The Application Of Encryption And Decryption To The Delivery Of Text Messages Using The Rc4 Algorithm (Rivest Code 4) Utilizes The Lsb (Least Of Significant Bit) Algorithm As An Insertion Into The Image

Al Boy In [1*] , Achmad Fauzi [2] , Hermansyah Sembiring [3]
[1,2,3] STMIK Kaputama Binjai, Indonesia

Email : alboyin11@gmail.com

Abstract

The use of image media information has several disadvantages, one of which is that it is easy to manipulate by certain parties with the help of technology that is developing today. Efforts that can be made in improving the security of the transmission of image information are cryptography, which is the science and art of keeping messages safe. In this study, the RC4 (Rivest Code 4) and LSB (Least Of Significant Bit) stegnography methods were applied which aimed to obtain a stronger cipher by inserting messages into the image so that it was difficult to intercept. RC4 (Rivest Code 4) algorithm for encrypting and decryption, LSB (Least Of Significant Bit) stegnography used to decode and decode images. The results of this study show that by applying RC4 (Rivest Code 4) and LSB Stegnography (Least Of Significant Bit) can secure messages inserted into the image and secure keys for data needs. The encoding and decoding process time is influenced by the number of messages that will be kept secret.

Keywords: Cryptography, Image, LSB, Message, RC4, Stegnography.

INTRODUCTION

The world of information technology that is developing rapidly these days has an impact on every aspect of life. One of them is the protection of confidential information. Basically, the transfer of information is carried out by transmitting data without protecting what is sent. Confidentiality of information is an important aspect, Confidential information needs to be hidden from unauthorized persons. Proper use of information technology is important for sending confidential messages to certain parties. However, the delivery is still not well secured, so the unwanted party can be misappropriated for adverse purposes to the detriment of the other party.

For this reason, a security system is needed that can protect messages sent through communication from being hidden into the image so that it is not easy to know the content of the message. One way that can be done safely by using the RC4 algorithm and Least Significant Bit steganography (LSB) is designed to maintain the confidentiality of the information contained in an image so that it cannot be known by unauthorized parties. For double protection of messages hidden in the image can create two layers of security and provide protection of such confidential messages. Secret messages can be extracted using the same key and the messages will return to the way they were originally.
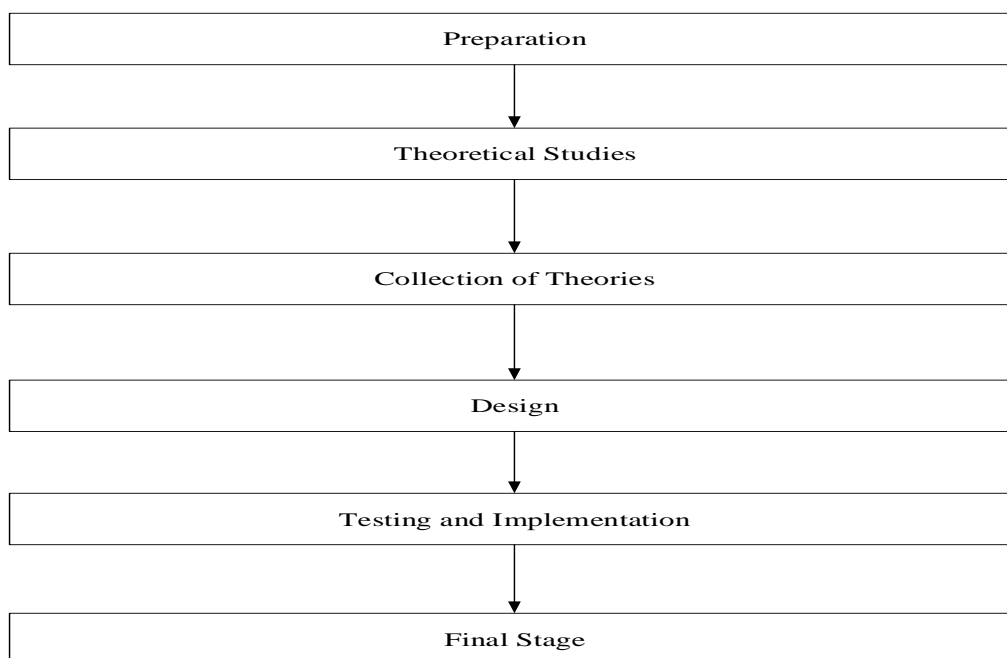
RESEARCH METHODS

