuracy and time efficiency used in the encryption and decryption process. In this study, the encryption process was carried out using the Hill Cipher algorithm and then followed by encryption using the Arnold Cat Map (ACM) algorithm. In the decryption process, it was obtained using the Arnold Cat Map (ACM) algorithm, then continued with the decryption using the Hill Cipher algorithm. The results of digital image encryption obtained from the application of the Hill Cipher and Arnold Cat Map algorithms have succeeded in producing a digital image that is more random and almost unrecognizable when compared to applications that only use the Hill Cipher algorithm or the Arnold Cat Map algorithm. **Keywords: Decryption, Digital Image, Encryption, Eye's Iris, Hill Cipher Algorithm, Arnold Cat Map Algorithm**

INTRODUCTION

Technological advances that continue to develop have a significant impact in all aspects of life. Smartphones are a clear example of the rapid technological progress that has taken place in recent times. With various innovations in smartphone technology, these devices have become even more functional and efficient. Smartphones are hardware devices designed to be compact for the convenience of the user, while also featuring sophisticated computer systems. One of the crucial aspects of smartphones is the authentication system, which is often based on outdated methods like pattern or password-based data storage and screen lock authentication. These methods have low levels of security and can easily be compromised by unauthorized parties.[1].

As a response to the COVID-19 pandemic, which has made it necessary to wear masks during all community activities, there is currently a growing trend towards developing biometric authentication systems for smartphones. By incorporating biometric authentication, smartphones can offer both data security and flexibility in processing transactions. Password-based authentication systems are known to be vulnerable to hacking, which makes biometric identification an effective means of enhancing computer system security.[2]. Several biometric authentications that can be used on smartphones are authentication with fingerprints and irises. Biometric authentication can provide a higher level of security because it is unique and has a low error rate [3] As is commonly understood, fingerprints and

irises are unique to each individual, and can be used for biometric identification. However, given the current public health situation, which mandates the use of face masks at all times, it is necessary to innovate the smartphone authentication process using a biometric method that can be performed without removing the mask. One solution is to use the iris, as fingerprints may be harder to identify due to texture damage caused by external factors. The iris, being an internal organ, is protected from such damage by a layer called the cornea.[3].

The existence of an authentication process certainly requires a high level of data security. This involves the science of cryptography that functions in data encryption and decryption. This research needs to be done to find out how the level of accuracy obtained is based on the initial image with the decrypted image, which is processed using the Hill Cipher algorithm and the Arnold Cat Map (ACM) algorithm to find out that the algorithm used can produce good encryption and decryption results. In addition, this study was conducted to determine the combination of the two algorithms and their effectiveness in securing iris images. The Hill Cipher algorithm is a classical encryption technique that is based on matrix multiplication, while the Arnold Cat Map algorithm is a chaotic encryption technique that is known for its ability to produce highly randomized outputs.

Hill Cipher is the application of modulo arithmetic to cryptography, this cryptographic technique uses a square matrix as the key used for encryption and decryption. Arnold Cat Map is a two-dimensional chaotic system that can be used to change the position of digital image pixels without removing any information from the digital image, the pixel position of the digital image can be assumed with $S = \{(x, y) \mid x, y = 0, 1, 2 \dots N - 1\}$. [5]

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab + 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \quad (1)$$

Where a and b are any positive integers. Applying Arnold's Cat Map algorithm once to the original pixel position (x, y) will result in a new position (x', y') . Repeatedly applying the algorithm d times will produce a randomly scrambled version of the original image, with all values of the same pixel appearing in the resulting drawing. The number of iterations required to achieve this depends on the parameters a, b , and the size of the original image (N). Therefore, the Arnold Cat Map algorithm can use parameters a, b , and d as a secret key.[7]

Structural Similarity Index Metrics or SSIM is one of the methods used to determine and measure the level of similarity between 2 images [4]. The structural Similarity Index Metrics algorithm is done by comparing structural features. With a straight comparison between structural similarity with image quality. So it can be concluded that the higher the similarity, the higher the image quality, and vice versa. The Structural Similarity Index Metrics algorithm has three main comparisons: luminance distortion, contrast distortion, and correlation. [4] explained that the Structural Similarity Index Metrics equation can be written with the following equation:

$$SSIM(a, b) = l(a, b)c(a, b)s(a, b) \quad (2)$$

Each comparison/feature is as follows:

$$\text{Luminance:} \quad l(a, b) = \frac{2\mu_a\mu_b + C_1}{\mu_a^2 + \mu_b^2 + C_1} \quad (3)$$

$$\text{Contrast:} \quad c(a, b) = \frac{2\sigma_a\sigma_b + C_2}{\sigma_a^2 + \sigma_b^2 + C_2} \quad (4)$$

$$\text{Structure:} \quad s(a, b) = \frac{\sigma_{ab} + C_3}{\sigma_a\sigma_b + C_3} \quad (5)$$

Where C_1, C_2, C_3 are constants to avoid errors due to the denominator = 0. Equation $l(a, b)$ is a comparison used to measure the similarity of the values of the luminance (μ) of the two images being tested. The maximum value of $l(a, b)$ is 1. The maximum value will be fulfilled if the value of $\mu_a = \mu_b$.

