International Journal Of Health, Engineering And Technology (IJHET) *E-ISSN 2829 - 8683*
Volume 1, Number 3, September 2022, *Page. 430 - 438*
Email : editorijhess@gmail.com

MSB Steganography Text Message Insertion Technique On Imagery With Otp And RSA Algorithms

Resti Afrelia Sibuea[1*)], Akim M.H. Pardede [2)], Katen Lumbanbatu [3)]
[1,2,3)] STMIK Kaputama Binjai, Indonesia

*Corresponding Author
Email : restiafrelia46@gmail.com

Abstract

The use of image media information has several weaknesses, one of which is that it is easy to be manipulated by certain parties with the help of currently developing technology. Efforts that can be made in increasing the security of sending image information are cryptography, which is the science and art of maintaining message security. In this study, the OTP, RSA and MSB (Most Significant Bit) steganography methods were applied which aim to obtain a stronger cipher by inserting a message into the image so that it is difficult to tap. OTP and RSA algorithms for encrypting and decrypting, MSB (Most Significant Bit) Steganography which is used for encoding and decoding images. The results of this study indicate that by applying the OTP, RSA and MSB (Most Significant Bit) Steganography algorithms can secure messages that are inserted into the image and secure the key for data needs. The encoding and decoding process time is affected by the number of messages to be kept secret.

Keywords: Cryptography, Image, Message, OTP, RSA, Steganography MSB (Most Significant Bit).

INTRODUCTION

Data exchange or transactions are things that are widely done in everyday life in the era of rapidly developing technology. The information sent is confidential or private. Therefore, data needs to be encoded or kept secret so that it is not known by irresponsible parties.

Cryptography is the science and art of keeping messages safe when messages are sent from one place to another. Cryptography is one of the components that cannot be ignored in building data security on a computer. The One Time Pad algorithm belongs to the group of symmetry cryptographic algorithms. One Time Pad (pad = paper block notes) contains rows of characters - key characters that are randomly generated, and their randomization does not use a specific formula. If the key is completely random, used only once, and maintained its confidentiality well, then this OTP encoding method is very powerful and unbreakable.

In data security, cryptographic techniques will generate ciphertext that will arouse suspicion to third parties that the data transmitted is confidential or important data. Therefore, other techniques are needed to dispel these suspicions. A technique that serves to hide data without arousing suspicion to third parties is Steganography.

Steganography in particular is a science, technique and art of how to hide confidential data in an image media so that the existence of the confidential data is not known by others. The steganography process is to hide data (embedding) on a medium, then through the extraction process (extracting), it can display the original data that is hidden. Steganography also has various concealment techniques, one of which is the MSB (Most Significant Bit) Technique.

