Jurnal Mandiri IT
Vol. 11 No. 4, April (2023), pp. 138-146

ISSN 2301-8984 (Print)

Face recognition system with vigenere cipher cryptography for document security

Sukri[1], Luluk Elvitaria[2], Wandiah Ayu Barus[3]
[1,2,3] Teknik Informatika, Universitas Abdurrab, Pekanbaru, Indonesia

A R T I C L E I N F O

Article history:

Received March 31, 2023
Revised April 28, 2023
Accepted April 30, 2023

Keywords:

Cryptography
Document
Information
System
vigenere cipher

ABSTRACT

The issue of data security and confidentiality is one of the most important aspects of an information delivery system. In this case, it is closely related to how important it is that the information be sent and received by interested parties. Information will no longer be useful if, in the middle of the delivery process, the information is intercepted or hijacked by unauthorized people. Computer security is something that is very important in this information age, especially for an organization or company. Data confidentiality The computer security problem is very important in this information age, especially for an organization or company because documents are some of the most important data for the continuity of the company's operations. The branch of science that studies ways to secure data is known as "cryptography." The Vigenère-Chiper algorithm is one of the cryptographic methods for encoding text. This study aims to create a cryptographic application that can encode text and send encrypted text over a network based on the Vigenère Chiper algorithm. This application performs cryptography on text in the form of letters, numbers, and symbols. The key used is alphanumeric, which is a combination of letters, numbers, and symbols. The results of this study are in the form of an application that can send encrypted text messages through a local area network (LAN) so that the confidentiality of the message can be maintained.

Corresponding Author:

Sukri,
Teknik Informatika,
Universitas Abdurrab,
Jl. Riau Ujung No. 73, Pekanbaru, 28291, Indonesia
Email: sukri@univrab.ac.id

1. INTRODUCTION

Every job and office activity, whether in government or private sector, requires data and information (Chetty et al. 2020)(Rahel and Ruru; Joyce, Jacinta, Rares 2022). One of the essential sources of information that an office must have is documents (Darwis et al. 2022). Documents are evidence and records of activities ranging from service activities to decision-making activities (Hasrul; Amriadi; Nur 2022). Document management can be done manually or using a computer to transform them into information that can be used as a basis for decision-making (Dharmawan, Prihati, and Simamora 2022). Proper document arrangement and security will facilitate the retrieval of important documents and prevent them from falling into the hands of irresponsible individuals. This way, when documents are needed for decision-making, the archive can be quickly found and confidentiality can be maintained.

Security is a form of action to protect something from various types of disturbances and threats Aspects related to security in the world of computers include privacy/confidentiality, which is an effort to protect information from unauthorized access (ensuring that personal data remains private), integrity, which is an effort to ensure that data or systems are not changed by unauthorized individuals, authentication, which is an effort or method to determine the authenticity of the information sent and opened by the correct person (original)(Sukri, Sukri; Jumiati 2017). Availability is related to the availability of systems and data (information) when needed (Sari and Sukri 2018).

The field of study that deals with methods of data security is known as Cryptography (Widodo and Purnomo 2020). *The Vigenere Cipher algorithm is one of the cryptography methods used for text encoding* (Alam, Habibi, and Widya 2022). This study aims to develop a cryptography application that can encode text and transmit the encrypted text over a network based on the Vigenere Cipher algorithm. This application performs cryptography on text containing letters, numbers, and symbols. The key used is an alphanumeric combination of letters, numbers, and symbols (Sutopo 2023). The result of this research is an application that can transmit encrypted text messages over a Local Area Network (LAN) network, ensuring the confidentiality and security of the message.

Security and confidentiality of data are important aspects in an information transmission system. It is closely related to how important the information is to be sent and received by the interested parties. The information will be useless if in the middle of the transmission process, it is intercepted or hacked by unauthorized individuals (Arfandy, Simanjuntak, and Pasaribu 2022). Computer security is something very important in this era of information, especially for an organization or company. Data confidentiality is a crucial issue in computer security because documents are one of the most important data in the continuity of the company's operation.

Vigenere Cipher is a method of encrypting alphabetic text using a series of Caesar ciphers based on the letters of a keyword (Hidayah, Mulyana, and Bachtiar 2023). Vigenere Cipher belongs to the class of polyalphabetic substitution ciphers.

