International Journal of Information System & Technology
Akreditasi No. 158/E/KPT/2021 | Vol. 7, No. 6, (2024), pp. 379-385

Combined Performance of Hill Cipher and Rivest Code 6 (Rc6) Algorithms in Image Security

Heri Santoso[1], Nia Sabrina Rambe[2], Suhardi[3]*
[1,2,3]Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
Email: herisantoso@uinsu.ac.id[1], niasabrinarambe11@gmail.com[2], suhardi@gmail.ac.id[3]

Abstract

Digital image files are a form of information that is accurate and reliable enough to describe something, so the level of authenticity of this information needs to be maintained. Especially when sent via the internet as in chat-based applications such as Facebook, WhatsApp, Instagram and other social media. To maintain the security and confidentiality of digital image/image information, it is necessary to have a technique called cryptography. Cryptography is a technique or algorithm for changing data or information to be different from the original information. For example, in everyday life, there is a result of a design order that is still in the development stage that needs to be shown to prospective buyers, a drawing file or documentation image file that is private and confidential, so it is important to pay attention to its security. This research will use the combined performance of the Hill Cipher and Rivest Code 6 cryptographic algorithms in securing image files. The results of the Hill Cipher and Rivest Code 6 cryptographic algorithm encryption are able to disguise the image during the encryption process. And can restore to the original image in the decryption process. So that the encrypted image is safer to send via the internet or social media.

Keywords: *Cryptography, Imagery, Hill Cipher, Rivest Code 6.*

1. Introduction

Currently, technological progress is very fast because almost all human activities use technology. The technology that is often used is the exchange of information via the internet. If information is available, data or facts can be known in real terms and are easy to understand. And in line with the development of information, the dangers regarding the information itself are increasing. The danger in data security is the efforts of someone who wants to gain illegal access to the network and data [1].

Cryptography is a technique or algorithm that is useful for changing data or information so that it is not the same as the original information, in Greek, namely cryptos and graphia "secret writing" is the science and art of studying how to make a sent message be delivered safely. Cryptography is part of a branch of mathematics called cryptology [2]. For example, in everyday life, there are design orders that are in the development stage that need to be shown to prospective buyers, image files or documentation files that are private and confidential, so it is important to pay attention to their security. With the details of this problem, one way to secure data in the form of image files is to secure it using encryption and decryption of the Hill Cipher and Rivest Code 6 cryptographic algorithms for image files. The author found several journals in previous research such as research conducted by Erla Rizky Febrianto in 2018, namely Digital Image Cryptography Using Android-Based Hill Cipher and Affine Cipher [3].

This application has been tested and compared with applications that simply use the Hill Cipher or Affine Cipher algorithms. In further research, Image Data Encryption with RGB Color Model and Threshold Using the Hill Cipher Algorithm [4]. Based on the implementation, studies and explanations that have been carried out, several conclusions can be drawn, namely that Object Encryption and data decryption can be

ISSN : 2580-7250

carried out on evidence in the form of images or images by drawing the RGB value bits from each pixel in the form of a numeric number, where the value ranges from 0- 255.

The pixel values are then operated using matrix multiplication from the Hill Cipher algorithm. Data in the form of images or images can be encrypted using the Hill Cipher algorithm, namely true color and grayscale images, meanwhile threshold images (black and white) cannot be encrypted because the color diversity is only small, namely only a few values, 0 and 255. Create a data input matrix for the Hill algorithm Cipher, the larger the matrix value entered, the better the encryption process will be and the original form will not be easily known.

In further research, securing digital images of medical records using a combination of Keccak and Rivest Code 6 hashing algorithms [5]. The conclusion that can be found is that the RC6 algorithm can secure digital images of medical records, and restore the encrypted image as well as the authenticity of the image. Based on tests carried out by modifying the encryption file, the file cannot be decrypted again, causingImage confidentiality is well maintained, and it is easy to find out if modifications occur.

Images are two-dimensional representations of objects from the visual world, involving various disciplines including art, human vision, astronomy, engineering, and so on. It is a collection of pixels or colored dots in two dimensions. Digital image processing is an image processing technique that aims to improve image quality so that it is easily interpreted by humans or computer machines, which can be in the form of photos or moving images [6].

The parameters contained in the image are MSE and PSNR with MSE being a quantitative analysis benchmark used to assess the quality of an output image and the superiority of the method used. Mean Square Error (MSE) is the average square error of the image pixel signals resulting from signal processing on the signal. original. For the best value, MSE is equal to zero. And Peak Signal to Noise Ratio (PSNR) is a comparison between the maximum value of the signal being measured and the amount of noise that affects the signal, in decibel units (dB). The greater the PSNR parameter, the more similar it is to the original image [7].