RESEARCH METHODS

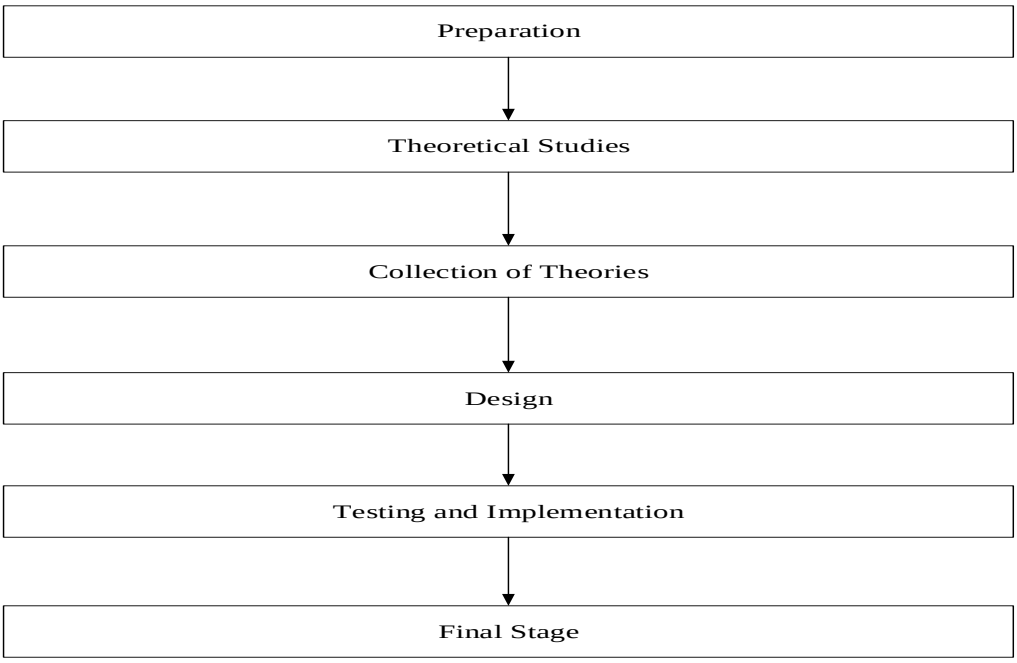

Figure 1. Research Workflow

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, OTP algorithms and RSA Steganography MSB, visual basics and images.

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 OTP algorithm and RSA Steganography MSB 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. Implements the MSB OTP and RSA Steganography algorithms into a Microsoft Visual Basic Net 2010 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 OTP Algorithm and RSA Steganography of the MSB File in resolving the problem. Where this design uses a flowchart to find out how the encoding encryption and decoding decryption processes will be designed in a system.