Cryptography, in general, is the science and art of keeping messages confidential (Nurcahya 2022). In addition to that definition, there is also the definition of a science that teaches mathematical techniques related to information security aspects such as data confidentiality, data authenticity, data integrity, and data authentication (Jamaludin et al. 2022).

Vigenere cipher belongs to the classical symmetric key cryptography type (Aripin and Syahrizal 2022). Vigenere cipher is a type of polyalphabetic substitution cipher, which means a character in plaintext is not always substituted into the same character, but is substituted based on the key used (Ginting 2020). The strength of this algorithm is its ability to avoid the frequency of characters in the ciphertext having similar patterns, as is the case with the single-alphabet cipher. The polyalphabetic nature of the Vigenere cipher is implemented with the Vigenere square (Simangunsong 2018).

A square table of the Vigenere cipher. This table contains letters of the alphabet written in 26 rows and columns (matrix 26). Tables are used to simplify the process of encrypting and decrypting text messages (Imam Riadi, Abdul Fadlil, and Fahmi Auliya Tsani 2022). The leftmost column represents the key character, the top row in the table indicates the plaintext character, and each row and column in the square represents the ciphertext character which is done using the Caesar cipher technique where the displacement of plaintext characters is determined by the key character..

The encryption process using a Vigenere square is done by dragging a line vertically down from the plaintext character, then dragging a line horizontally to the right of the key character. The point of intersection of the two lines shows the ciphertext character of the plaintext character concerned. The decryption process is carried out in reverse from the encryption process, first draw a line horizontally to the right from the key character used to the intended ciphertext character, then draw a line vertically upwards from the ciphertext character to the top line, the character on the top line represents plaintext.

Each line in the square represents the ciphertert letters obtained with the Caesar cipher, in which the number of plain text letter shifts is determined by the numeric value of the key letter (a=0, b=1, c=2, …, z=25). For example, the key letter c (=2) states that the plaintext letters are shifted 2 letters to the right (from the alphabetical order), so that the ciphertext letters are in line c.

The vigenere square is used to obtain a ciphertert using a predetermined key. If the key length is shorter than the plain text length, then the key is repeated (periodic system), then the key length is up to m.

The general description of the application is that it is a solution to the problem of security and confidentiality of documents designed in an application for transmitting facial detection information for document security. In this case, the faces detected by this application are the faces of employees at the company. Face detection or facial recognition for document security using the Vigenere cipher cryptographic algorithm is a user who wants to save documents first performs a face scan on the menu available in the application. Before the process is carried out, the document storage process fails to be carried out. This is closely related to how important it is that information is sent and received by interested people only. Information will be useless if in the middle of the delivery process, the information is intercepted or hijacked by unauthorized persons (Arfandy, Simanjuntak, and Pasaribu 2022).

2. RESEARCH METHOD

To get the maximum research results, a clear framework is needed. This framework is the steps that will be taken in solving the problem. The framework used can be seen in Figure 1.

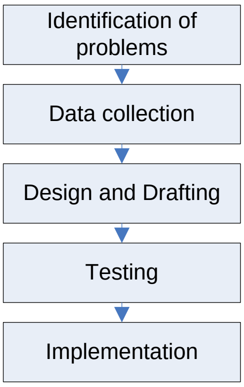

Figure 1. Research framework

2.1 Identification of problems

In this stage the author makes observations and records regarding the problems faced by the company for document security. The author visits directly at the research location to find obstacles and look for ideas and the right solutions. This stage is an important stage because without identifying the problem, researchers will find it difficult to conduct research at a later stage. The research tools and materials are in the form of hardware and software.

a. *Hardware*
In designing this system, hardware (hardware) is needed to run the software used in system design. The supporting hardware used is a computer/laptop, LCD, keyboard, printer, and keyboard

b. *Software*
In this design is used as a tool in designing and designing the program. Below is the supporting software in system design, namely Windows 8, DBMS MySQL, C# (Visual Studio Code), PDF (Portable Document Format), Microsoft Word, and Microsoft Visio.

