http://journal.uir.ac.id/index.php/JGEET

E-ISSN : 2541-5794
P-ISSN : 2503-216X

Journal of Geoscience,
Engineering, Environment, and Technology
Vol 9 No 1 2024

RESEARCH ARTICLE

File security using Advanced Encryption Standard and Least Significant Bit

Felicia Lykke*[1], Andreas Edvard, Feri Saputra[1]

[1] *Department of Computer Science and Engineering, University of Gothenburg Göteborg, Sweden*

* Corresponding author : GirishAnd@gmail.com
Tel.:+91-12-226-9887
Received: Jun 16, 2023; Accepted: Mar 7, 2024.
DOI: 10.25299/jgeet.2024.9.1.19194

Abstract

Computer technology of rapid development has triggered crimes that take advantage of weaknesses in computer systems. One form of crime was the act of hackers who take data and information through computer security holes. The data was used for various things that are not appropriate. Information sent via communication media can be taken and misused by irresponsible parties. An electronic data security system has been developed. With the emergence of various data security methods such as encryption and steganography. Encryption was a way of securing data files by randomizing a document, while Steganography was securing electronic data by hiding a file within another file. Based on the feasibility test of the system with a questionnaire by 20 respondents, the result of 87%, which is categorized as "very good".

Keywords: Encryption, Cryptography, Steganography.

1. Introduction

1.1 Background of the Problem

The development of information and communication technology is currently very rapid. This is marked by the use of computer technology at all levels of society. The rapid development of computer technology has triggered crimes that take advantage of weaknesses in computer systems. One form of crime is the act of hackers who take data and information through computer security holes. The data is used for various things that are not appropriate. Information sent via communication media can be taken and misused by irresponsible parties.

In this case, of course, the use of technology to transmit information becomes vulnerable for some parties. Such as sending company documents, sending government documents, and even sending documents that personal privacy will feel disturbed.

An electronic data security system has been developed. With the emergence of various data security methods such as encryption and steganography. Encryption is a way of securing data files by randomizing a document and it can only be rearranged using a password or password that has been previously set. Meanwhile, steganography is securing electronic data by hiding a file within another file.

Therefore, in this study, the authors are interested in building a system that can encrypt data while hiding data and information in video files, thus data and information sent via electronic media can be guaranteed security.

2. Library Studies

Muhamad Fitra Syawal in TICOM Journal Vol.4 No.3 May 2016 researched the Implementation of Steganography Techniques Using the Vigenere Cipher Algorithm and the LSB Method. This research was made using a web programming language. In this research, the object of research is to enter text into images to produce files that are hidden and cannot be accessed by unauthorized parties..

Jhoni Verlando Purba has conducted research entitled Implementation of Steganography of Text Messages Into Sound Files (.Wav) By Modifying Byte Spacing in the Least Significant Bit (LSB) Algorithm in 2017. The purpose of this research is to hide files with the extension .txt in files with the extension. Wav. This study used web programming language.

Tri Prasetyo Utomo has conducted research and published his research results in a journal entitled Image Steganography Using the Least Significant Bit Method for Communication Protection in Online Media. In this journal, a message is inserted in an image file thus it can be extracted back into a message. This method is done to secure the message and prevent unauthorized parties from taking advantage of the message.

The research conducted by Tri Prasetyo Utomo, Jhoni Verlando Purba, and Muhamad Fitra and the research conducted by the authors both secure data by hiding the data in other data. The difference lies in the object under study, the research method, and the programming language used in developing the system.

Python (programming language) is a high-level programming language that can execute several multi-purpose instructions directly (interpretatively) with the Object Oriented Programming method and also uses dynamic semantics to provide a level of syntax readability. As a high-level programming language, python can be learned easily because it is equipped with automatic memory management.

Steganography and the Advanced Encryption Standard (AES) method, this steganographic technique has existed since 4000 years ago in the city of Menet Khufu, Egypt. Initially, it was the use of hieroglyphics, namely writing using characters in the form of pictures. Scribes used this

ancient Egyptian writing to narrate the life of their master. These ancient Egyptian writings became the idea for creating secret messages today.

Cryptography and the Least Significant Bit Method, Cryptography (cryptography) comes from the Greek, namely cryptos which mean secret (secret), while graphien means writing (writing). The originally the language of cryptography means secret writing (secret writing). Cryptography has several definitions. One definition of cryptography is the study of mathematical techniques related to aspects of information security such as data confidentiality, data validity, data integrity, and data authentication.