Figure 1. Research Workflow

The explanation of the research workflow picture above is as follows:
1. Preparation
This stage is the initial activity in conducting research, namely by making a background problem then the formulation of the problem then limiting the problem to be solved and determining the goals and benefits of this research. After that, the author determines the image to be encrypted encoding and decoding decrypted which later the image is encoded and cannot be opened by a third person.
2. Theoretical Studies
In this stage, the author collects various theories both from books borrowed from libraries, journals and the internet to support the research to be carried out. The theories collected include securing the insertion of messages into images, the RC4 (Rivest Code 4) LSB (Least Significant Bit) steganography algorithm, visual basics and image.
3. Collection of Theories
At this stage, the author conducts a Library Study (Library research) Library study is carried out with the aim of knowing what methods will be used to solve the problems studied, as well as getting strong reference basics in applying a method that will be used in this thesis, namely by studying books, journals or internet sites related to the problems to be discussed.
4. Design
At this stage, the author performs or makes calculations manually with the RC4 (Rivest Code 4) algorithm of LSB steganography (Least Significant Bit) which then designs the system to be built.

5. Testing and Implementation
a. This stage is a very important stage, namely testing and implementing the system that has been created. This stage is based on the design that has been carried out. Implemented the RC4 (Rivest Code 4) algorithm LSB steganography (Least Significant Bit) into a Microsoft Visual Basic Net 2012 programming language.

b. Perform and run the program to see the results of the insertion of the k message in the encoded image, whether there is still an error (error).

c. Correct revisions to the design of program applications that experience errors (errors).

6. Final Stage

At this stage, the author will discuss the conclusions and also suggestions from the results of the research that has been carried out.

System Analysis

System Analysis is defined as a technique used to understand and create specifications with details of what the System should do. With the analysis of the system, the system to be designed is expected to be better and easier in the next system development. The purpose of this system analysis itself is to help model the design of the System to be implemented in tangible form.

Problem Analysis

Developments in the field of online technology as they are today have allowed everyone to exchange information with each other without any restrictions on distance and time. It is not closed to the possibility of data leakage during the information exchange process carried out, so that the sender of the information. So it can reduce threats that can occur in the exchange of confidential information in a data communication process can be done by coding the information that will be stored or sent quickly and accurately. The problem in this system is how to secure the exchange of information, especially in the form of messages inserted into the image.