2.2 Data Collection

One important component in research is the process of researchers in data collection. Errors made in the data collection process will make the analysis process difficult. In addition, the results and conclusions that will be obtained will be ambiguous if the data collection is not carried out correctly, therefore the authors arrange activities in the data collection process starting from literature studies, observations and documentation.

a. Literature review

At this stage the author carries out a series of activities related to methods of collecting library data, reading and taking notes, as well as managing research materials, looking for theoretical references that are relevant to cases or problems found either from the library or from the internet.

In the research object, the authors look for constraints on the running system, security issues and data confidentiality are one of the important aspects of an information system. In this case, it is closely related to how important the information is sent and received by the people concerned. Information will be useless if in the middle of the delivery process, the information is intercepted or hijacked by unauthorized persons. Computer security is very important in this information age, especially for an organization or company. Data confidentiality Computer security issues are very important in this information age, especially for an organization or company because documents are one of the most important data in the continuity of the company.

b. *Observation*

The data collection method is carried out by directly observing an event that is happening. Direct observations were made at the Company for Document Security regarding matters related to the research being carried out such as observing the work system at that place.

2.3 Design and Drafting

After the data collection stage has been completed, the author already knows clearly what must be done by thinking about how to form the system starting from drawing, planning and sketching so that it becomes a unified whole and functions.

2.4 Testing

In this stage, the modules that have been made and tested are developed. Testing is carried out to see the compatibility between the software and the design that has been made, and to see whether there are still errors or not, so that the system can still be repaired before being refined. In testing, the validation of the interface will also be seen, indicated by an "ok" statement.

2.5 Implementation

This is the stage where the document security system that has been built by the author will be implemented as a document security system container using the Vigenere Chiper Cryptographic Algorithm for employees of a company.

3. RESULTS AND DISCUSSIONS

3.1 Problem Identification Stage

This stage is one of the steps of research work which is arguably the most important among the others, because it will determine the quality of the research. In this study, identification of employee document security problems by managing documents manually or using a computer that is useful for employees is an application that contains employee facial recognition information that can be used as a basis for decision making. then the author wants to design an information system that is useful as a good and correct arrangement and security of documents which will facilitate retrieval and keep important documents from falling into the hands of irresponsible people, so that when documents are needed in decision making, these archives can be immediately discovered and kept confidential. Document security is designed in the form of action, namely by way of facial recognition using the vigenere cipher cryptographic algorithm.

3.1.1 Flowchart

At this stage is the creation of a flowchart of the system from the facial recognition application for document security after completion of the design and planning stages. Analyze the needs and systems that will be used in the process of making facial recognition applications for document security in detail, but it can also provide an overview of what information can be generated by the designed system.

3.1.2 Use Case Diagram System

There is 1 access user who wants to do security on the file. Can be seen in figure 2.

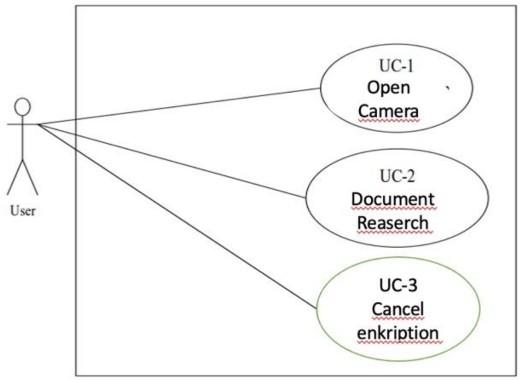

Figure 2. Use case diagram

3.1.3 *Activity Diagram*

An activity chart is a visual form of a workflow containing activities and actions, which can also contain choices and loops. The Encryption Activity activity diagram describes the workflow in an outline of the functions and actions contained on the Encryption Activity page.

