JOURNAL OF DATA SCIENCE | Vol.2023:19
eISSN:2805-5160

Information Security Analysis and Solution using LSB Steganography and AES Cryptographic Algorithm

Nurul Adha Oktarini Saputri[1], Novita Epa Sari[2]

[1,2]Faculty of Computer Science, Informatics Engineering, Bina Darma University

Email: [1]nuruladhaos@binadarma.ac.id, [2]novitaepasari@gmail.com

Abstract

The significance of information security analysis and solutions has been emphasized by earlier research in several application areas. As a result, information technology has advanced more, particularly in the areas of security and data secrecy. An essential component of data exchange is security and confidentiality. A message must first be hidden or encrypted in the picture media to ensure its security and confidentiality. Our research presents a method for this study, which involves hiding digital images with color at a depth of 24 bits. Through the development of a system to improve the security and confidentiality of data in the form of critical messages, this study seeks to provide senders with solutions. Images are encrypted using the least significant bit (LSB) steganography technique. The AES algorithm is the cryptographic technique used to lock or encrypt data. The LSB utilized in this work involves putting ciphertext bits into the image's color component pixel matrix's diagonals. In this work, the recovery elements of the modified LSB and AES algorithms were examined to conduct testing.

Keywords

Steganography, Modified LSB, Cryptography, AES

Introduction

Many institutions are still hindered by a lack of awareness of the importance of maintaining the secrecy of data that is considered important. Even after what happened in Tanding Marga Village, one of the institutions where we conducted our study, implementing the security and secrecy system is still a difficult challenge. In addition, there is a problem with the system's inability to store community data or information. Based on the current issues, we as the researchers develop a prototype system development method that includes directly involving users in the system's design and employing iterative design until the desired agreement is reached to create a system to secure critical data in Tanding Marga Village.

The use of the system is divided into two parts: one is for the sender of the message to be able to encrypt the message first before it is sent to the recipient of the message, and the second is for the recipient of the message to be able to read the message first to extract the message so that

Submission: 26 November 2023; **Acceptance:** 1 December 2023

the recipient of the message can read it, by using the LSB (Least Significant Bit) steganography method and AES (Advanced Encryption Standard) cryptography.

In addition, this system uses an image (image) as a container that is used to insert a secret message by first encrypting the message and becoming a ciphertext so that no one can read the message except the recipient of the message by describing the message with a key that is known only to the sender and recipient.

Steganography comes from the Greek language and consists of 2 syllables: steganos, which means hidden, and graphia, which means writing. Thus, steganography is the science or art used to hide. Those who can find out are only the message's owner and trusted people. This LSB steganography will discuss how to insert or disguise messages (Anwar, 2017).

The least significant bit (LSB) method is one of the substitution techniques in the steganography method. In this LSB, every bit that is the lowest in the digital image bytes will be immediately replaced with the bit that will be inserted in the message. In general, steganography has two processes: message embedding and message disclosure (extraction) (Putra et al., 2018).

Since 1976, the United States government has chosen the DES (Data Encryption Standard) algorithm as the cryptographic standard. But in 1990, the DES key was considered too short, and then in 1998, DES was successfully broken within 96 days, and in 1999, within 22 days, it could be solved again. Therefore, NIST (National of Standards and Technology) held a competition to find a replacement for DES. NIST uses participating participants from all over the world (Anwar, 2017).

Cryptography comes from the Greek words cryptos (secret) and graphia (writing). Thus, cryptography means secret writing or secret writing (Putra et al., 2018). Combining the LSB steganography algorithm and AES cryptography will improve the quality of data security. From the above explanation, the researcher aims to apply steganographic and cryptographic methods to messages that will later become security targets.

The science or art used to hide messages is called steganography. Implementing steganography aims to keep the secret message from being known by others. Those who can find out are the owner of the message and the person he wants (Kumar & Km, 2010). The substitution technique used in the steganography method is the LSB method. Each lowest bit in the digital image bytes will soon be replaced by the message bit to be inserted. The image has an arrangement of three colors, namely red, green, and blue (RGB), in which there is an arrangement of 8 bits (1 byte) from 0 to 255 or in binary format 00000000 to 11111111. The LSB method is the simplest and easiest to implement steganography. This method uses a digital image as cover text to arrange bits in a byte (1 byte – 8 bits). The leading bit is called the most significant bit (MSB), and the last bit is called the least significant bit (LSB) (Pristiwanto & Hasugian, 2021).