In research using the RC6 algorithm, the encryption and decryption process time is faster than the RSA algorithm. In this case the author uses the classic Hill Cipher cryptographic method. Hill Cipher is a classic algorithm that is very difficultto be solved if you only know the ciphertext. Because the Hill Cipher algorithm uses matrix multiplication as the basis for encryption and decryption, not just changing each letter that is similar in plaintext to the letter in the ciphertext. To strengthen security, the authors combine it with modern cryptographic methods. In this case the author chose the modern Rivest Code 6 (RC6) algorithm.

In the RC6 algorithm, the level of security is based on the strength of rotation based on data. Its standout features include the use of four registers instead of two registers as in the RC5, and the inclusion of integer multiplication as an additional primitive operation. The use of multiplication with four functional registers greatly increases the achieved diffusion of rotation, allows for greater security, as well as increasing the effective data transfer speed (throughput). It is also capable of handling plaintext block sizes and*ciphertext*128-bit and suitable for implementation using hardware or software.

2. Research Methodology

2.1. Problem analysis

One way to identify the causes and effects of designing a system is so that the system to be built can operate in accordance with the objectives for which the system was built. The problem here is how to secure digital images by utilizing a combination of two encryption algorithms. This digital image encryption uses the Hill Cipher and RC6 algorithms and the PNG file format.

2.2. Data collection technique

The data collection technique used in this research is to look for relevant sources and references regarding the Hill Cipher and RC6 algorithms in digital image encryption, both from journals, theses and also ebooks which can be used as a basic theory in conducting this research.

a. Planning

In designing an application, a concept is needed to build the application the. There are two designs carried out in this research, namely interface design and flowchart design.

1) Interface design in research on the combined performance of the Hill Cipher and RC6 algorithms in image security. The interface design is designed with objects that make the application easy and comfortable for the user.
2) Flowchart design is a simple mapping tool that displays a sequence of actions in a process in a form that is easy to read and communicate. Flowcharts are used to make it easier to simplify a series of processes to facilitate user understanding of a program [8].

b. Research Flowchart

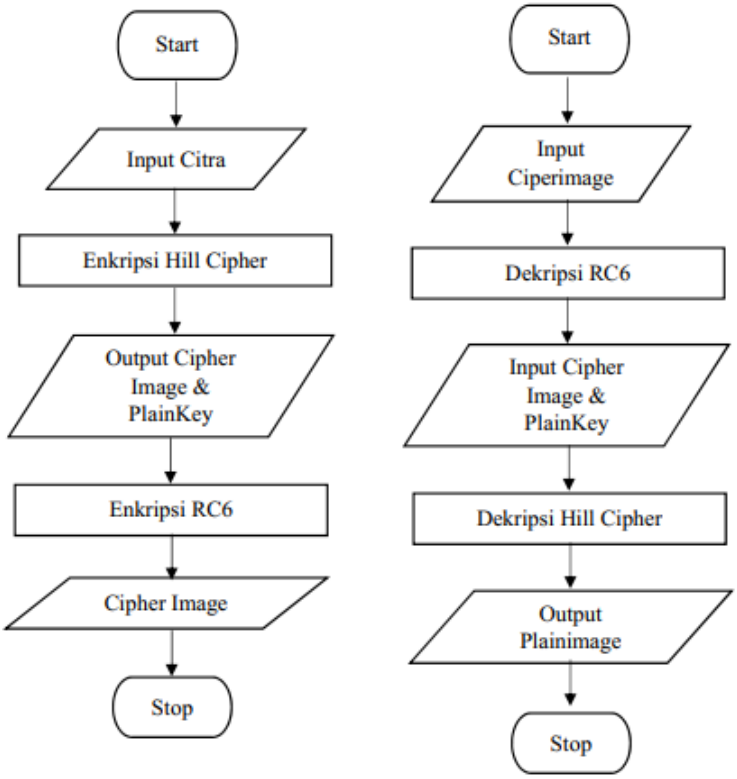

Figure 1. Encryption and Decryption Process

2.3. Needs Analysis

Requirements analysis must be carried out on a system to achieve goals. In this designed application, the requirements that must be met in running the Hill Cipher Algorithm and the RC6 Algorithm in encrypting digital images are:

a) The system must be able to read image files.
b) The system must be able to encrypt image files in PNG file format using the Hill Cipher Algorithm and the RC6 Algorithm.
c) The system to be built has a system that will make it easier for users to use it.
d) The system can be used well even though it saves money in operation.

e) The system was built as simply as possible to make it easier for users to use the application.

3. Results and Discussions

3.1. Application of the Hill Cipher Algorithm

The Hill Cipher algorithm is a polyalphabetic cipher which can be classified as a block cipher, because the text to be processed will be divided into blocks of a certain size. Each value in one block will influence other values in the encryption and decryption process, so that similar values are not mapped to similar values.Algorithm*Hill Cipher* In the solution, it uses a matrix as a key to carry out encryption and decryption as wellmodulo arithmetic.

