ISSN: 2581-1274

Encryption and Description of RGB Values in Images Using the Hill Chiper Algorithm

T. Sukma Achriadi[a,1,*], Hardisal[b,2] , Asmaidi[c,3], M. Sulthan Hanafi [d,4]

[a,b,d] *Politeknik Aceh Selatan, Address, Tapaktuan 23711, Aceh Selatan*
[c]*Universitas Mulawarman, Address, Samarinda 75123, Kalimantan Timur*
[1] *adimarlago@gmail.com*,[2] hardisal@poltas.ac.id,[3] asmedmat@gmail.com,[4] sulthanhanafi909@gmail.com;*
** corresponding author*

ARTICLE INFO

Article history:
Accepted

Keywords:
Java
hill cipher
cryptography
digital
RGB
Encryption
Description

ABSTRACT

Information security related to computer use cannot be separated from cryptography. Hill cipher is an application of modulo arithmetic in cryptography. This cryptography technique uses a square matrix as the key used to carry out encryption and decryption. This cryptographic technique was created with the intention of being able to create ciphers (codes) that cannot be broken using frequency analysis techniques. Hill Cipher does not replace each of the same letters in the plaintext with other letters that are the same in the ciphertext because it uses matrix multiplication as a basis for encryption and decryption. Hill Cipher cryptography is a type of classic cryptography that uses a substitution method by providing random keys and the number is the same as the plaintext. The use of encryption and decryption using the Hill cipher algorithm is to help secure data so that it is not easily falsified or accessed by irresponsible people by changing the original image into a different form where the image is not easy to recognize. The encryption and decryption process were designed using the Java programming language using NetBeans 8.2 and the Hill Cipher algorithm to encrypt RGB digital images.

I. Introduction

The exchange of information is very important at this time, so important is the exchange of information, of course, it must be accompanied by information security. Technological advances in the field of computers allow thousands of people and computers throughout the world to be connected to one virtual world known as the Internet. Likewise, hundreds of organizations such as government companies and even private individuals have made information a very valuable asset. This makes it very important for data to be protected from information manipulation. Information security related to computer use cannot be separated from cryptography. Safe means that during the sending of the information it is hoped that it cannot be read by unauthorized people. One way to secure this data is with Hill Cipher.

Hill cipher is an application of modulo arithmetic in cryptography. This cryptography technique uses a square matrix as the key used to carry out encryption and decryption [1]. This cryptography technique was created to be able to create ciphers (codes) that cannot be broken using frequency analysis techniques. Hill Cipher does not replace each of the same letters in the plaintext with other letters that are the same in the ciphertext because it uses matrix multiplication based on encryption and decryption. The process of changing plaintext to ciphertext is called encryption (from the word encryption) the process of turning ciphertext into plaintext again is called decryption (from the description word). Hill Chipper cryptography is a type of classic cryptography that uses the substitution method by providing random keys and the number is the same as the plaintext.

1.1. Formulation of the problem

Based on the background of the problem above, it can be concluded that the problem formulation in this final project is:

1. How to implement the Hill cipher encryption and decryption process using Java programming?
2. What are the results of applying the Hill cipher cryptographic algorithm to image data security applications?

1.2. Research purposes

Based on the background of the problem above, it can be concluded that the problem formulation in this final project is:

1. How to implement the Hill cipher encryption and decryption process using Java programming?
2. What are the results of applying the Hill cipher cryptographic algorithm to image data security applications?

II. The Proposed Method

2.1. Understand cryptography

Cryptography comes from Greek which consists of two syllables, namely crypto and graphic which means writing. Cryptography is a science that studies mathematical techniques related to aspects of information security, such as data confidentiality, as well as data authentication, data validity, data integrity, and data authentication. However, not all aspects of information security can be resolved with cryptography [2].

Cryptography is one of the appropriate data security solutions or methods to maintain the confidentiality and authenticity of data and can improve aspects of data or information security. This method aims to ensure that information that is confidential and sent over a network, such as a LAN or the internet, cannot be known or utilized by unauthorized people or parties. Cryptography supports the need for two aspects of information security, namely protecting the confidentiality of information data and protecting against falsification and unwanted changes to information [3].

2.2. Hill Cipher Algorithm

The HillCipher algorithm uses a mxm-sized matrix as the key to carry out encryption and decryption. The basic matrix theory used in HillCipher includes multiplication between matrices and performing inverses on matrices. HillCipher is a modulo arithmetic application for cryptography. This cryptography technique uses a square matrix as the key used to carry out encryption and decryption. HillCipher does not replace every same letter in the plaintext with another letter in the ciphertext because it uses a matrix as the basis for encryption and decryption. HillCipher, which is a polyalphabetic cipher, can be categorized as a block cipher because the text to be processed will be divided into blocks of a certain size. Each character in a block will affect other characters in the encryption and decryption process so that the same character is not mapped to the same character. HillCipher is a classic cryptographic algorithm that is very difficult for cryptanalysts to solve if only by knowing the ciphertext file. However, this technique can be accomplished easily if the cryptanalyst has a ciphertext file and a piece of the plaintext file. This cryptanalysis technique is known plaintext attack [6].