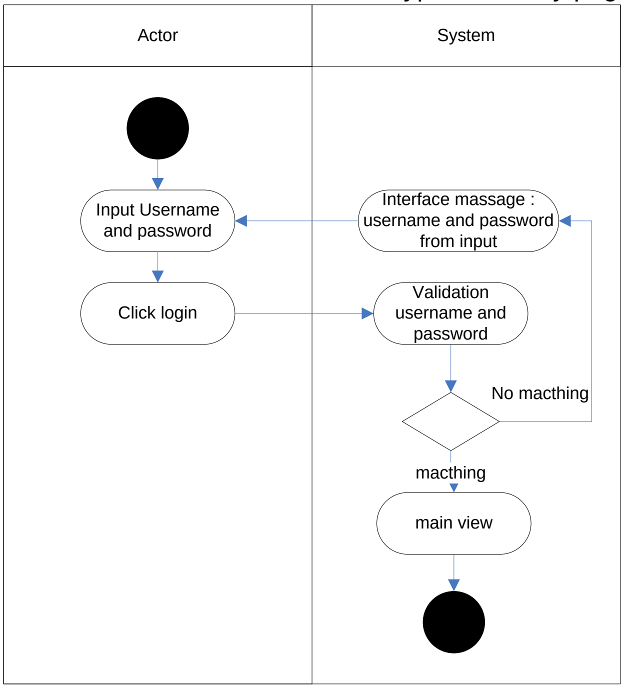

Figure 3. Activity login diagram

3.2 Data Collection Stage

At this stage the authors search for theoretical foundations that are relevant to the problems and research objectives supported by a literature study. Can be searched from journals, books, theses, and the internet. The output of this literature study is the collection of references that are relevant to the formulation of the problem. The aim is to strengthen problem analysis as well as a theoretical basis for conducting research in designing document security information systems for company employees.

3.3 Design and Design Stages

This stage is the design and design of the information system described in the form of tables, menus, inputs, outputs that exist in the system later. So that a system design is produced that will be used as the basis for making a system at the implementation stage.

3.3.1 Table Design

This section is an activity that designs tables from the Face recognition system with vigenere cipher cryptography for document security.

a. Table Admin

Table 1. Table Admin

Field	Type	Information
id_admin	varchar(50)	id_admin
Name	varchar(50)	Neme
username	varchar(50)	username
password	varchar(100)	password

b. Document Type

Table 2. Table document type

Field	Type	Information
id_Type	Int (11)	id_Type
Documen Type	Varchar (50)	Document Type

c. Employee

Table 3. Table employee data

Field	Type	Keterangan
id_employee	varchar(50)	id_karyawan
name	varchar(50)	Name employe
address	varchar(50)	alamat
no_phone	varchar(50)	Phone number
username	varchar(50)	username
password	varchar(100)	password

3.3.2 User Interface Design

In Designing a Face Recognition Application for Document Security Using the Vigenere Chiper Cryptographic Algorithm, the author collects application designs such as facial recognition applications and collects existing employee data, coding the design of this application using the Visual Studio Code application and other supporting applications.

3.4 Testing Stages

This test is carried out with respect to finding errors that result from unexpected interactions. Such as the process of importing data, changing, and deleting data by entering sample data from the user.

3.4.1 Interface Testing

Table 4. Testing of the face recognition system

No.	Pengujian	Interfacae yang diharapkan	Hasil Uji
1	*Interface*Login	Face Recognition admin login page	OK
2.	*Application initial interface*	Application start page	OK
3.	*The interface displays facial recognition admin data*	The page displays facial recognition admin data	OK

4.	*The interface displays data Document type Face Recognition*	Face Recognition document type page	OK
5.	*The interface displays Face Recognition employee data*	Introductory employee data page New face	OK

3.5 Implementation Stage

This section will discuss the results and creation of a Face Recognition Application for Document Security Using the Vigenere Chiper Cryptographic Algorithm which will contain several application views and features.

a. Login Page

Admin login is a page for admins to enter the system and have access rights to the system by entering a username and password.

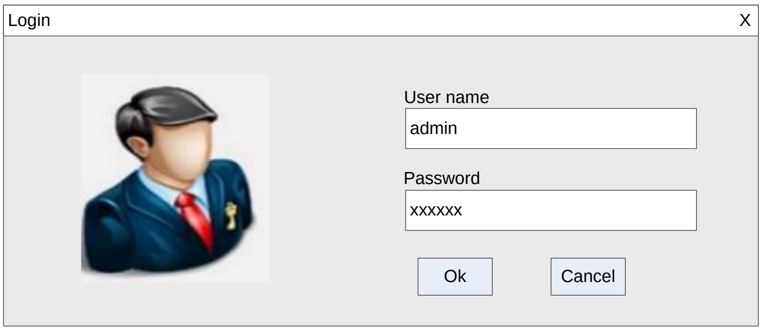

Figure 4. Login display

b. System Main Page

The start page of the Face Recognition Application for Document Security Using the Vigenere Chiper Cryptographic Algorithm which is the initial information of the application.

