Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 420-427 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Implementation Of Message Security In Pictures Using Playfair Chiper Algorithm

Muhamad Maksum Hidayat[1], Wahyu Nugroho[2], and Dony Ariyus[3]

[1, 2,3)] MTI Universitas Amikom Yogyakarta
Jl. Ringroad Utara, Condong Catur, Depok, Sleman, Yogyakarta

e-mail: maksum.hidayat24@gmail.com[1], wahyunugraha1395@gmail.com[2], dony.a@amikom.ac.id[3]

ARTICLEINFO

Article history:
Received: 25/01/2020
Revised: 31 / 01/2020
Accepted: 01/02/2020

***Keywords**:*
Cryptography, Playfair cipher, Letter hijaiyah, Security

ABSTRACT

Cryptography implementations are now widely solved by cryptanalyst in the process of securing a messaging system, and therefore the need to add a method of steganography. Steganography is the art of hiding secret messages in any medium other than the sender and receiver that no one would know or realize there is a secret message in the media is sent. In this journal, conducted a study on the implementation of cryptography in the form of encryption and decryption of a message using the Playfair cipher algorithm is modified by letter hijaiyah. Then the implementation of steganography in a PNG image media, the testing process is done by sending the media image using email, whatsapp, facebook, and telegram. Research aims to make the encryption process stronger and more secure,

1. Introduction

Information security is a very important thing to note, especially for those who have valuable and confidential information. Along with the development of technology today, a lot of the process of sending messages easy to use social media like whatsapp, facebook, or telegram without security, so we need the process of securing a message or data to be sent, one of the techniques used to secure the data is to perform encryption on a message or a file called cryptographic techniques and concealment of a message or file is called steganography techniques.

Cryptography is one technique for securing messages or information, which can be used as an alternative to minimize criminal actions against the important and confidential information. Based on research conducted by Nani Widyasari said that one of the cyber crime that happens on the Internet is a crime against important documents and confidential[1], Therefore the application of cryptographic techniques is very important to protect the data that is submitted via a communication network or the Internet[2],

In the science of cryptography there are many algorithms that can be used to alter the original text (plaintext) into certain symbols (ciphertext). One of cryptographic algorithms that can be applied is the Playfair cipher[3], the working principle of this algorithm is to transform plaintext into a form that has a key poligram sebanya 25 letter by eliminating characters J and arranged squares 5 x 5, then enkiripsi decryption process undertaken at the poligram[4], However, this method has a weakness, which can be solved by using a cryptanalyst poligram frequency of occurrence information that only contain 25 characters uppercase[3], In addition to the replacement process with i j character at the preparation stage of encryption is also a drawback for Playfair cipher method, as it would be ambiguous to a word that has the character of the letter i in the decryption process[5], For that we need a modification to the Playfair cipher method so that this method becomes more secure and difficult to solve.

Along with the development of technology today, the process of securing messages using cryptography are still felt less because it can be solved by cryptanalyst, therefore there is need to do additional message security by hiding secret messages encrypted into another file or called steganografo[6].*Steganografi* is one of the effective methods used to trick the recipients and the sender of

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 420-427 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

the message that is sent when melihan file. And one of the methods in the science of steganography can be used is a method End of File.

Several previous studies have done the modifications to the Playfair cipher method is Pratika Sari [7], Which modifies the Playfair cipher by means of combining it with vernam cipher algorithm. The research aims to chiperteks produced will be more difficult to resolve because it has been through the process twice with two ciphertext encryption algorithm, so that the generated code will be more complicated. Haodudin[5]also modifying the Playfair cipher algorithm by modifying the cipher into a 12x12 table that can contain characters uppercase letters, numbers, and symbols, making a statistical relationship between the plaintext, the ciphertext, and the key to be complex and get a great confusion. On difusionnya combined with process changes LFSR bits that are affected by the change bit encryption.

Hariati et al[3], Modifying the Playfair cipher algorithm by means of combining it with a zig-zag method. Enkripasi on Playfair cipher process conducted by mensubtitusikan each text character with a new character corresponding formulations will then be carried transposition or scrambling characters using a zig-zag, so that the generated code will be more complicated. The other study was conducted by Zulfansyuri and Abdullah[8] , Who made modifications to the Playfair cipher algorithm to transform into a 6x6 matrix and add 0-9 then performs the sorting character based arrays in introducing it into the matrix, the goal that the generated code is more powerful than standard Playfair.