This technique uses a square matrix as the key used to carry out the encryption and decryption processencryption is done by multiplying the key matrix by the key matrix*plaintext*, while decryption is done by multiplying the inverse key matrix by the key matrix*ciphertext*.Therefore,*Hill Cipher* You can only use a square matrix as the key matrix. Pseudo inverses or pseudo inverses can be used in algorithms*Hill Cipher*, so that the key matrix used is not limited to square matrices only. Using a rectangular matrix makes*ciphertext* longer than*plaintext*. This of course makes the image data more obscure.The image used is an RGB image with an image size of 240*160 pixels in PNG format with a key length of 4 characters.

3.2. Image Pixel Reading

In the initial stage, the 24 bit color image (true color) where the RGB values are directly described in bitmap data in binary form. To read the RGB value, a search is carried out for each header and bitmap data which contains information on the dimensions, format and pixel values of the image. Each bitmap data element is 3 bytes long, each byte represents the components R, G, and B. Each byte of data represents 8 bits, so the color image has 3 bytes x 8 bits = 24 bits of color content [9].

In a color image, each pixel contains 24 bits of color content (8 bits) for each basic color (R, G, and B), with a content value range between 0 to 255 for each color. The goal to be achieved is to get the RGB value.

In this research the author carried outsecret image security using the Hill Cipher algorithm. This polyalphabetic cipher algorithm can be grouped as a block cipher, because the image to be encrypted is divided into blocks of a certain size. The basis of this technique is modulo arithmetic on image matrices using matrix multiplication techniques and matrix inverse techniques. The key in Hill Cipher is an nxn matrix where n is the block size. The K matrix that is the key should be an invertible matrix, that is, it has multiplicative inverse K-1 up to: KK-1 = K-1.K = 1. The key must have an inverse because the K-1 matrix is the key used to carry out decryption [10].

In the initial stage, data is entered in the form of a color image in .PNG format with a size of 240 x 160 pixels. In the image, pixel values are read in the form of red, green and blue color component values. Next, encryption is carried out using the Hill Cipher algorithm to produce a Hill Cipher cipher image. Next, the Hill Cipher cipher image is encrypted using the RC6 algorithm which produces an RC6 cipher image which will be distributed via the communications network to reach the rightful person. To be able to see the image, the recipient side will decrypt it using the RC6 and Hill Cipher algorithms and get the original image back [11].

3.3. Application System Design

At this stage, we will design the appearance of the application system on the system to be designed. The function of designing this application system is as a means of communication for the user and the system.

a) Menu Display

The menu display is the initial page of the system, where there is the main title of the system, the name of the system manufacturer and the system NIM. At the bottom there is campus information.

Figure 2. Appearance Menu Forms

b) HILLCRC6 Form Display

This display is useful for encrypting and decrypting image files. In this display, image input is carried out by pressing the Load button and creation of encryption keys for the Hill Cipher and RC6 algorithms.

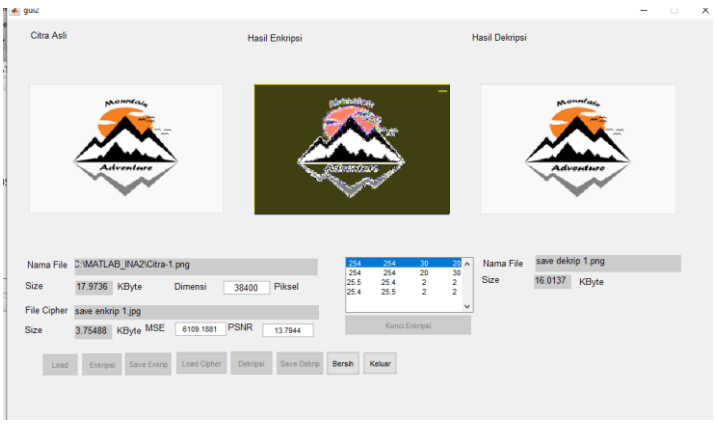

Figure 3. HILLCRC6 Display

c) System Test Results

From the test results above, the author can display the results of testing on the system that has been built. The image data will be tested for encryption as many as 10 data.