Cryptography is the most effective way to use important information, transmitted in communication networks and stored in government media. Cryptographers are people who do encryption, while cryptanalysts are people who study science and art or people who can solve the algorithm without knowing the key (Bhattacharya, 2019).

The science and art used to protect secret messages by encoding them into a form that is no longer easy to understand is the meaning of cryptography. Cryptography also consists of two processes, namely encryption and description. The process of encoding an open message into a secret message (ciphertext) is the meaning of encryption. This ciphertext will be sent via the communication channel (Sharma, 2017).

The ciphertext received by the recipient of the message will be converted again into an open message, which will go through an encryption process so that the message can be re-read by the recipient (Karlita, 2017). The encryption process and process description will be described in Figure 1.

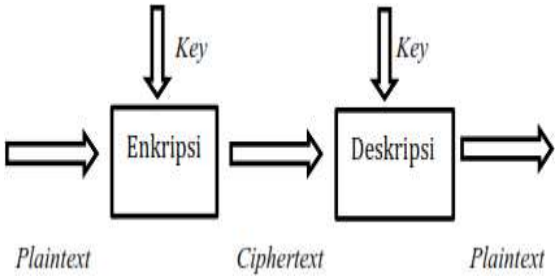

Figure 1. Encryption process and description

In this research, an experiment for implementation of Data and Information Security with LSB Steganography and AES Cryptographic Algorithm is conducted.

Methodology

Data Collection Methods

In this study, researchers used data collection methods as follows (Kabir, 2016):

Observation

Observations were carried out to collect data by interacting directly by coming to a place that would become the object of research and meeting with the Tanding Marga Village Head to record or record every event/incident with scientific or other purposes with the help of tools.

Interview

Interviews were conducted as a communication process by asking directly to relevant informants directly to obtain accurate and reliable information as a reference for research material. Questions are profound, with the objectives set to receive data according to the researcher's wishes.

Library Studies

A literature study is intended to gain deeper insight into analyzing each problem by examining each written source from various expert opinions in books or journals to support data collection in studying each issue being researched.

System Development Method

In developing the system this time, the researchers used the prototype method. It will start with gathering user requirements after creating a prototype that will be built, then evaluated by the user on the Prototype, and will be used to define what is needed for software development (Tizkar & M. Tabatabaei, 2009).

In prototyping, there are several stages, namely as follows:

Collection of Requirements

Customers and developers will initially get together to define all software formats, then identify all needed and the system line to be built.

Building prototypes

Creating a temporary system design and focusing on serving the user is a way of building prototypes.

Prototyping Evaluation

This stage will evaluate whether the prototyping design that has been made is as desired. Step 4 can be taken if appropriate, and if it is not suitable, then the prototyping will be repeated back to steps 1,2 and 3.

Encoding System

The appropriate prototyping will be applied to the agreed programming language at this stage.

Testing the System

The system has become software and is ready to use. So, it must be tested before use. The tests will be carried out in white boxes, black boxes, primary paths, architectural tests, and so on.

System Evaluation

The user evaluates the system to determine whether the system is following what is desired. If it is appropriate, then step 7 will be taken.

Using the System

Software that has been tested and confirmed is then received by the user and is ready to be used. After going through the stages of prototyping development, it can be continued with the goals to be achieved with the prototyping.

Results and Discussion

System Analysis

In general, there are two steganography processes: embedding and extracting.

Process Embedding Message

The steps involved in the embedding process start from AES encryption, which transforms the original message (plaintext) into a random message (ciphertext), followed by embedding it in the digital image of the carrier (carrier). The illustration will be explained below, as shown in Figure 2.

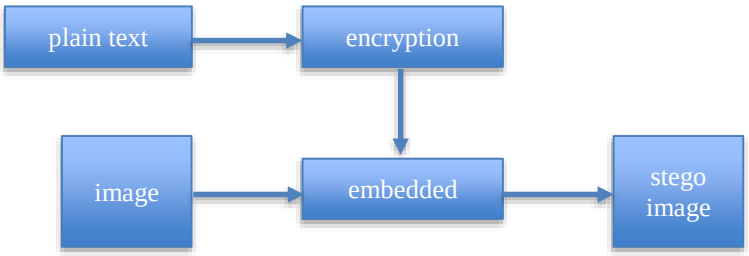

Figure 2. Embedding process

Message Extraction Process

Ciphertext can be extracted from a stego image by extracting the message using a modified LSB, which will replace the byte diagonal to insert ciphertext, as shown in Figure 3.