Tools in system analysis and planning are divided into: Data Flow Diagrams (DFD) are diagrams used to describe the flow of data in the system. DFD is often used to describe an existing system or a new system that will be logically developed without considering the physical environment where the data flows (eg by telephone, mail, and so on) or the physical environment where the data will be stored. DFD is a tool used in structured system development methodology (structured analysis and design). An activity Diagram is a diagram that is used to describe the activities that occur within a system. Flowcharts are job symbols that designate a flowchart of connected processes. Thus, each symbol defined by the American National Standards Institute Inc. Flowcharts is used to simplify programming. By using a flowchart, programming logic is easier to understand and analyze, thus you can determine the appropriate programming codes for the job.

3. Research Method

This research methodology consisted of 6 stages including data collecting, literature study, system planning, system implementation, testing and evaluation, preparation of research reports.

3.1 Analysis Use Case Diagram

Broadly speaking, on the system that will be developed, the user inputs the files to be secured. Then the user will receive a file in the form of a result file that has been secured. To parse it again, the user simply inputs the file to be parsed, the system will process it automatically and the user receives the decomposed file.

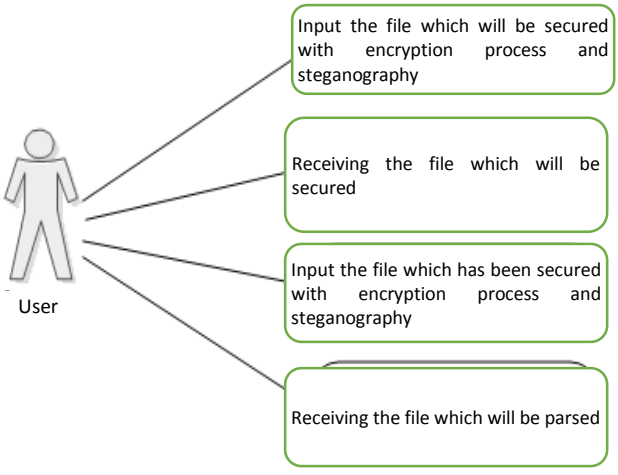

Fig 1. Use Case Diagram

3.2 Diagram Context

Context Diagram outlines the flow of data that runs within the system. In the context of the diagram, it is illustrated that there is one type of user in the system. Users can access system features in the form of a process of securing files with cryptography and steganography. Users can also access the menu to decompose the secured file into its original form.

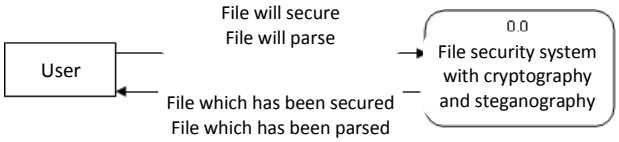

Fig 2. Diagram Context of the system being developed

3.3 Hierarchy Chart

Hierarchy chart can be seen that in the system to be built, there are 5 level 0 processes. The DFD level 0 process consists of input object files, input target files, security results, input decomposition files, and decomposition results.

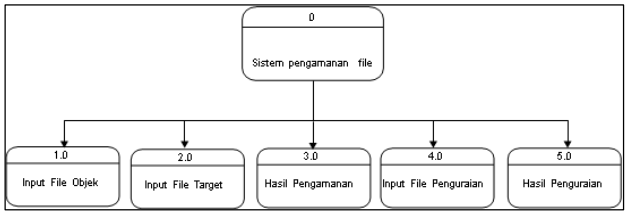

Fig 3. System Hierarchy Chart under Development

3.4 Input Design

display design File security data input. In this design, there are fields needed to complete the data. The type of input provided by the system has been adjusted to the data requirements in that field.

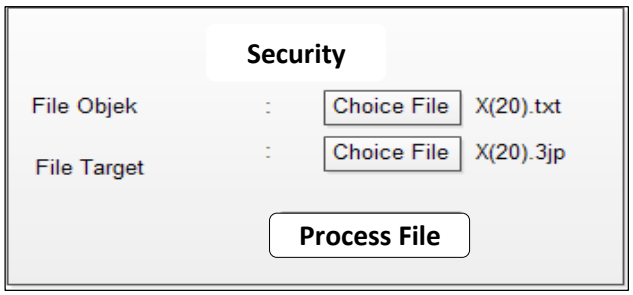

Fig 4. File Safeguard Input Design

file parsing data input display design. In this design there are fields needed to complete the data. The type of input provided by the system has been adjusted to the data requirements in that field.