1) Plain Image Encryption Test Results

Table 1. Image Encryption Testing Plain Image

No	Original image	Ex	Size (KB)	Ciperimage	Size (KB)	MSE/PSNR
1		png	17.9736 KB		3.75488 KB	6109.1881/13.7944
2		png	20.8828 KB		4.79102 KB	5814.6039/13.5798

No	Original image	Ex	Size (KB)	Ciperimage	Size (KB)	MSE/PSNR
5		png	11.3291 KB		1.30957 KB	6650.1025/14.1629
8		png	17.6318 KB		7.3291 KB	807.7658/5.00745

2) Plain Image Encryption Test Results

Table 2. Image Decryption Testing Cipher Image

No	*Cipherimage*	Ex	Size (KB)	*Plainimage*	Size (KB)
1		png	3.75488 KB		16.0137 KB
2		png	4.79102 KB		18.6699 KB
5		png	1.30957 KB		9.68457 KB
8		png	7.3291 KB		15.8291 KB

A large PSNR value means that the difference between the original image and the encrypted image is small. In the graph above, you can see that the PSNR value with the encryption results is below 30 dB, this means there is a big difference between the original image and the encrypted image.

4. Conclusion

From the process and series of design to implementation, it was concluded that the results of the encryption and decryption performance of the combined Hill Cipher and Rivest Code 6 (RC6) algorithms in this research could disguise the image during the encryption process and could restore the original image during the decryption process. Based on the evaluation of the test results of original images and encrypted images from a total of ten image data files tested, the ideal MSE value was above 30, which means the level of randomness is increasingly error and the best MSE value is 6650.1025. Meanwhile, the PSNR value of a total of ten image data files tested produced an ideal cryptographic PSNR value of under 30 dB with the best value of 5.00745 dB. And the size of the plain image that is encrypted and produces a cipher image and then decrypted changes. The size of the plainimage becomes smaller than the initial plainimage before it is encrypted.

References

[1] A. G. Gani, "Pengenalan Teknologi Internet Serta Dampaknya," *J. Sist. Inf.*, vol. 2, no. 2, 2018.

[2] J. Jamaludin and R. Romindo, "Rancang Bangun Pengamanan Teks Menggunakan Kombinasi Vigenere Cipher dan RSA dalam Hybrid Cryptosystem," *Pros. Semin. Nas. Ris. Dan Inf. Sci.*, vol. 2, 2020.

[3] E. R. Febrianto and E. A. Sarwoko, "Kriptografi Citra Digital Menggunakan Algoritma Hill Cipher Dan Affine Cipher Berbasis Android," *J. Masy. Inform.*, vol. 10, no. 2, pp. 11–21, 2019, doi: 10.14710/jmasif.10.2.31495.

[4] A. Ommi, "No TiEnkripsi Data Citra Untuk Model Warna RGB dan Treshold

Menggunakan Algoritma Hill Ciphertle," *J. Nas. Inform. dan Teknol. Jar.*, vol. 4, no. 1, 2019.

[5] H. B. Seta, R. Yulistiani, and T. Theresiawati, "Pengamanan Citra Digital Rekam Medis Menggunakan Perpaduan Hashing Algoritma Keccak Dan Rivest Code 6," *J. Ilm. Matrik*, vol. 22, no. 3, pp. 257–269, 2020, doi: 10.33557/jurnalmatrik.v22i3.1077.

[6] J. Jumadi, Yupianti, and D. Sartika, "Pengolahan Citra Digital Untuk Identifikasi Objek Menggunakan Metode Hierarchical Agglomerative Clustering," *J. Sains dan Teknol.*, vol. 10, no. 2, 2021.

[7] S. Y. Doo, S. Tena, and V. M. Ndolu, "Implementasi Pengamanan Data Menggunakan Metode Kriptografi Hill Cipher Dan Steganografi Least Significant Bit (Lsb) Pada Media Citra Digital," *J. Media Elektro*, vol. 8, no. 2, 2019.

[8] J. I. Sari, Sulindawaty, and H. T. Sihotang, "Implementasi Penyembunyian Pesan Pada Citra Digital Dengan Menggabungkan Algoritma Hill Cipher Dan Metode Least Significant Bit (LSB)," *J. Mantik Penusa*, vol. 1, no. 2, pp. 1–8, 2017.

[9] S.Y.Iriyanto and T.M.Zaini, "Pengolahan Citra Digital," in *Anugrah Utama Raharja*,

[10] A. R. Tuasikal, D. Indra, and F. Fattah, "Analisis Perbandingan Known Plaintext dan Chosen Plaintext Pada Metode Hill Chiper," *Bul. Sist. Inf. dan Teknol. Islam*, vol. 1, no. 1, pp. 1–5, 2020, doi: 10.33096/busiti.v1i1.514.

[11] M. A. Fikri and F. X. Ferdinandus, "Optimasi Teknik Steganografi Amelsbr Pada Empat Bit Terakhir Dengan Cover Image Berwarna," *Antivirus J. Ilm. Tek. Inform.*, vol. 16, no. 1, pp. 25–38, 2022, doi: 10.35457/antivirus.v16i1.1967.