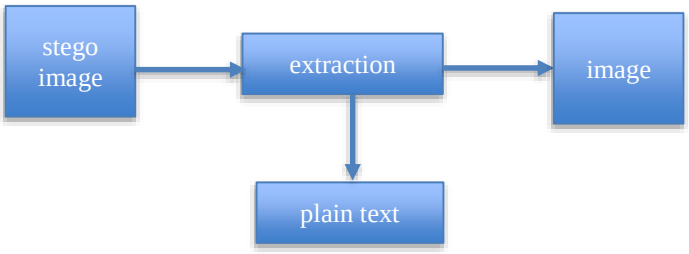

Figure 3. The process of extraction

System Design

The insertion process (embedding) selects a predetermined cover object to insert a message. For a clearer picture, see the Figure 4 below.

Then, carry out the extraction process. First, re-enter the *stego* image (the image result after the embedded process) that has been inserted with the message, and the goal is to be able to read back the message hidden in the image, as shown in Figure 5.

The AES cryptographic algorithm method has a process of encryption and description. The encryption process consists of 4-byte transformation stages: SubBytes, ShiftRows, Mixcolumns, and AddRoundKey. In encrypting messages that have been input into the state, they will transform SubBytes, ShiftRows, MixColumns, and AddRoundKey. Repeatedly, as many as Nr (Kong et al., 2013). The AES algorithm is called a round function. The last round is the state that does not undergo a Mix of Columns transformation.

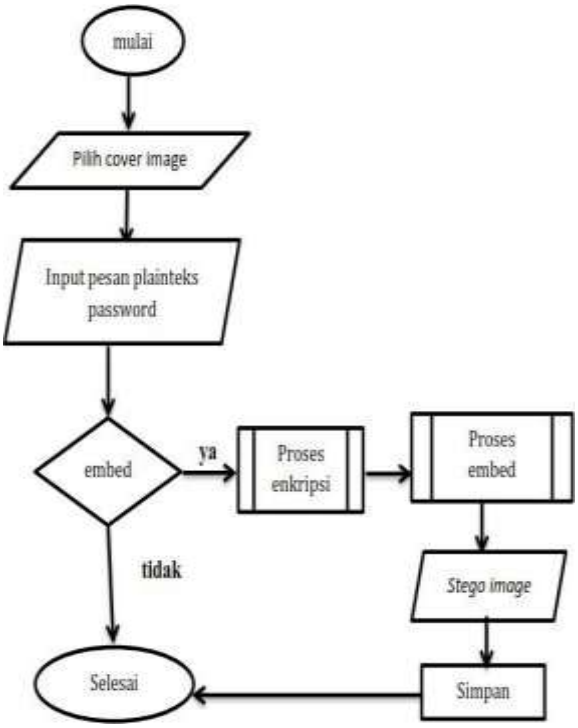

Figure 4. Embedding process flowchart

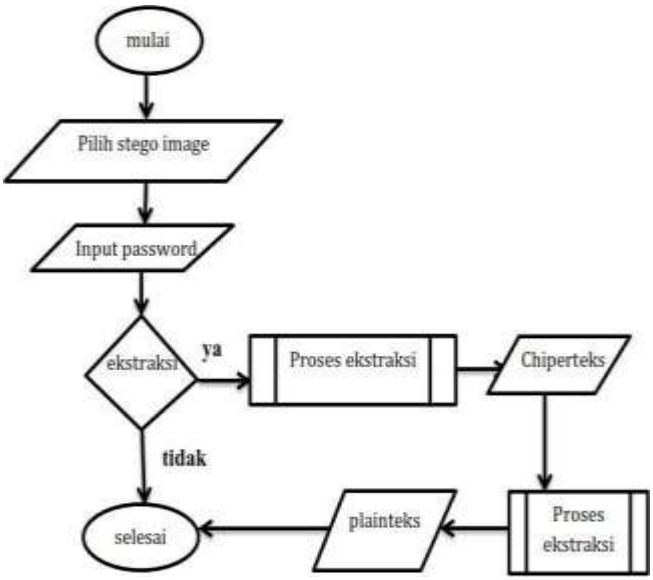

Figure 5. Extract process flowchart

Next is the transformation cipher, the opposite of encryption, to generate a hopeful cipher inverse for the AES algorithm. The Byte transformations used in the inverse chipper are InvShifftRows, InvSubBytes, InvMixColumns, and AddRoundKey.