The Role of The System

In the application system of insertion of messages in this image the author uses the algorithm RC4 (Rivest Code 4) steganography LSB (Least Significant Bit) in solving the problem. Where this design uses a flowchart to find out how the encoding encryption process and decryption decoding will be designed in a system.
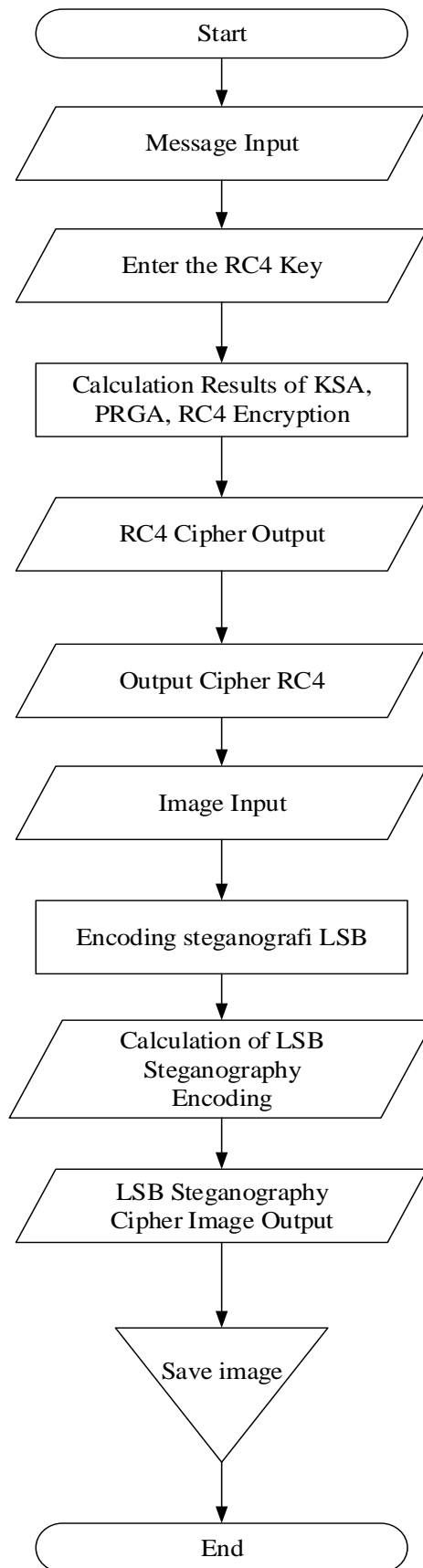
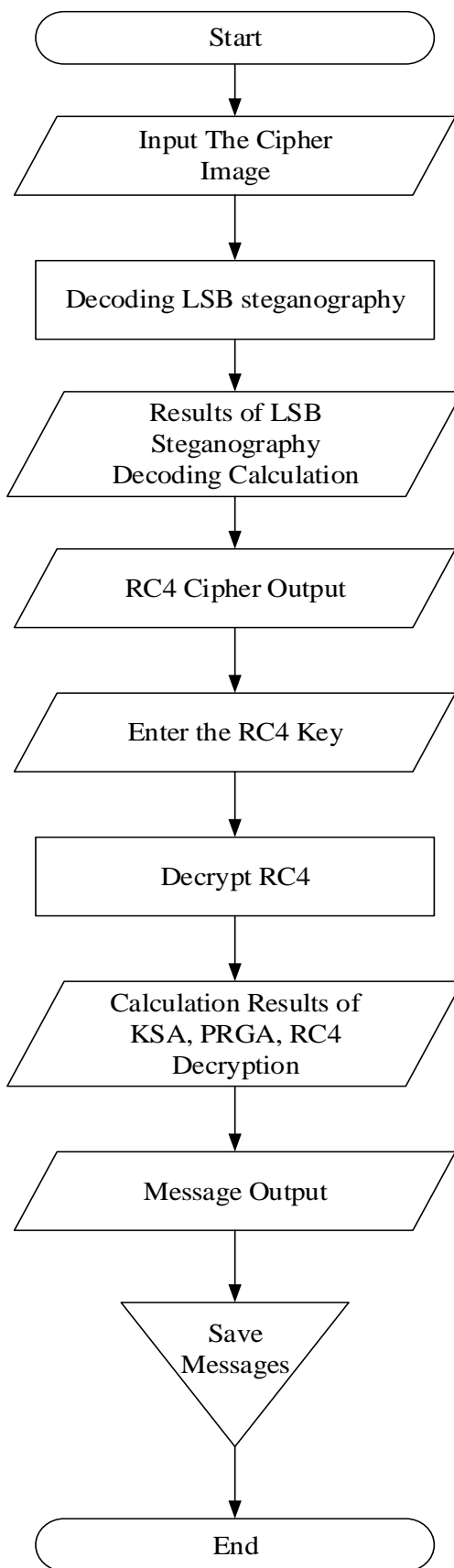**Figure 2. Flowchart Encryption Encoding**

Figure 3. Flowchart Decoding Decryption

RESULTS AND DISCUSSION

Discussion of System Interfaces

The appearance of the image repair system that has been designed using the Visual Basic 2012 programming application, with the application of the RC4 algorithm and LSB Steganography in insertion of messages on the image, is as follows:

System Main Page View

After the program is run, the system will display the main page of the system that has been built, in the main page view of the system there is a menu that can be used by the user, namely the main page menu, encoding encryption, decoding decryption and exit. The main page display of the system is as follows:
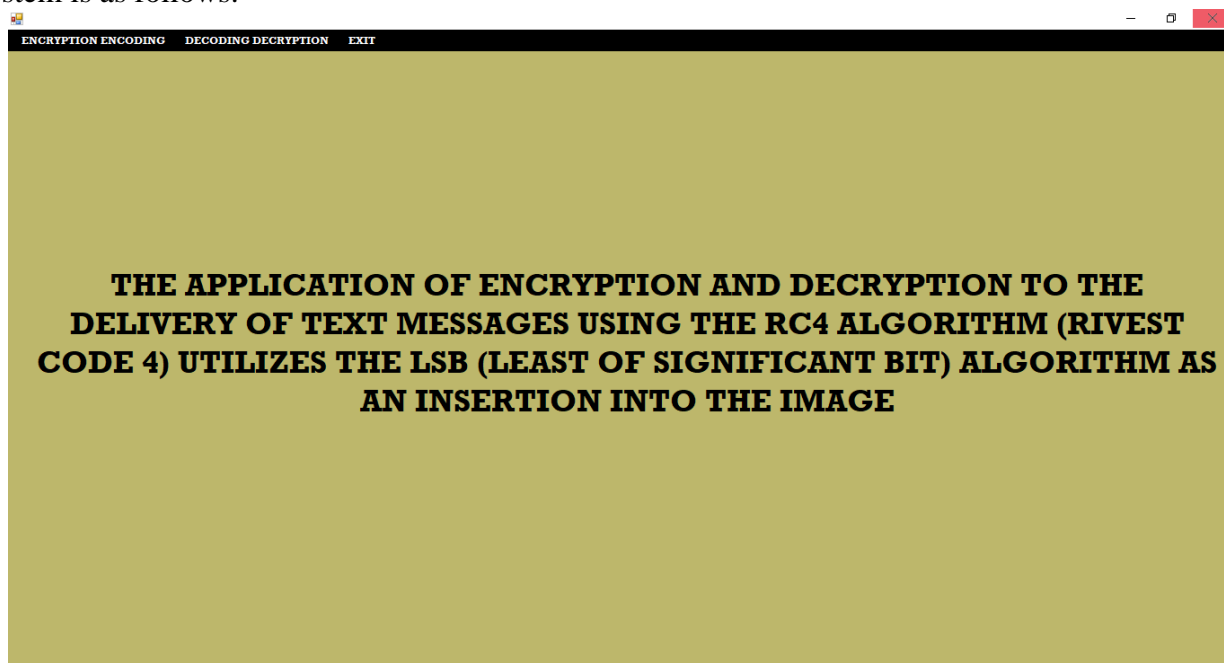

ENCRYPTION ENCODING　　DECODING DECRYPTION　　EXIT

THE APPLICATION OF ENCRYPTION AND DECRYPTION TO THE DELIVERY OF TEXT MESSAGES USING THE RC4 ALGORITHM (RIVEST CODE 4) UTILIZES THE LSB (LEAST OF SIGNIFICANT BIT) ALGORITHM AS AN INSERTION INTO THE IMAGE