Denni Bayu Kurniawan and Priyatna[9], In his research malakukan playfai cipher algorithm modification by changing the cipher matrix size to 13 x 13, so as to accommodate the characters to 196 characters to be capitalized and lowercase letters, but it also combines it with the algorithm LFSR (Linear Feedback Shift Register). The result of this cipher algorithm playfir stronger and faster encryption and decryption.

Based on several studies that have been done earlier, the author will modify the Playfair cipher algorithm by combining it with an alpha character hijaiyah and 5x5 matrix table. The process combination that would do is convert the letter to the alphabet letters hijaiyah after the Playfair cipher encryption algorithm so that the generated code in the form of letters hijaiyah, this process will be difficult cryptanalyst to decode the cipher algorithm modified playfai. Besides pelakukan encryption and decryption using the Playfair cipher algorithm writers will also combine the process of securing messages using steganographic techniques so that messages sent over the gated.

2. Research methods

The method applied is the development of systems using the SDLC Waterfall[10] as follows :

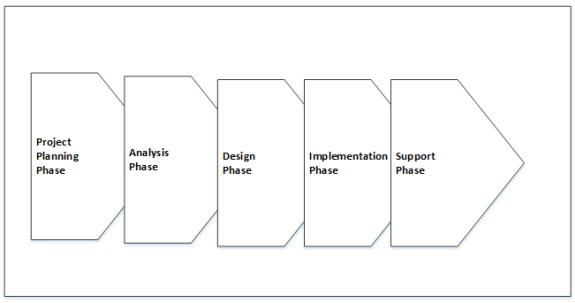

Fig 1. SDLC Waterfall

A. *Project Planning Phase*

This stage is the stage of collecting data from previous studies related to cryptography and steganogafi. This phase includes the identification of problems of cryptography and steganography, data collection supporting research, analysis of theory, research schedule creation, define solutions, and analyze the needs of the system (hardware and software).

B. *analysis Phase*

In this phase, the analysis stage cryptography and steganography process depicted in schematic form as follows:

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 420-427 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

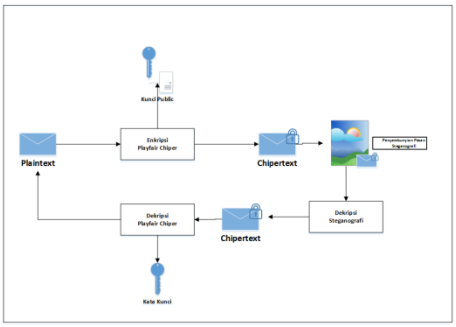

Fig 2. Process Encryption and Decryption

C. ***Design Phase***

In this phase, using object-oriented design in the form of the design process and user interface design.

D. ***Implementation Phase***

In the phase of implementation steps are as follows:

a. Installation System, which is executing the application installation process.
b. Procedural training, which provides an explanation of how the application works.
c. Testing of the system

3. Results and Discussion

In this discussion will present the encryption and decryption process using the Playfair cipher algorithm that is modified with an alpha character hijaiyah.

A. Results Project Planning Phase

Table 1.
Results Project Planning Phase

NO	stages	result
1	Identification of problems	Identify the problem in this research are: 1. Change the secret messages sent and received use you-kan technique Playfair cipher cryptographic algorithm. 2. Hiding a message that was encrypted using the media image formats including PNG.
2	Data collection	The collection of data obtained from research journals and books related to cryptographic techniques with Playfair cipher algorithms and techniques of concealment of messages using steganography techniques.
3	analysis Theory	Related reference derived from the theory as follows: 1. Techniques Playfair cipher cryptographic algorithm. 2. Steganographic techniques using media images. 3. The method of system development using the waterfall SDLC approach has four phases: Project planning phase, Analysis Phase, Design Phase, Implementation Phase, and Support Phase.
4	manufacture of Schedule	This research was conducted in September 2019 until December 2019.
5	Finding Solutions	Created cryptographic applications to encrypt secret messages to be transmitted and received to secure the message. Steganography application was made to hide the message that has been encrypted to an object (picture) to obscure confidential messages from unauthorized parties receive the message.

a. *Process analysis*

Playfair cipher algorithm flowchart process and steganography:

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 420-427 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