Figure 5. Main page

c. Admin Page

The admin data display page is the admin data information page for the Face Recognition Application for Document Security Using the Vigenere Chiper Cryptographic Algorithm.

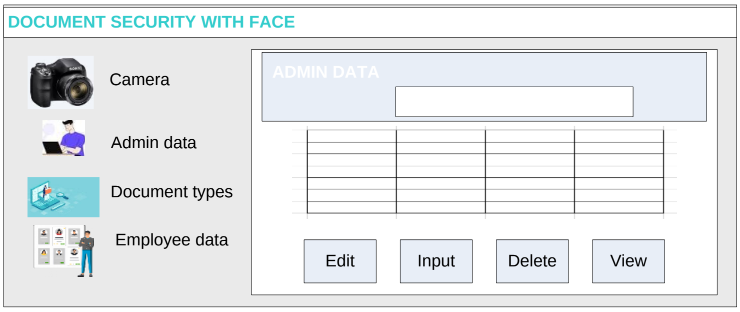

Figure 6. Admin page

d. Document Type Page

The data display page for document types is an information page for data types of admin and employee documents. Facial Recognition Application for Document Security Uses the Vigenere Chiper Cryptographic Algorithm.

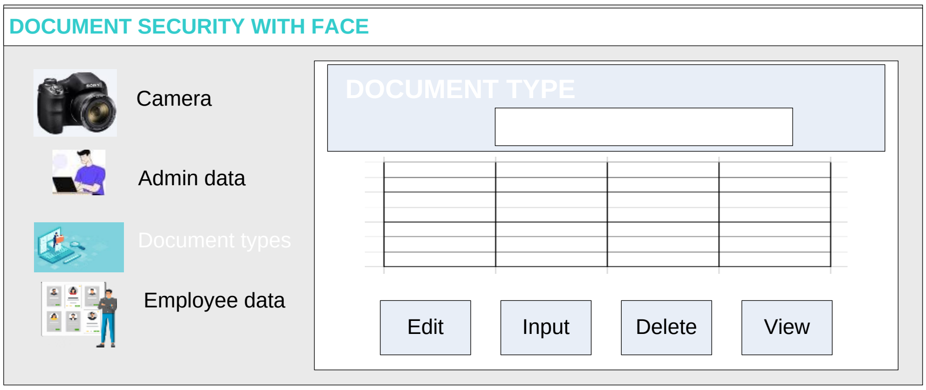

Figure 7. Document type page

e. Employee data page

The employee data display page is the employee data information page. Facial Recognition Application for Document Security Using the Vigenere Chiper Cryptographic Algorithm.

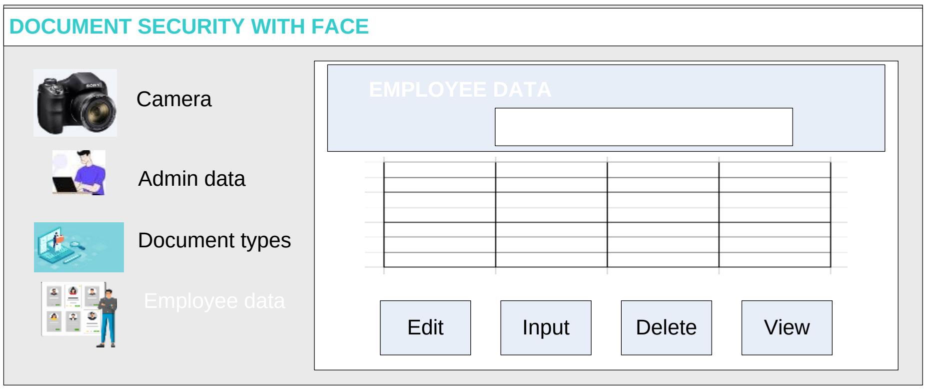

Figure 8. Employee Page

4. CONCLUSION

From all the research conducted in the previous chapters, the authors draw conclusions about Designing Face Recognition Applications for Document Security Using the Vigenere Chiper Cryptographic Algorithm as a means of information. face safety. This research produces a Face Recognition Application for Document Security Using the Vigenere Chiper Cryptographic Algorithm with Admin processing features. This application can help the Admin in securing important documents.