The equation $c(a, b)$ is a comparison of the contrast values obtained from the comparison of the standard deviation (σ) of the tested image. Same with equation $l(a, b)$ where the maximum value that can be obtained is 1, provided that $\sigma_a = \sigma_b$.

The equation $s(a, b)$ is a structural comparison that measures the correlation coefficient in the 2 images tested. Where σ_{ab} is the covariance value between a and b .

Structural Similarity Index Metrics produces values from a range of 0 to 1[6]. Where the value of "0" indicates that the two images are not correlated or not the same. While the value of "1" indicates that the two images tested are similar or exactly the same.

RESEARCH METHODS

Research data

The data used in this study is RGB image data (digital image) with size 240x240pixel with *.bmp file format consisting of 5 iris images each left and right from 46 people, with a total of 460 images. The data used in this study is the MMU Iris Dataset which can be obtained for free on the Kaggle website which has been licensed by the Multimedia University Iris Database for Biometric Attendance System at the link <https://www.kaggle.com/naureenmohammad/mmu-iris-dataset>. The data held will be processed using a computer program with a programming language, namely python with the help of the Pillow library.

Data analysis technique

The encryption and decryption process in this study is a combination of Hill Cipher algorithm and the Arnold Cat Map (ACM) algorithm. The stages used are starting with encryption using Hill Cipher algorithm, then followed by encryption using the Arnold Cat Map (ACM) algorithm. The decryption process is carried out using the Arnold Cat Map (ACM) algorithm, then followed by decryption using Hill Cipher algorithm.

Encryption process

The encryption process is carried out by applying two algorithms, namely Hill Cipher algorithm and the Arnold Cat Map (ACM) algorithm. Here are some steps that need to be done in the encryption process with details:

1. Prepare a plain image, which is a digital image of the iris of the eye with dimensions of $N \times N$, which is 240 x 240 pixels.
2. Converts the plain image into a matrix form and initializes each plain text matrix entry with the value of the grey level R(Red), G(Green), and B(Blue).
3. Specifies three integer numbers (a, b, d)
4. Make a key in the form of a 2×2 matrix using two integer numbers (a, b)
5. The matrix key is multiplied by each of the two entries in the plain-image matrix and modularized by 256
6. Obtained cipher-image matrix (HC)
7. Substituting numbers (a, b) and the length of the cipher-image (HC) into the Arnold Cat Map equation
8. Transforms the position of each cipher-image matrix entry (HC) with iteration (d) times
9. Obtained cipher-image matrix (HC-ACM)
10. Returns the cipher-image matrix (HC-ACM) into a digital image
11. Obtained encrypted digital image.

Decryption process

The decryption process is carried out by applying two algorithms, namely the Hill Cipher algorithm and the Arnold Cat Map (ACM) algorithm. Here are some steps that need to be done in the decryption process with details:

1. Prepare a cipher image, which is an encrypted digital image of the iris of the eye with dimensions of $N \times N$, which is 240 x 240 pixels.

2. Converts the cipher image into a matrix form and initializes each plain text matrix entry with the value of the grey level R(Red), G(Green), and B(Blue).
3. Specifies three integer numbers (a, b, d)
4. Substituting numbers (a, b) and the length of the cipher-image (HC-ACM) into the Arnold Cat Map equation
5. Transforms the position of each cipher-image matrix entry (HC-ACM) with iteration (d) times
6. Obtained cipher-image matrix (HC)
7. Calculate inverse of the encryption matrix key
8. The inverse of matrix key is multiplied by each of the two entries in the cipher-image (HC) matrix and modularized by 256
9. Obtained a plain-image matrix
10. Returns the plain-image matrix to a digital image
11. Obtained digital image of the decryption results













Evaluation

The evaluation phase involves a critical review of the methods that have been implemented, with the aim of assessing the degree of success of the algorithm used in the study. To evaluate the algorithm's performance, the Structural Similarity Index Metrics (SSIM) method will be employed. SSIM is a technique that analyzes the similarity between the decrypted image and the original image prior to encryption, providing a measure of accuracy for both the encryption and decryption processes under study.