System Implementation

System Interface Implementation
In implementing the system, researchers used Microsoft Visual Studio, which was used as a tool for implementing steganography and cryptography using the PHP programming language. The coding function is implemented and integrated into the GUI (graphical user interface). Implementation of all stages of analysis and design of the interface can be seen as follows:

Display Home Page
The home page is the main page before inserting a message, as shown in Figure 6.

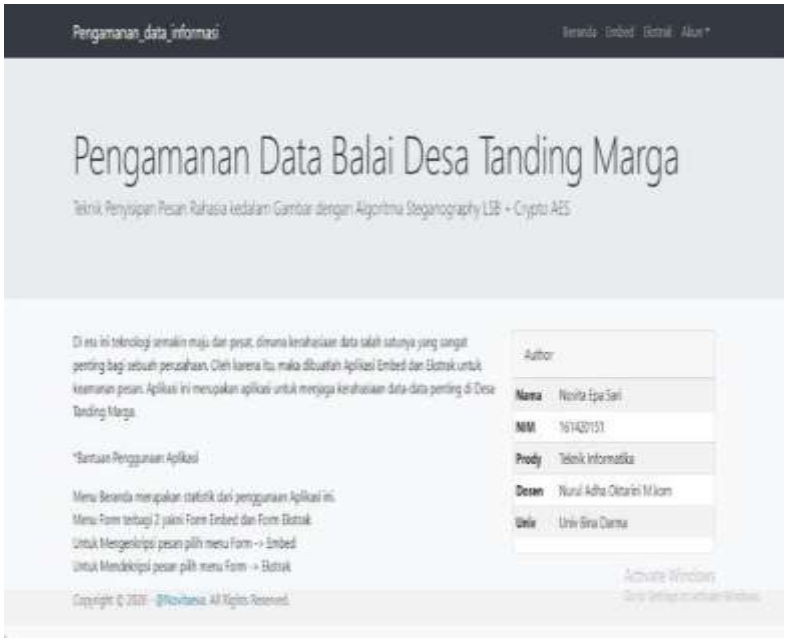

Figure 6. Home page

View the Embed Page
The embed page is a page for inserting a secret message into the cover object, namely a digital image, and is a page that plays an essential role in this system because the system will not work if there is no embed page, as shown in Figure 7.

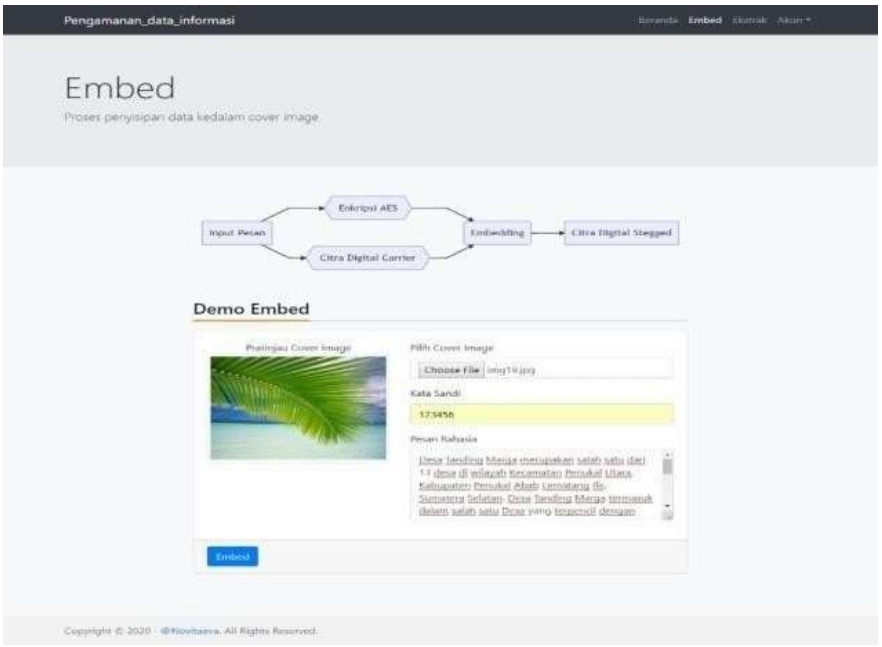

Figure 7. Embed page.