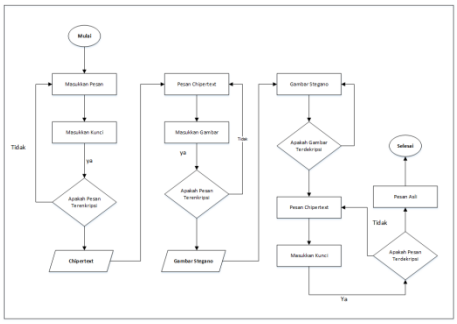

Fig 3. Process Playfair Chiper and Steganography Algorithm

b. Cryptanalysis

Based on the flow of the flowchart in Figure 3, the original message will be encrypted to first become a secret message as follows:

1) Encryption process

In the process of message encryption using the Playfair cipher algorithm modification with the letter hijaiyah, things that need to be prepared is plaintext or messages to be encrypted and the ciphertext or key word. As an example that will be used in this study is the message "gathering one hour in the lobby" and the keyword used is "crypto". The next step is to change the plaintext to form Bigram and converted to karkater hijaiyah letter, as well as ciphertext used are also converted into letter hijaiyah, it aims to increase the value of confusion so that the pattern of the plaintext and ciphertext difficult to solve by cryptanalyst. For the conversion of ciphertext of "crypto" into زعرط فض. For the conversion of plaintext to the letter hijaiyah shown in Table 2 along with bigramnya form.

Table 2.
Converting the results to the alphabet letters letter hijaiyah

MY	MP	UL	JA	MS	AT	UD	IL	OB	IX
زق	شط	قس	بر	شغ	بف	قج	رس	ضت	رم

After the process of converting plaintext and ciphertext of the character alphabet into character letters hijaiyah, the next step is to enter the plaintext that has been shaped Bigram to table Playfair cipher modification (5x5), and enter a keyword or ciphertext to table algotitma Playfair cipher in a spiral or circular from the left above, as shown in Table 3 below:

Table 3.
Table Chiper

ز	ع	ر	ط	ق
ض	ب	ت	ث	ج
ح	خ	د	ذ	س
ش	ص	ظ	غ	ف
ك	ل	م	ن	ه

The next step is to encrypt the plaintext that has been inserted into the table Playfair cipher using the cipher algorithm rules that have been modified, resulting from the initial plaintext "gathered in the lobby one hour" after the encrypted transformed into مررزدقضزصجذحعتحززغمك.

2) Decryption process

Decryption process is the process of the encrypted message into the original message or plaintext readable. Steps to be done is the opposite of the process of message encryption, message encryption in the form of the Arabic alphabet مررزدقضزصجذحعتحززغمك fox to form Bigram be مك - غز- زح- ع ـتـ حذ- جص- زض- ـقـ د- زر- gnisu egassem eht tpyrced ot si pets txen eht ,margiB smrof ot detrevnoc ecnO .رم the table chipper with keywords such as that used in the table chipper when the encryption process and

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 420-427 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

rules used algorithm is an algorithm Playfair cipher modified by letter hijaiyah in reverse, so that the message will go back into plaintext early زقزقطشقبرسشغبفقجرسضرتم hijaiyah in the form of letters.

Table 4.
Conversion to Alphabet Letter Hijaiyah

ز	ق	ش	ط	ق	س	ر	ب	ش	غ	ب	ف	ق	ج	ر	س	ض	ت	ر	م
K	U	M	P	U	L	I	A	M	S	A	T	U	D	I	L	O	B	I	X

The process of conversion of plaintext character to character alphabet letter hijaiyah menghasilkanplainteks "KUMPULIAMSATUDILOBIX". From these results, although still no irregularities words such as IAM and LOBIX, but already biased read and analyzed that the letter I in the word IAM is the replacement character J are discarded when creating tables Playfair cipher standard, and the character X on LOBIX an additional letters for the numbers of odd number when the change process to form Bigram, then after filtered decrypted message will change to "GATHER ONE HOUR lobbied" appropriate initial plaintext before encrypting.

B. Results Analysis System

Analysis of the system applied in this peenelitian use tools activity diagram, as shown in Figure 3 below:

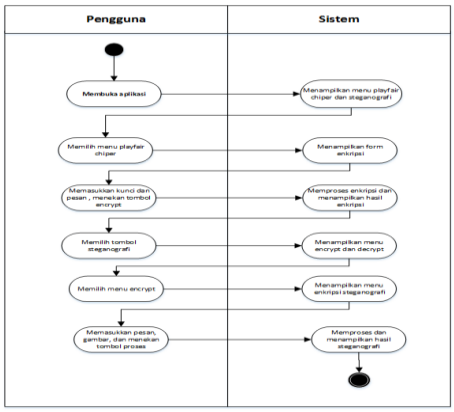

Fig 3. Activity Diagram message encryption process

C. *Design Phase*

1) Interface design Playfair cipher encryption applications

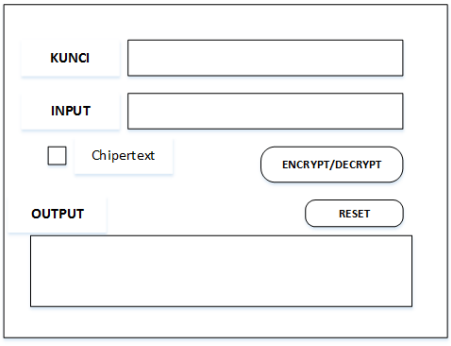

Fig 4. Design Playfair cipher encryption interface

2) Steganography application user interface design

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 420-427 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Fig 5. Design steganographic encryption interface

3) Steganography decryption interface design

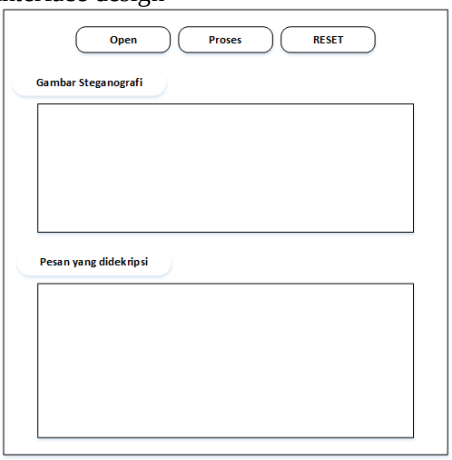

Fig 6. steganography decryption interface design

D. *Implementation Phase*

1) Display cryptography and steganography applications.

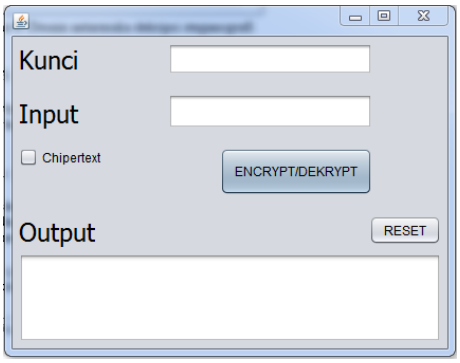

Fig 7. Cryptography Application

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 420-427 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

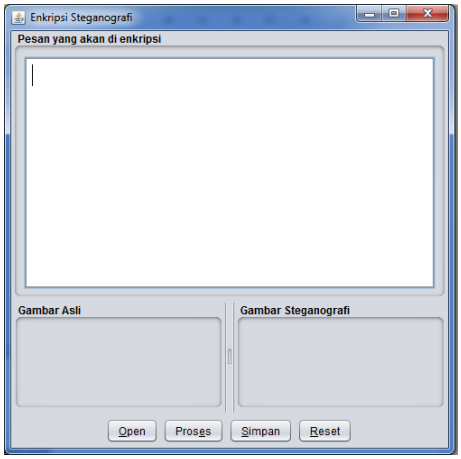

Fig 8. Display Encryption Steganography Applications

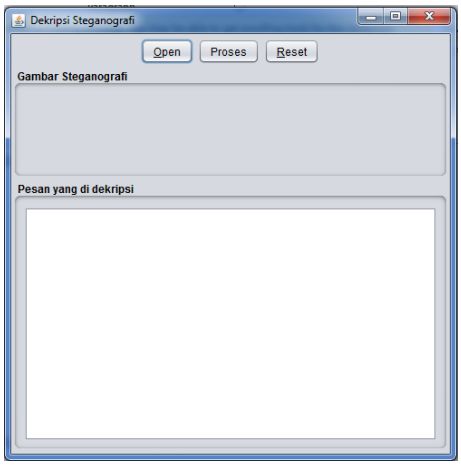

Fig 9. Display decryption Steganography Applications

2) Against Testing System

At this stage of the testing process by sending the image file in PNG and JPEG that contains the secret message that was encrypted using cryptographic techniques Playfair cipher. Files that are used for the test image consists of two files: the first image to the original size jpeg format 4.79 KB file, both PNG file with the original file size 78,8KB. Steps taken for testing are:

a) Encrypt messages using cryptographic applications with Playfair cipher algorithm.
b) The encrypted message is inserted into an image using steganography applications.
c) The image file is sent using the media sender email, facebook, whatsapp with the file format, whatsapp format photographs, telegrams with the file format, and the telegram format photographs.
d) Files sent decrypted using steganography and cryptography applications.