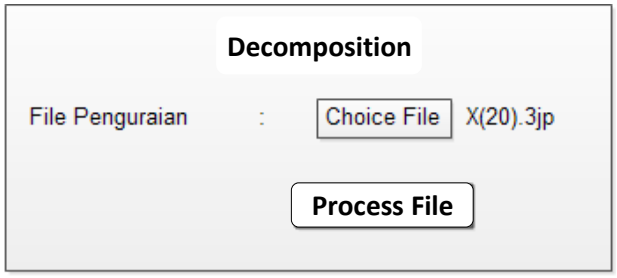

Fig 5. File Parsing Input Plan

3.5 Output Design

file security result display design. The security result file has been hidden in the target file. Then the user can save the file to the drive.

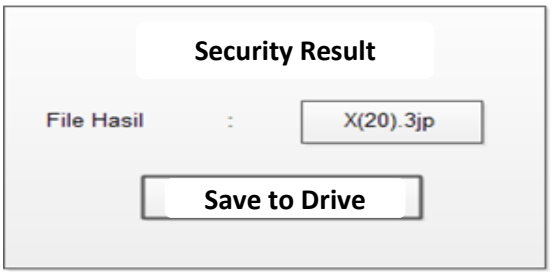

Fig 6. File Safeguard output Design

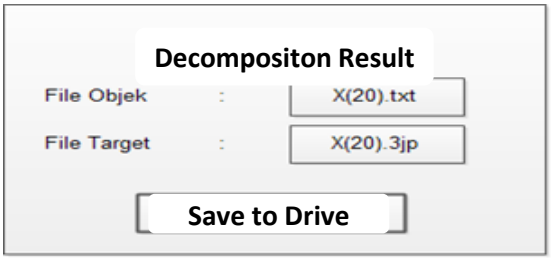

Fig 7. File Decomposition Output Plan

file parsing results display design. Files hidden in the target file have been parsed into their original form.

4. Results and Discussion

4.1 Black Box Encryption From Testing

Black box testing is a software testing method that focuses on the functionality side, especially on application input and output.

Based on the tests that have been carried out, it can be concluded that the black box testing that has been carried out on the system on the encryption form has met expectations.

4.2 Black Box Form Description Testing

Based on the tests that have been carried out, it can be concluded that the black box testing that has been carried out on the system in the description form has met expectations.

4.3 Conclusion of Black Box Testing

the form of the File Security Application Using the Advanced Encryption Standard and the Least Significant Bit has been running as expected or can be said to be 100% running according to its function. time required for system implementation.

Table 1. Black Box Form Encryption Testing

No.	Tested Component	Examiner Scenario	The Expected Result	Result
1.	Button Choose Object File	Pressing the button of choose object file	The system will display a new dialogue box to choose the desired file	[✓]As Expected [ ] Not As Expected
2.	Button Choose Target File	Pressing the button of choose target file	The system will display the new dialogue box to choose the desired file	[✓]As Expected [ ] Not As Expected
3.	Encription Button	Pressing encription button	The system will emerge a dialogue box for filling in the keyword	[✓]As Expected [ ] Not As Expected
4	Encription Process	Filling in keywords	The sistem will process the encription then stegano. Emerging notification the result of encription in stegano folder	[✓]As Expected [ ] Not As Expected

4.5 System Implementation

Implementation of the system used is to make a questionnaire with 5 (five) questions and 20 correspondents which are addressed to individuals who are considered intellectuals. The 20 correspondents were asked questions related to the performance of the application. The five questions in question are as follows:

1. Is the information displayed easily understood by the user?
2. What do you think about the appearance of this application?
3. Is the language used in this application easy to understand?
4. Is the application easy enough to use (operate)?
5. In your opinion, is this application worthy of publication?

From the questions above, the results of answers or responses can be concluded from the following results:

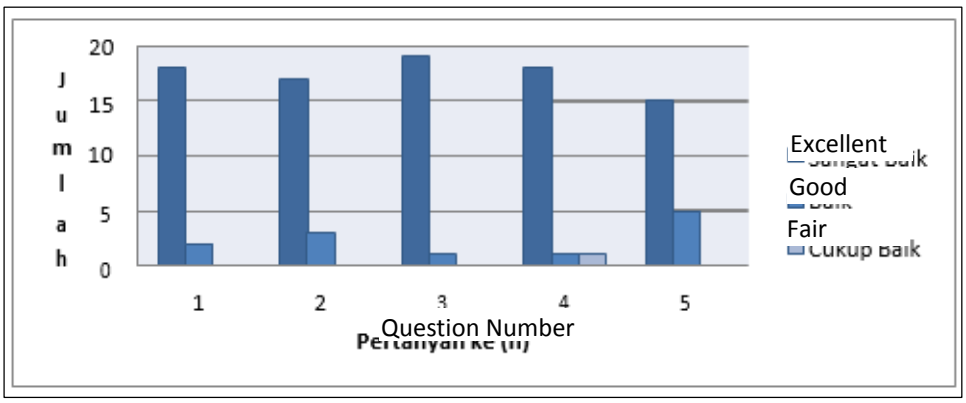

Fig 8. Questionnaire Results Graph

4.6 Conclusion of Questionnaire Testing

Based on the results of the questionnaire, it can be concluded that the data security system using cryptography and steganography with the Advanced Encryption Standard and Least Significant Bit Steganography methods has the following percentages:

Table 2. Result Percentage Value of Each Question Questionnaire

No	Question	Number of Correspondents' Percentage		
		Excellent	Good	Fair
1	Is the information displayed easy to be understood by the user?	90%	10%	0%
2	How is your opinion about the display of this application?	85%	15%	0%
3	Is the language used in this application easy to understand?	95%	5%	0%
4	Is the application quite easy to be used (operated)?	90%	5%	5%
5	According to you is the application feasible to be published?	75%	25%	0%

Based on the percentage results in Table 2. above, the data security system using cryptography and steganography with the Advanced Encryption Standard and Least Significant Bit Steganography methods is as expected, because the system built has good performance, Performance is the performance or achievement value of the system built, with a questionnaire percentage value stating Very Good an average of 87%, thus the application can be implemented.

5. Conclusions and Suggestions

5.1 Conclusion

After conducting research, designing and testing data security systems using cryptography and steganography with the Advanced Encryption Standard and Least Significant Bit Steganography methods, the following conclusions can be drawn:

1. Has succeeded in creating a data security system using cryptography and steganography with the Advanced Encryption Standard and Least Significant Bit Steganography methods.
2. Based on the results of tests that have been carried out using the Black box, the data security system using cryptography and steganography with the Advanced Encryption Standard and Least Significant Bit Steganography methods is following what is expected.
3. Based on the results of system testing carried out using the questionnaire method.

5. 2 Suggestion

Based on the results of the research, several suggestions should be made for the development of this system to be better, including the following:

1. In further system development, a data security system using cryptography and steganography with the Advanced Encryption Standard and Least Significant Bit Steganography methods can be developed using the Android programming language thus it can be more easily used on smartphone devices.
2. In further system development, a data security system using cryptography and steganography with the Advanced Encryption Standard and Least Significant Bit Steganography methods can be implemented using algorithms other than AES and LSB.
3. In further system development, a data security system using cryptography and steganography with the Advanced Encryption Standard and Least Significant Bit Steganography methods can use the Ms object file. Office (Ms. Word, Ms. Power Point, Ms. Excel) hidden in video files.

References

Andri Kristanto. 2017. *Perancangan Sistem Informasi dan Aplikasinya,* Gava Media, Yogyakarta.

A. Sadikin, Rifki., 2012, *Kriptografi untuk Keamanan Jaringan*. Yogyakarta.

Bonnie, Soeherman. 2016. *Designing Information System Concept & Cases with Visio,* PT Elex Media Komputindo, Jakarta.

Fitra, Muhammad, Syawal, dkk., 2016, *Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Chiper Dan Metode LSB,* Vol.4 No.3.

John Mc. Manama. 2014. *Design dan Perencanaan SistemInformasi,* Luxima, Jakarta.

Murdick, Robert, G, dan Joel, Ross, E., 2015, *Sistem Informasi untuk Manajemen Modern*, Erlangga, Jakarta.

Prayudi, Yudi dan Halik, Idham. 2005. *Studi dan Analisis Algoritma Rivest Code 6 Dalam Enkripsi/Dekripsi Data*. ISBN = 979-756-061-6.

Prasetyo , Tri, Utomo., 2012, *Steganografi Gambar dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media Online.*

Purba, Jhoni Verlando., Marihat, Situmorang, & Dedy, Arisandi. 2012. *Implementasi Steganografi Pesan Text ke Dalam File Sound (.Wav) dengan Modifikasi Jarak Byte pada Algoritma Least Significant Bit (LSB).*

Sutabri, Tata., 2012, *Konsep Dasar Informasi*. Andi, Yogyakarta,