RESULTS

This section describes the testing process that was conducted using the Jupyter Notebook text editor in Python. The encryption and decryption of digital images were performed by inputting the relevant keys into the text editor, and the output results were then analyzed. The accuracy of the encryption and decryption process was evaluated using the Structural Similarity Index Metrics (SSIM) method. This involved measuring the level of structural similarity between the original image prior to encryption and the image that had undergone the encryption and decryption processes.

TABLE 1. Image result of encryption and decryption process.

No.	Plain Image	Method	Cipher Image	SSIM Encryption	Decryption Result	SSIM Decryption
1.		Hill Cipher		0,06		1
2.		Arnold Cat Map 1 iteration		0,14		1
3.		Hill Cipher And Arnold Cat Map 1 iteration		0,02		1
4.		Hill Cipher And Arnold Cat Map 2 iteration		0,01		1

The Structural Similarity Index Metrics (SSIM) value can serve as a reference point for determining the degree of structural similarity between the original and encrypted images. A lower SSIM value indicates better results as the encrypted image has a distinct structure from the original image. On the other hand, a maximum SSIM value of 1 is required during the decryption process to confirm its success, as the decrypted image should have the same structural structure as the original image. In addition, when conducting testing on the same iris digital image but with different key values and maximum iterations, the SSIM value obtained from the encryption and decryption process was found to be the same.

In table 1, it can be seen the results of tests carried out with a total of 4 experiments on 1 digital image of the iris of the eye using different algorithms and different maximum iterations for the Arnold Cat Map algorithm. In the encryption process, the value of Structural Similarity Index Metrics (SSIM) is 0.06 when the method that used only Hill Cipher, and the value of Structural Similarity Index Metrics (SSIM) is 0.14 when the method that used only Arnold Cat Map, and the value of Structural Similarity Index Metrics (SSIM) is 0.02 when the method Hill Cipher and Arnold Cat Map one iteration, This shows that the combination of two algorithm more effective to encrypt the iris image, but it's more effective using two iteration on Arnold Cat Map algorithm, because the value of Structural Similarity Index Metrics (SSIM) is 0.01, smaller than using only one iteration. This shows that the digital image of the iris produced in the encryption process is not identical or the same as the initial digital image of the iris. Then in the decryption process, the average value of Structural Similarity Index Metrics (SSIM) is 1 for all tests. This shows that the digital image of the iris that has gone through the encryption and decryption process is identical or the same as the initial digital image of the iris.

CONCLUSION

The time required for the encryption and decryption process is influenced by the size of the digital image and the value of the d key that is entered using the Arnold Cat Map algorithm. The results of digital image encryption obtained from the application of the Hill Cipher and Arnold Cat Map algorithms have succeeded in producing a digital image that is more random and almost unrecognizable when compared to applications that only use the Hill Cipher algorithm or the Arnold Cat Map algorithm. But it's more effective using the Hill Cipher and Arnold Cat Map algorithms two iterations, because the value of Structural Similarity Index Metrics (SSIM) is 0.01, smaller than using only one iteration. The contribution of this research lies in it's novel approach to securing iris digital images using a combination of classical and chaotic encryption techniques and the comprehensive analysis of the proposed method's performance.

REFERENCES

1. J. Nader, A. Alsadoon, P. W. C. Prasad, A. K. Singh, and A. Elchouemi, "Designing Touch-Based Hybrid Authentication Method for Smartphones," in *Procedia Computer Science*, 2015, vol. 70, pp. 198–204. doi: 10.1016/j.procs.2015.10.072.
2. E. G. Kristanto, E. Rompas, and S. Wangko, "Identifikasi Iris Opsi Identifikasi Iris," *Jurnal Biomedik*, vol. 5, pp. S7-11, 2013.
3. S. Vatsal and Mr. S. S. Dwivedi, "Advanced IRIS Recognition System: A Review," May 2018.
4. H. B. Sumarna, E. Utami, and A. D. Hartanto, "Tinjauan Literatur Sistematis tentang Structural Similarity Index Measure untuk Deteksi Anomali Gambar Systematic Literature Review of Structural Similarity Index Measure for Image Anomaly Detection," *Citec Journal*, vol. 7, no. 2, 2020.
5. R. Munir, "Algoritma Enkripsi Citra Digital Berbasis Chaos dengan Penggabungan Teknik Permutasi dan Teknik Substitusi Menggunakan Arnold Cat Map dan Logistic Map," *J. Nas. Pendidik. Tek. Inform. JANAPATI*, vol. 1, no. 3, pp. 166–181, Dec. 2012, doi: 10.23887/JANAPATI.V1I3.9814
6. U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," *Journal of Computer and Communications*, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.
7. E. Hariyanto and R. Rahim, "Arnold's Cat Map Algorithm in Digital Image Encryption," *Int. J. Sci. Res.*, vol. 5, pp. 2319–7064, 2013, doi: 10.21275/ART20162488