Figure 4. Main Page View

Page View Encryption Encoding Insertion Of Messages On Imagery

In this display, the system will display the Message Input to be secured, after that enter the key where the result of encrypting the message with the RC4 algorithm, then the RC4 calculation appears. next will input an image that will be selected after that carry out the encoding process where the LSB steganography calculation will appear and the encoding results will appear that have been inserted, then will save the image that has been inserted. Button resets to reset if there are any errors, and Button exits when it has finished encoding encryption. The display of the encoding encryption page is as follows:
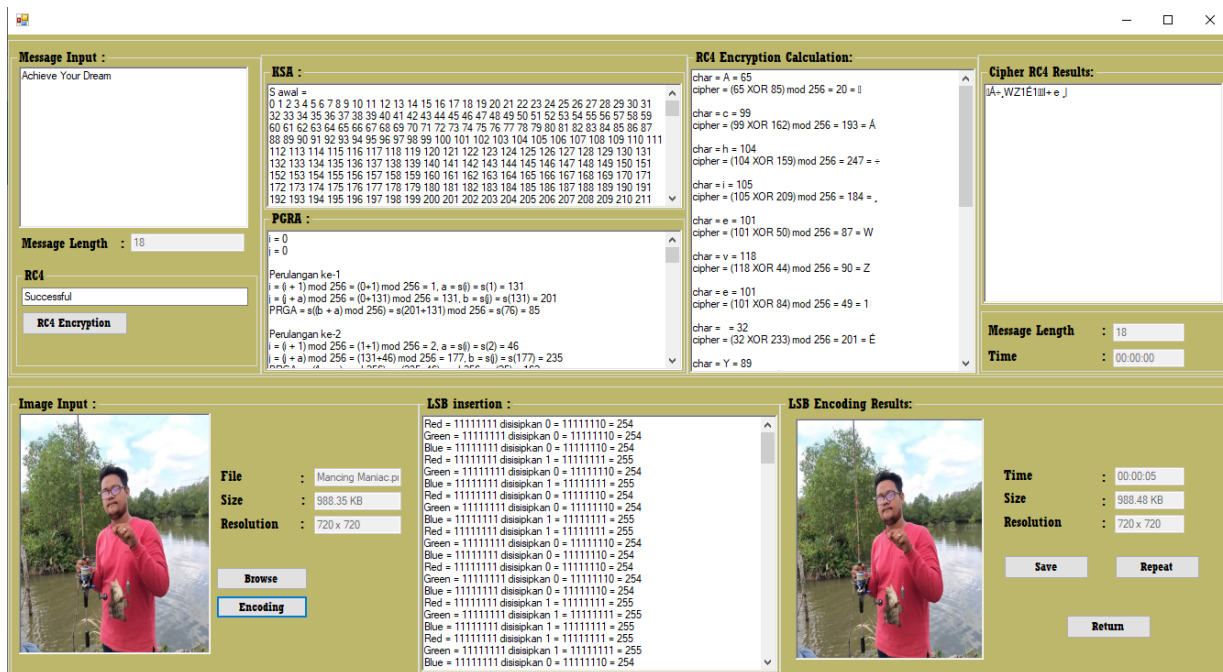
Figure 5. Page View Encoding Encryption

Page View Decoding Decryption of Message Insertion On Imagery

In this display, the system will display the Input Image password and will decode and appear the LSB steganography decoding calculation and the RC4 cipher result, input the key to perform RC4 decryption, the RC4 decryption calculation will appear and the original message content will appear. Next will do save the message. Button reset to reset if there is an error, and Button exits when it is finished decoding decryption. The decryption decoding page display is as follows :
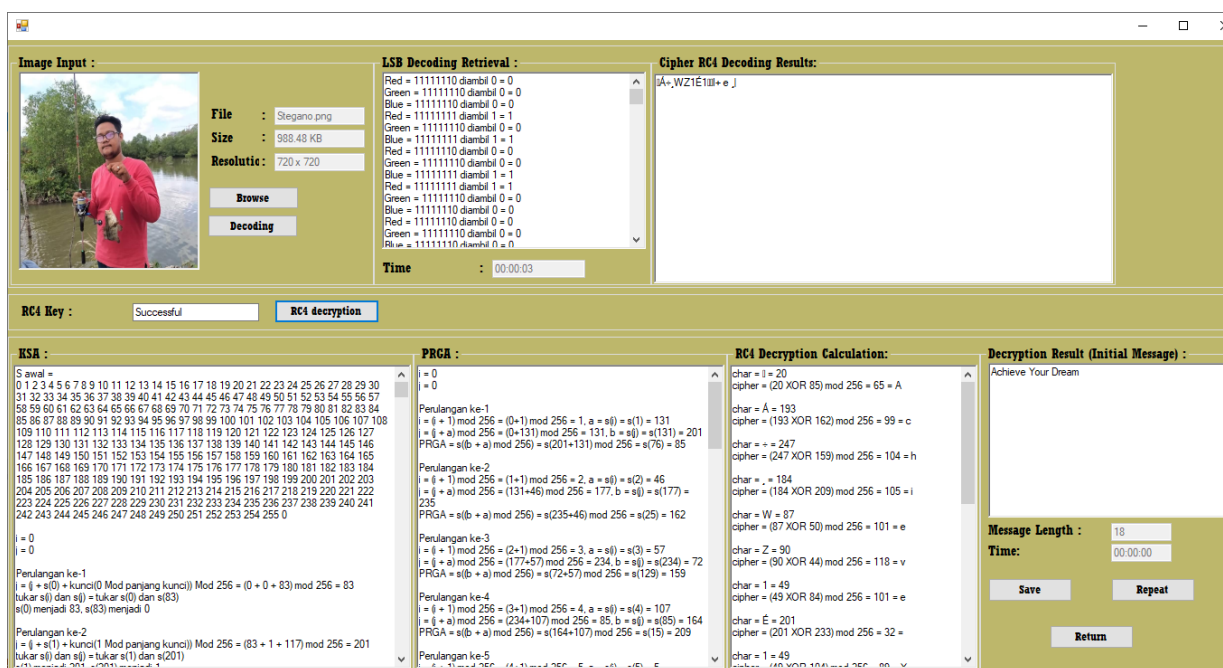