The test results are as follows:

a) Tests on the first image jpeg file with original size 4,79KB.

Table 5.
Results of the first test

examination	Media	HasilEkstensi	Size	decryption
encryption	Steganography applications	PNG	19,6KB	succeed
testing 1	E-mail	PNG	19,6KB	succeed
testing 2	Facebook	JPEG	4.49 KB	Failed
testing 3	Whatsapp File	PNG	19,6KB	succeed
testing 4	Whatsapp Photos	JPEG	4,96KB	Failed

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 420-427 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

testing 5	telegram File	PNG	19,6KB	succeed
testing 6	telegram Photo	JPEG	4,35KB	Failed

b) Testing of the first image with the original size of the PNG file 78,8KB

Table 6.
Results of second test

examination	Media	extension Results	Size	decryption
encryption	Steganography applications	PNG	54,7KB	succeed
testing 1	E-mail	PNG	54,7KB	succeed
testing 2	Facebook	JPEG	36.7 KB	Failed
testing 3	Whatsapp File	PNG	**54,7KB**	succeed
testing 4	Whatsapp Photos	JPEG	55,8KB	Failed
testing 5	telegram File	PNG	54,7KB	succeed
testing 6	telegram Photo	JPEG	36,4KB	Failed

4. Conclusion

Based on the discussion that has been done, some of the conclusions of this study are as follows:

a. Modification of rules on the Playfair cipher method can be applied.
b. In the process of steganography there is a difference between jpeg and png,
c. If the file extension jpeg ber when done steganography file size is increased.
d. If the file extension PNG ber when done steganography file size will be reduced.
e. In the testing process when the steganographic image files sent using social media facebook, wa and telegrams photo file will be compressed and loaded messages disappear and can not be encrypted.
f. When the file is sent in the form of a file the size of the uncompressed file and message successfully decrypted.

5. Reference

[1] N. W. Sari, "Kejahatan Cyber dalam Perkembangan Teknologi Informasi Berbasis Komputer," *J. Surya Kencana Dua Din. Masal. Huk. dan Keadilan*, vol. 5, no. 2, pp. 577–593, 2018.
[2] E. Setyaningsih, "Penyandian Citra Menggunakan Metode Playfair Cipher," *J. Teknol.*, vol. 2, pp. 213–219, 2009.
[3] A. Hariati, "Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks," *J. Penelit. Tek. Inform.*, vol. 2, no. 2, pp. 13–17, 2018.
[4] A. Syahputra, "Analisa Implementasi Pengamanan File Audio Menggunakan Algoritma Playfair," *J. Pelita Inform.*, vol. 17, no. 4, pp. 366–374, 2018.
[5] E. H. Nurkifli, "Modifikasi Algoritma Playfair Dan Menggabungkan Dengan Linear Feedback Shift Register (Lfsr)," in *Seminar Nasional Teknologi Informasi dan Komunikasi 2014 (SENTIKA 2014)*, 2014, pp. 366–371.
[6] A. Rohmanu, "Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End Of File," *J. Inform. SIMANTIK*, vol. 1, no. 2, pp. 1–11, 2017.
[7] P. S. Eka, "Implementasi Keamanan Data Menggunakan Algoritma Vernam Cipher Dan Playfair Cipher," *J. Pelita Inform.*, vol. 17, no. 4, pp. 430–435, 2018.
[8] M. Z. Siambaton and A. Muhazir, "Modifikasi Algoritma Playfair Cipher Dengan Pengurutan Array Pada Matriks," *J. Ilmu Komput. dan Inform.*, vol. 02, no. April, pp. 66–71, 2018.
[9] B. Priyatna, U. Buana, and P. Karawang, "PENGAMANAN DATA BERBASIS MOBILE ANDROID DENGAN PENGAMANAN DATA BERBASIS MOBILE ANDROID DENGAN PENGGABUNGAN LINEAR FEEDBACK SHIFT REGISTER (LFSR) DAN MODIFIKASI MATRIKS," *J. Telemat. MKOM*, vol. 10, no. 1, 2018.
[10] H. Al Fatta, *Analisis Perancangan Sistem Operasi Untuk Keunggulan Bersaing Perusahaan dan Organisasi Modern*. Yogyakarta: Andi Offset, 2007.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.