Page View Extract
On this extract page, messages hidden in the *stego* image can be re-read, as shown in Figure 8.

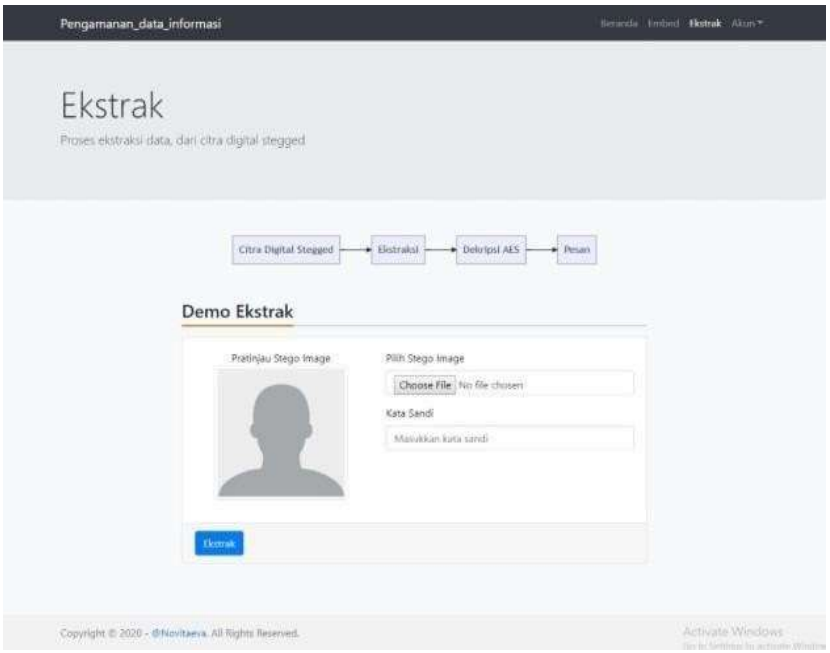

Figure 8. Extract page.

System Discussion

Embedding process page (insertion)
The user is asked to enter a cover image as a message storage medium in the embedding process (Kumar Bandyopadhyay et al., 2010). The user enters a password and enters data in the form of

text, which has a maximum number of words of 244800 bytes, by copying the text file into the secret message form and then clicking the embed button, as shown in Figure 9. If the hidden text exceeds capacity, then the system will give an error.

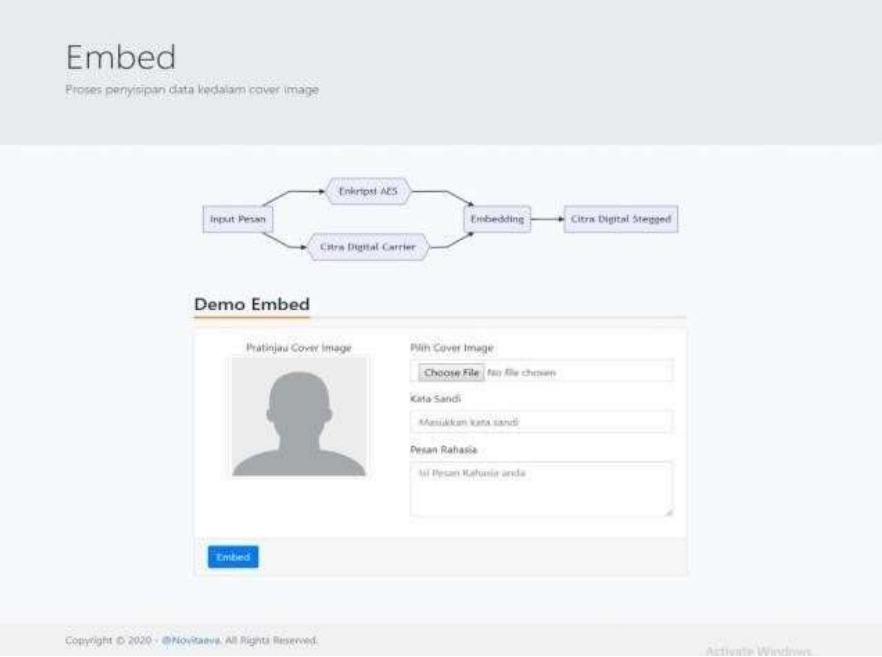

Figure 9. Embed process.