2.3. Digital Image

Image is a combination of points, lines, planes and colors to create an imitation of an object, usually a physical object or human. Images can be in the form of two-dimensional images, such as paintings, photographs, or in three-dimensional form, such as statues. Image is defined as a description of the object being observed [7].

2.4. System Development Life Cycle (SDLC)

In this research, researchers took a System Development Life Cycle (SDLC) development model approach so that the process of building this information system was carried out sequentially and well organized.

Fig. 1. System Development Life Cycle (SDLC)

2.5. The SDLC conceptual process model includes:

a. Planning
   In this section, the researcher identifies the problem and determines the scope of the research to determine the steps in the process of solving the problem under study, including determining resources, financial budget, and technical workmanship.
b. Needs Analysis
   In this section, researchers carry out a needs analysis involving system functional requirements for end users.
c. Designing systems
   In this section, researchers design modules, security, architecture, and information system interfaces and evaluate the software in both functional and operational aspects.
d. Building Software
   In this section, the team works on building, coding, and improving the overall required technical and physical configuration.
e. Software Testing
   This stage tests the system as a whole to answer the expected goals. This is done to ensure satisfaction with the use of the system for end users and to find errors in the system.
f. Software Implementation
   This stage is to release the software ready for use by end users.
g. Maintenance
   At this stage, end users can contribute to system improvements to improve performance and add features. This stage is important to carry out to evaluate performance, and application of new technology to anticipate cyber security.

In getting maximum results in the development of this historical information system, the author focuses on using a parallel model approach [8]. This methodology is a development of the waterfall methodology, where the process of system design and implementation is carried out sequentially for the entire system and then divided into different sub-activities which are carried out in parallel.

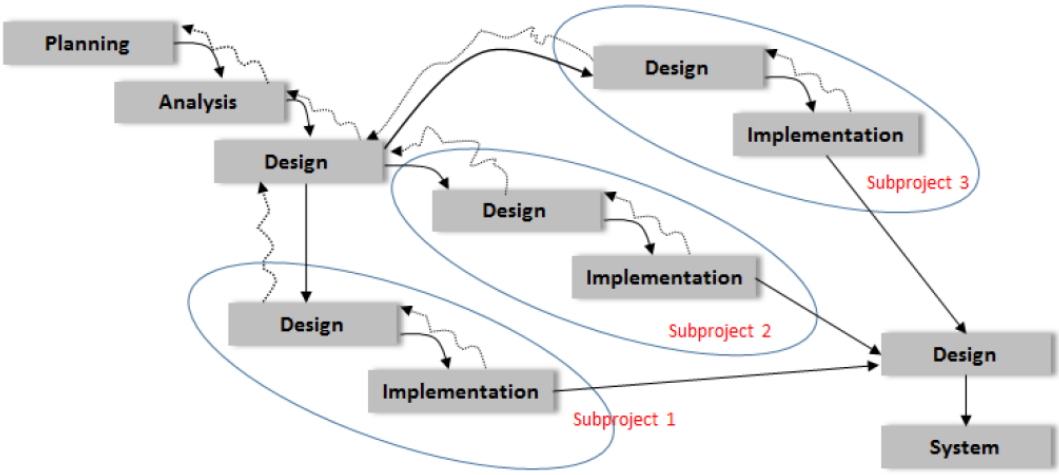

Fig. 2. Parallel Model Approach [8]

2.6. Unified Modeling Language (UML)

UML is a collection of tools used to abstract an object-based system or software. Based on research [6], the use of UML is very good in improving the quality of the software produced and the ease of software maintenance in the future, because using UML can identify 11 types of errors in uses case scenarios and 7 errors when modeling uses cases.

III. Method

The research procedure can be seen in the fishbone below:

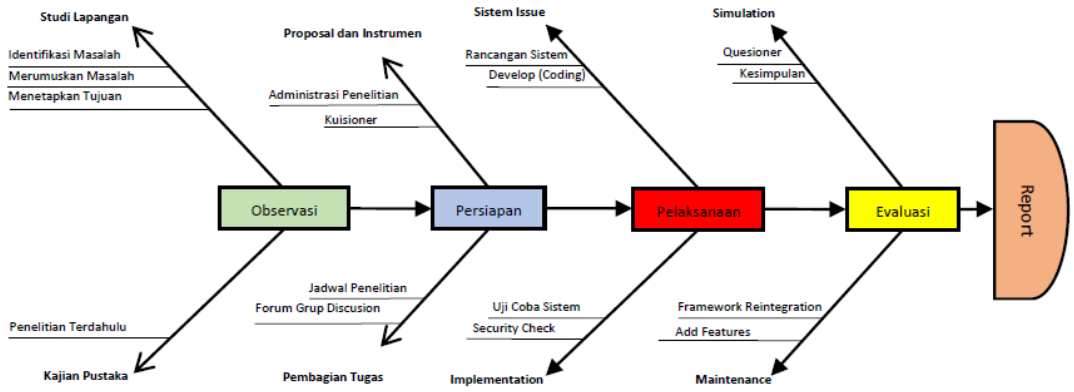

Fig. 3. Fishbone Research

There are 5 (five) procedural stages in this research, namely:

a. Observation Stages
   Researchers together with members carry out observations using field studies to obtain running system data, collect information to identify problems in the running system then formulate problems and set research objectives. Next, carry out a literature review by looking at previous research to support the research carried out.
b. Preparation Stages
   At this stage, proposals and supporting instruments are prepared, such as a Focus Group Discussion (FGD) between the chairman and research members regarding the topic of the research being carried out, preparing research administration such as research letters and RAB, preparing a research schedule and dividing tasks between the chairman and research members.
c. Implementation Stages
   In this stage, the lead researcher jointly implements the tasks at the preparation stage, including system issues and frameworks that will be used, designing coding, and testing

the system, finding debugging of the system, both security and user interface issues, and then implement it following the SDLC methodology.

d. Evaluation Stages
At this stage, the head researcher together with the research members compiled, created, and distributed a questionnaire regarding the information system being studied to see weaknesses and possible additional features for maintenance. Next, conclude the questionnaire data regarding overall system readiness.

e. Stages of Implementation Results
At this stage, the chairman makes a report about the results of the encryption application simulation and RGB description of the image.

f. Place and Research Subjects
The research was carried out in South Aceh Regency. The subject of this research is an image whose RGB values are encrypted and described.

IV. Conclusion

Research result

Based on the research, it can be concluded that encryption and description of RGB values can be done by encrypting the normal values and appearance of the image and changing the RGB value from the form of a normal image to a negative image.

References

[1]. Widyanarko, arya. 2007. Studi dan Analisis mengenai Hill Cipher, Teknik Kriptanalisis dan Upaya Penanggulangannya. Bandung: Fakultas Teknik ITB

[2]. Ariyus, D. (2006).”Kriptografi Keamanan Data dan Kriptografi”.Yogyakarta: Penerbit Andi Offset

[3]. Sindar, A., & Sinaga, R. M. (2017). Implementasi Teknik Threshoding Pada Segmentasi Citra Digital. *IMPLEMENTASI TEKNIK THRESHODING PADA SEGMENTASI CITRA DIGITAL*, *1*(2), 48–51.

[4]. Maulana, A.,R. (2012). “Penerapan Algoritma WAKE Pada Aplikasi Chatting & Internet Monitor Berbasis LAN”. Yogyakarta: STMIK Amikom Yogyakarta.

[5]. Sindar, A., & Sinaga, R. M. (2017). Implementasi Teknik Threshoding Pada Segmentasi Citra Digital. *IMPLEMENTASI TEKNIK THRESHODING PADA SEGMENTASI CITRA DIGITAL*, *1*(2), 48–51.

[6]. Muamal Khoerudin (2015, Maret 22-29). Algoritma Hill Cipher (Sandi Hill) Materi Perkuliahan Pada Jurusan Teknik Informatika

[7]. Achriadi, T. Sukma (2019), Journal Publications & Informatics Engineering Research, Feature Extraction Method GLCM and LVQ in Digital Image-Based Face Recognition,(4:1 october 2019)

[8]. Sindar, A., & Sinaga, R. M. (2017). Implementasi Teknik Threshoding Pada Segmentasi Citra Digital. *IMPLEMENTASI TEKNIK THRESHODING PADA SEGMENTASI CITRA DIGITAL*, *1*(2), 48–51.

[9]. Sindar, A., & Sinaga, R. M. (2017). Implementasi Teknik Threshoding Pada Segmentasi Citra Digital. *IMPLEMENTASI TEKNIK THRESHODING PADA SEGMENTASI CITRA DIGITAL*, *1*(2), 48–51.

[10]. Suryadi, H.S., dkk.. Teori Dan Soal Pendahuluan Aljabar Linier. Serial Matematika. Jakarta: Ghalia Indonesia. 1990

[11]. Sindar, A., & Sinaga, R. M. (2017). Implementasi Teknik Threshoding Pada Segmentasi Citra Digital. *IMPLEMENTASI TEKNIK THRESHODING PADA SEGMENTASI CITRA DIGITAL*, *1*(2), 48–51.

[12]. Aplikasi Desktop. (2023). Diperoleh 29 April 2023, dari https://javatekno.co.id/page/aplikasi-desktop