REFERENCES

Alam, H, A K Habibi, and H Widya. 2022. “Penggunaan Algoritma Vigenere Cipher Dan One Time Pad Untuk Keamanan Pesan Teks.” *Seminar Nasional Teknik ….*

Arfandy, Dicky, Magdalena Simanjuntak, and Tio Pasaribu. 2022. “Penerapan Metode Vigenere Cipher Untuk Mengamankan Data Text.” *Jurnal Teknik Informatika Kaputama (JTIK) Vol.6,* 6(1): 448–56.

Aripin, Soeb, and Muhammad Syahrizal. 2022. “Analisis Modifikasi Algoritma Kriptografi Klasik Menggunakan Algoritma Blum-Micali Generator.” *Jurnal Sains Komputer & Informatika (J-SAKTI* 6(1): 136–47.

Chetty, Raj, John N Friedman, Nathaniel Hendren, and Michael Stepner. 2020. *The Economic Impacts of COVID-19: Evidence from a New Public Database Built Using Private Sector Data*. national Bureau of economic research.

Darwis, Dedi et al. 2022. “Pelatihan Pengarsipan Secara Elektronik (E-Filling) Bagi Perangkat Desa Di Pekon Sukanegeri Jaya.” *Journal of Social Sciences and Technology for Community Service (JSSTCS)* 3(1): 108.

Dharmawan, Alexander, Yani Prihati, and Putri Maria Simamora. 2022. “Sistem Informasi Administrasi Persuratan Pada Kantor Kecamatan Semarang Tengah.” *Jurnal Elektro Luceat* 8(2).

Ginting, Victor Saputra. 2020. “Penerapan Algoritma Vigenere Cipher Dan Hill Cipher Menggunakan Satuan Massa.” *Jurnal Teknologi Informasi* 4(2): 241–46.

Hasrul; Amriadi; Nur, Fadillah Suprayitno. 2022. “Perancangan Sistem Informasi Pengarsipan Surat Pada Kantor Kejaksaan Kabupaten Mamuju Utara.” *Jumistik* 1(1): 31.

Hidayah, Vara Maulidyah, Dadang Iskandar Mulyana, and Yuliana Bachtiar. 2023. “Algoritma Caesar Cipher Atau Vigenere Cipher Pada Pengenkripsian Pesan Teks.” 05(03): 8563–73.

Imam Riadi, Abdul Fadlil, and Fahmi Auliya Tsani. 2022. “Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher.” *JISKA (Jurnal Informatika Sunan Kalijaga)* 7(1): 33–45.

Jamaludin, Jamaludin et al. 2022. *Kriptografi: Teknik Keamanan Data*. Yayasan Kita Menulis.

Nurcahya, Saputra Dwi. 2022. “Implementasi Aplikasi Kriptografi Metode Kode Geser Berbasis Java.” *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)* 5(4): 694–97.

Rahel, Tumewu, and Joorie Ruru; Joyce, Jacinta, Rares. 2022. “Sistem Informasi Manajemen Dalam Pelayanan Publik Di Kantor Catatan Sipil Kota Tomohon.” *jurnal administrasi publik* VIII(118): 72–79.

Sari, Ira Puspita, and Sukri Sukri. 2018. “Analisis Penerapan Metode Antrian Hirarchical Token Bucket Untuk Management Bandwidth Jaringan Internet.” *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)* 2(2): 522–29.

Simangunsong, J. 2018. “Modifikasi Algoritma Vigenere Cipher Untuk Pengamanan Pesan Rahasia.” *… Informasi Neumann (Pitin)*: 23–27.

Sukri, Sukri; Jumiati, Jumiati. 2017. “Analisa Bandwidth Menggunakan Metode Antrian Per Connection Queue.” *Rabit : Jurnal Teknologi dan Sistem Informasi Univrab* 2(2): 244–57.

Sutopo, Ariesto Hadi. 2023. *Pemrograman Blockchain Smart Contract Di Polygon*. Topazart.

Widodo, Berita Estu, and Agus Sidiq Purnomo. 2020. “Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy.” *Jurnal Teknik Informatika (Jutif)* 1(2): 69–77.