Embedding Result Page (insertion)
Messages inserted in a *stego* image will then automatically be stored in the download folder on the user's computer and are difficult to distinguish by the human senses because there is no visible difference, as shown in Figure 10.

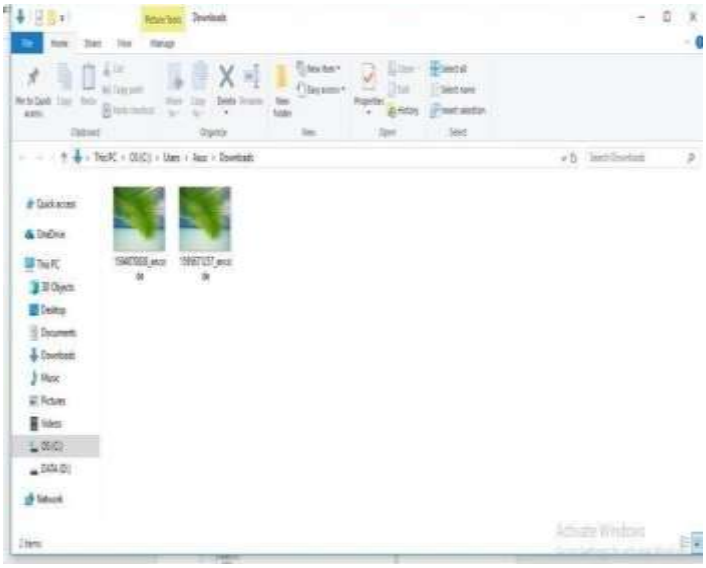

Figure 10. Embed results.

Extraction Process page

This extract process page will explain how to process the hidden message description by re-entering the *stego* image in the extract menu, entering the password created on the embed page, and then clicking the extract button, as shown in Figure 11.

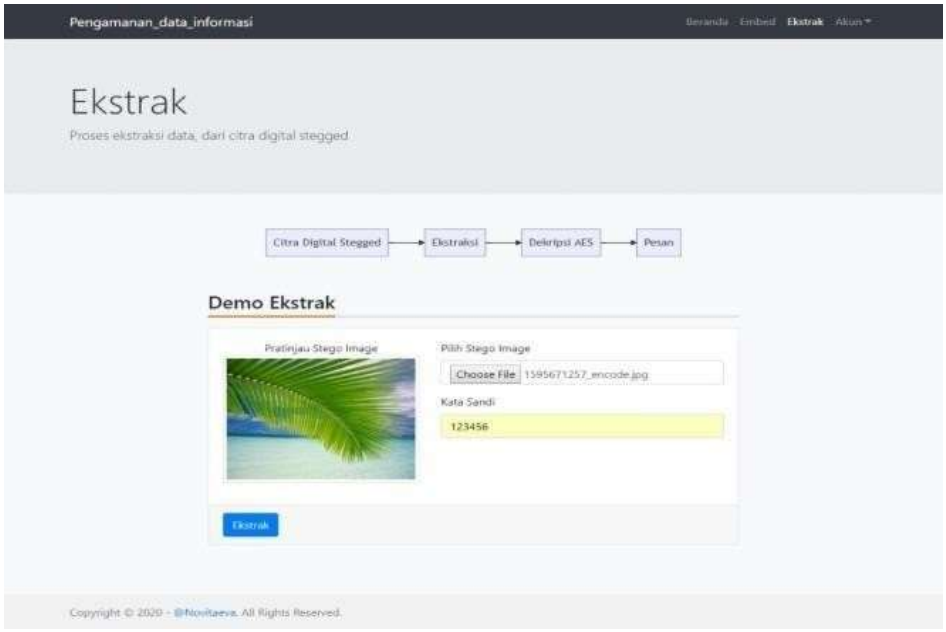

Figure 11. extraction process

Extraction Results

On this page, the results of extracting messages and users can re-read messages stored in the *stego* image into plain text messages. Anyone can read them because they are no longer hidden in digital images, as shown in Figure 12.