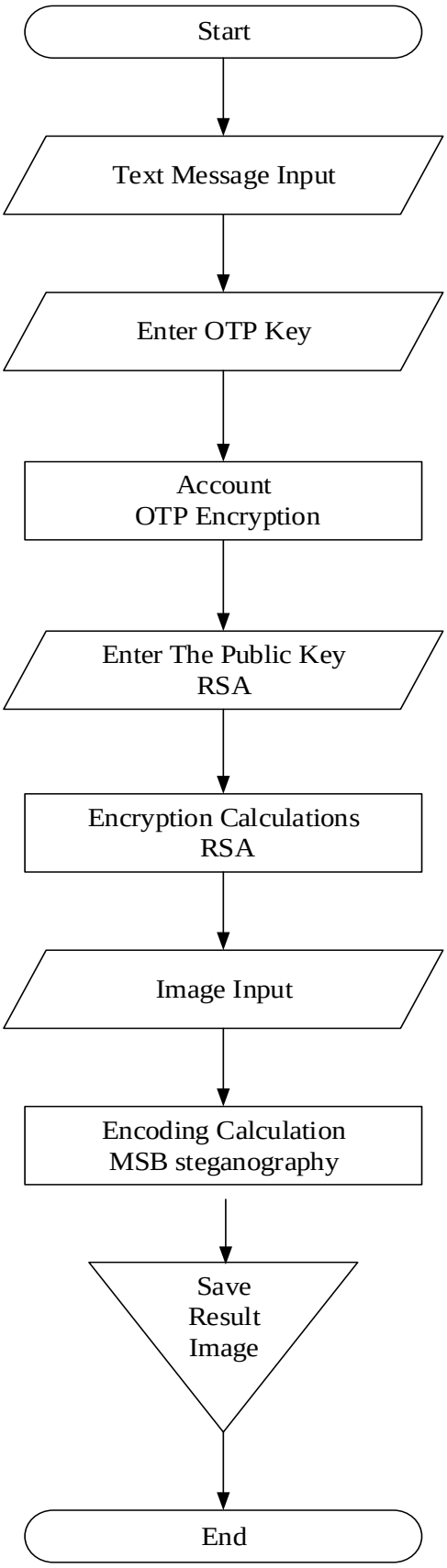

Figure 2. Flowchart Encryption Encoding

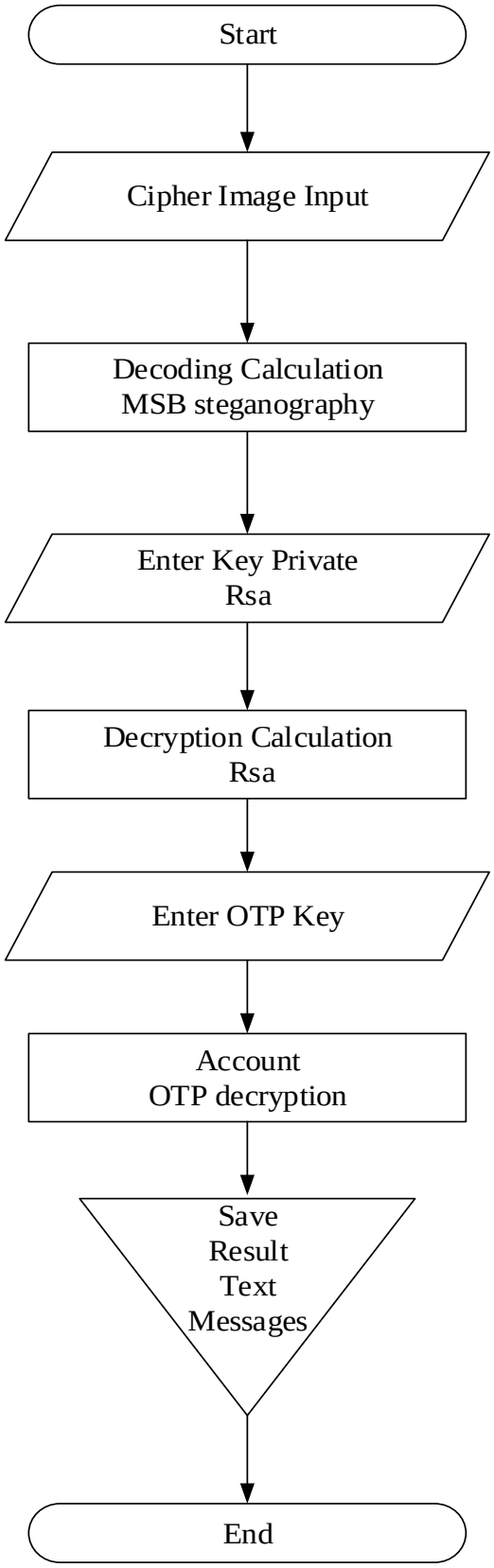

Figure 3. Flowchart Decoding Decryption

RESULTS AND DISCUSSION

Discussion of System Interfaces

The appearance of the image repair system that has been designed using the Visual Basic 2010 programming application, with the application of OTP, RSA and MSB Steganography algorithms in insertion of messages on the image, which 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, generate keys, encryption encoding, decoding decryption and exit. The main page display of the system is as follows:

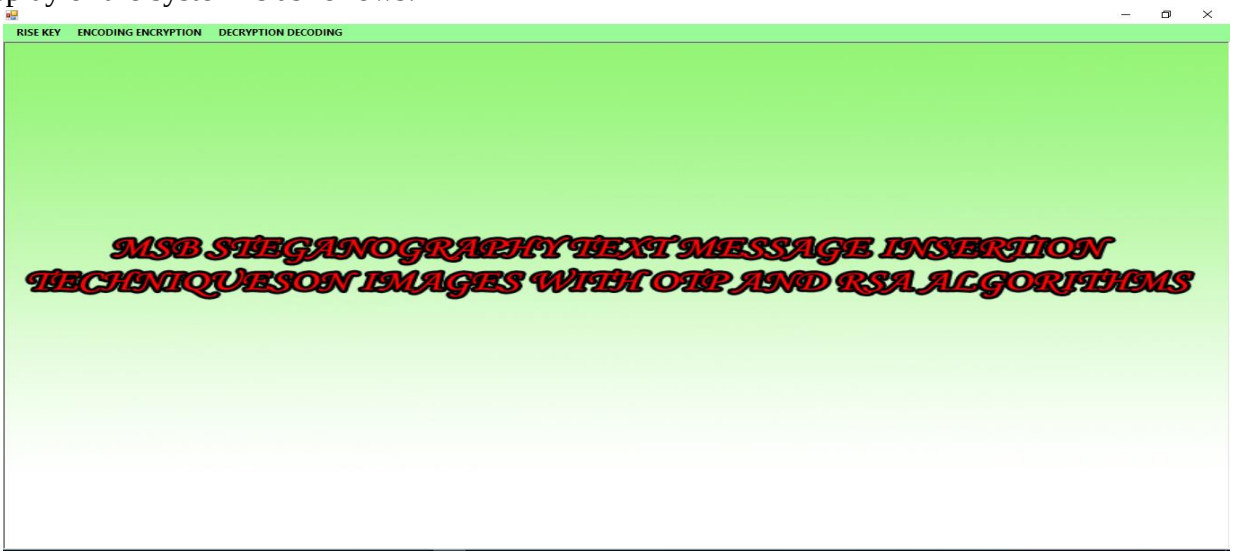

Figure 4. Main Page View

Key Rise Process Page View

In the key rise view displays several lines for the key awakening process, in this view the system user must store a key which later to be used in the encryption or shortening of the message to be secured, the key rise page view is as follows:

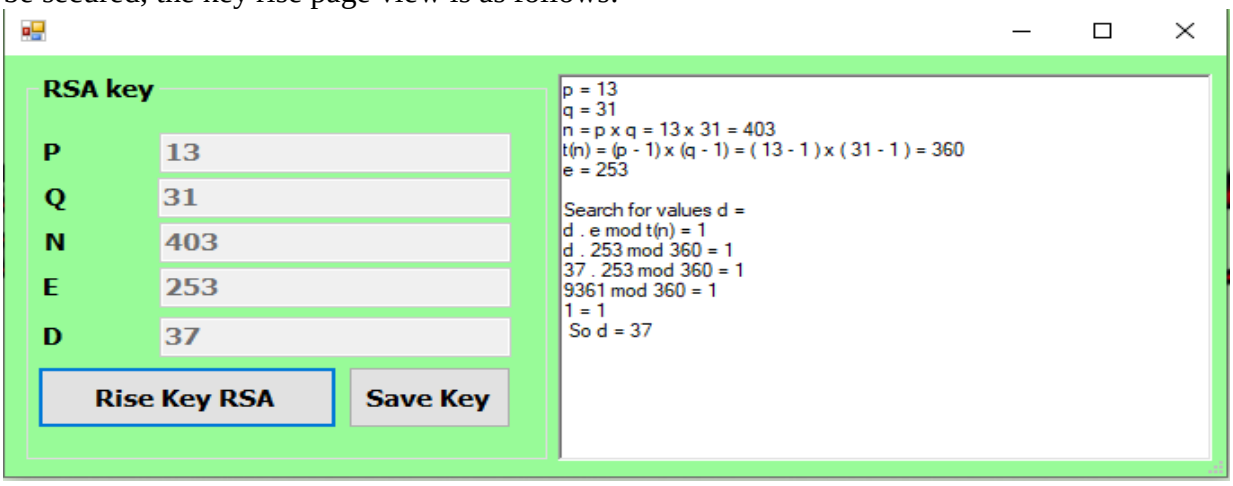

Figure 5. RSA Key Rise Menu Display

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 encryption inserts the message with the OTP algorithm, then the OTP calculation appears. Next, carry out the encryption process of the RSA algorithm to enter the public key, then the RSA calculation appears. Next will input an image that will be selected after that carry out the encoding process where the MSB steganography calculation will appear and the results of the encoding that have been inserted will appear, then it 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:

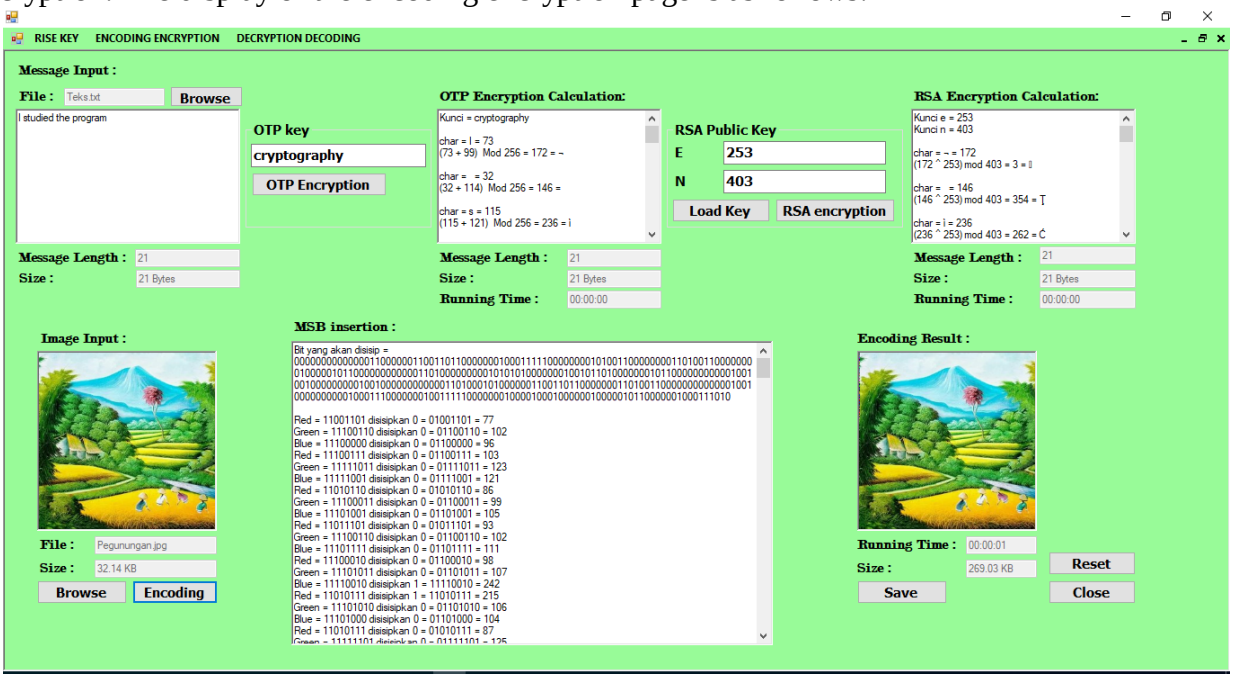

Figure 6. Page View Encoding Encryption

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 MSB steganography decoding calculation, enter the private key to decrypt RSA, the RSA decryption calculation will appear then enter the same key in the OTP algorithm decryption process, then the OTP 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 looks as follows:

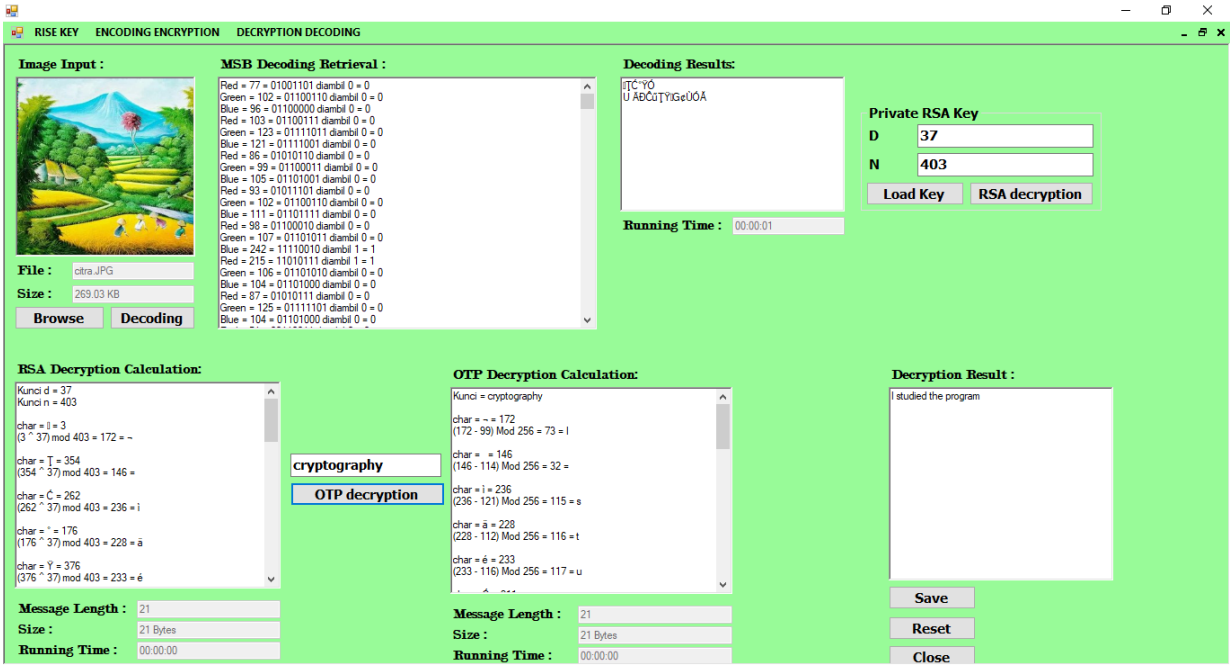

Figure 7. Page View Decoding Decryption

CONCLUSION

1. In insertion of messages into the image is successfully implemented and is able to carry out the process of encoding encryption and decryption decoding more and more of these messages, the time for 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 OTP, RSA and MSB Steganography algorithms, has the same information content as the original message that has been inserted.
2. Insertion of messages on images by using OTP, RSA and MSB Steganography to keep messages private goes well. the message was successfully inserted into the image by means of encryption encoding and decryption decoding processes, experiments carried out on OTP, RSA and MSB Steganography.

REFERENCES

Afandi, I. (2019). *Implementation Of Linear Congruential Generator (Lcg), Most Significant Bit (Msb) Algorithm And Fibonacci Code In Compression And Securing Messages Using Imagery*. Medan: University of North Sumatra.

Brink, J. van den (Pieter J. C. M., Monumentenstichting Baet en Borgh., N. B., Historische Vereniging Tweestromenland., J., & Azanuddin, A. (2014). Mensen van Maas en Waal. *Journal of SAINTIKOM (Journal of Informatics and Computer Management Science)*, *18*(1), 30–34. https://ojs.trigunadharma.ac.id/index.php/jis/article/view/100

Fahlevi, M. R., Ridha, D., Putri, D., & Doni, R. (2020). *Text File Security Techniques Using Cryptography With One Time Pad Cipher Algorithm*. *4*(September), 588–597.

Fauzi, A., Maulita, Y., & Novriyenni. (2017). Designing Message Security Applications Using Elgamal Algorithms By Utilizing One Time Pad Algorithms as Key Generators. *Kaputana Journal of Informatics Engineering (JTIK)*, *1*(1), 1–9.

Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). Implementation of RSA Cryptographic Algorithms for Email Encryption and Decryption. *Journal of Computer Technology and Systems*, *3*(2), 253. https://doi.org/10.14710/jtsiskom.3.2.2015.253-258

Hidayatullah, P. (2017). *Digital Image Management Theory And Real Application.* Bandung: Informatics Bandung.

Ladjamudin, A.-b. B. (2006). *Information System Design Analysis* . Graha

Lutfi, S., & Rosihan, R. (2018). Comparison of Lsb (Least Significant Bit) And Msb (Most Significant Bit) Steganography Methods To Hide Confidential Information Into Digital Images. *JIKO (Journal of Informatics And Computers)*, *1*(1), 34–42. https://doi.org/10.33387/jiko.v1i1.1169

Microsoft, (2021). *File format for saving documents*. Retrieved June 22, 2019, from https://support.office.com/id-id/article/format-file-untuk-menyimpan-dokumen-88de3863-c9e5-4f89-be60-906f9065e43c.

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

Oetomo, B. D. (2006). *Information System Planning & Development.* Yogyakarta: C.V ANDI OFFSET.

Rini, B. (2011). *Microsoft Visual Basic 2010 And Mysql For Point Of Sales Applications.* Wahana Komputer, Yogyakarta.

Sitorus, S. H., Ristian, U., Engineering, J., & Computer, S. (2020). *STEGANOGRAPHY COMPARISON OF LEAST SIGNIFICANT BIT + 3 (LSB + 3) METHOD WITH MOST SIGNIFICANT BIT (MSB)*. *08*(01).

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

Supriyono. (2008). Testing of encryption-decryption systems with the rsa method for document security. *Journal of the College of Nuclear Technology – BATAN*, *2*, 179–194. https://doi.org/10.1111/j.1365-2923.2010.03863.x