Figure 6. Page View Decoding Decryption

CONCLUSION

1. In insertion of messages into the image is successfully implemented and able to carry out the encoding encryption process and decryption decoding the more the message, the time of the encoding encryption process and decryption decoding will take a longer time, The test results on the system are obtained that messages that have undergone the encoding encryption process and decryption decoding with RC4 algorithms and LSB Steganography, has the same information content as the original message that has been inserted.
2. Insertion of messages on images by using RC4 algorithms and LSB Steganography to keep messages secret goes well. the message was successfully inserted into the image by means of encoding encryption and decryption decoding processes, experiments carried out on the RC4 algorithm and LSB Steganography.

REFERENCES

Ardiansyah, A., & Kurniasih, M. (2018). Concealment of Secret Messages On Digital Images With Steganograpi Technique Using Least Significant Bit Method. XIII(November), 96–101.

Darwis, D. (2016). Implementation Of Least Significant Bit Steganography Techniques (LSB) And Compression For Securing Electronic Mail Sending Data. Journal of Technoinfo, 10(2), 32. https://doi.org/10.33365/jti.v10i2.8

Mukhtar, H. (2018). Cryptography For Data Security. Yogyakarta: CV. MAIN BOB.

Kusniyati, H., Diansyah, S., Yusuf, R., Informatics, J., Computer, F. I., & Buana, U. M. (2018). Application of the rivert code 4 (rc 4) algorithm to document cryptographic applications. 11(1), 38–47.

Minarni, M., & Fernando, A. G. (2020). IMPLEMENTATION OF THE END OF FILE (EoF) ALGORITHM ON IMAGE STEGANOGRAPHY. TechnoIf Journal, 8(1), 25. https://doi.org/10.21063/jtif.2020.v8.1.25-31

Nurdin, A. P. N. (2017). Cryptographic Analysis and Implementation of Confidential Messages. Jesik, 3(1), 1–11. nnurdin69@gmail.com

Prabowo, D. A., & Abdullah, D. (2018). Object Detection and Calculation Based on Color Using Color Object Tracking. Pseudocode, 5(2), 85–91. https://doi.org/10.33369/pseudocode.5.2.85-91

Saragi, D. R., Gultom, J. M., Tampubolon, J. A., & Gunawan, I. (2020). Securing Text File Data (Word) Using RC4 Algorithm. Journal of Computer Systems And Informatics (JSON), 1(2), 114. https://doi.org/10.30865/json.v1i2.1745

Simatupang, J., & Sianturi, S. (2019). Design of Bus Ticket Booking Information System On Po. Handoyo Based Online. Intra-Tech, 3, 16-18.

Sugiarti, Y. (2013). UML Analysis and Design (Unifed Modeling Language). Graha Ilmu, Yogyakarta

Wahana, K. (2013). Visual Basic 2012 Programming (Hernita P ed.). (A. O. C.V, Ed.) Semarang: Computer Rides. Retrieved 2013

Zebua, T., & Ndruru, E. (2017). Digital Image Security Based on Algorithm Modifications Rc4. 4(4), 275–282. https://doi.org/10.25126/jtiik.201744474