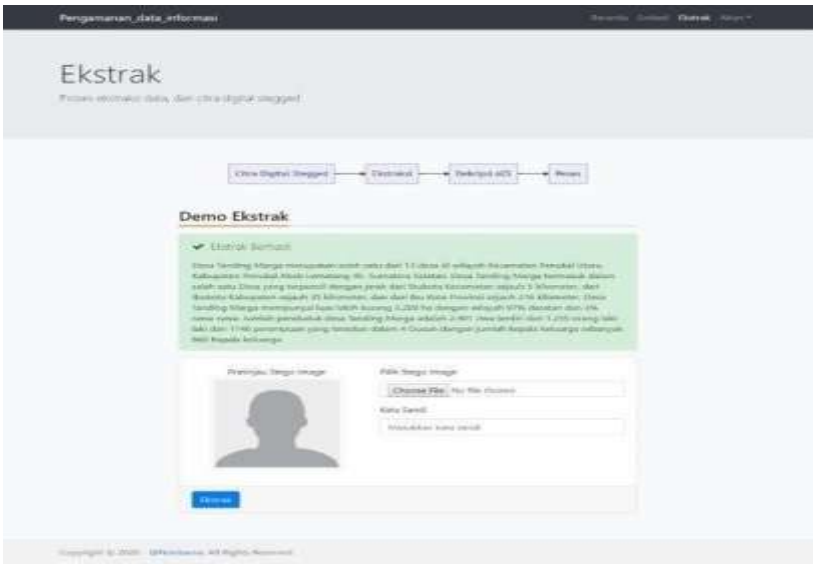

Figure 12. extraction results

Conclusion

Following the completion of all experiments, it can be concluded that the LSB steganography method and the AES cryptographic algorithm have been successfully implemented. Additionally, testing has been done on several instances. It can demonstrate whether the adjusted LSB approach is suitable in situations when it is challenging to visually recognize hidden messages embedded in digital photos. The reason for this is that the stego image has not undergone any noticeable alterations or adjustments. The size of the messages determines how quickly they are encrypted and embedded. For future enhancement of this security system, it is hoped that in the future, it will be possible to secure messages in the form of Microsoft Word files so that they can be more effective and efficient, and there is no need to copy the file's contents into the secret message form on the embed menu. It is expected to create an Android-based security system to make it easier.

References

Anwar, S. (2017). Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES. *Jurnal Format*, *6*(1), 65–74.

Bhattacharya, S. (2019). Cryptology, Cryptography, and Cryptoanalysis-Past, Present and Future Role in Society. *International Journal of Computer Science and Information Technology Research*, *7*, 16–33. www.researchpublish.com

Kabir, S. M. (2016). METHODS OF DATA COLLECTION. In *Basic Guidelines for Research: An Introductory Approach for All Disciplines : Vol. Chapter 9* (pp. 201–275).

Karlita, T. (2017). HILLMAIL: A SECURE EMAIL SYSTEM FOR ANDROID-BASED MOBILE PHONE USING HILL CIPHER ALGORITHM. *Kursor*, *8*, 141. https://doi.org/10.28961/kursor.v8i3.89

Kong, J. H., Ang, L.-M., & Seng, K. P. (2013). A Very Compact AES-SPIHT Selective Encryption Computer Architecture Design with Improved S-Box. *Journal of Engineering*, *2013*, 785126. https://doi.org/10.1155/2013/785126

Kumar, A., & Km, P. (2010). Steganography- A Data Hiding Technique. *International Journal of Computer Applications*, *9*. https://doi.org/10.5120/1398-1887

Kumar Bandyopadhyay, S., Datta, B., Chakrabarty, D., Majumdar, A., Bhowmick, S., & Ghosh, N. (2010). A NEW METHOD FOR EMBEDDING DATA WITHIN AN IMAGE. In *Journal of Global Research in Computer Science Journal of Global Research in Computer Science* (Vol. 1, Issue 5). www.jgrcs.info

Pristiwanto, P., & Hasugian, A. (2021). Steganography Formation by utilizing Enhanced Least Significant Bit Algorithm. *Jurnal Info Sains : Informatika Dan Sains*, *11*, 19–22. https://doi.org/10.54209/infosains.v11i1.38

Putra, R. R., Sari, M., Utama Siahaan, A. P., & Iqbal, M. (2018). Implementation of LSB Steganography on Embedding Messages in Digital Image. *International Journal of Scientific Research in Science and Technology*, 38–43. https://doi.org/10.32628/ijsrst18401112

Sharma, S. (2017). Cryptography: An Art of Writing a Secret Code. *International Journal of Computer Science and Telecommunications*, *8*(1).

Tizkar, A., & M. Tabatabaei, N. (2009). Rapid Prototyping for Software Projects with User Interface. *Scientific Bulletin of University of PITESTI, Electronics and Computer Science Series*, *2*, 85.