Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 412-420 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Modification Of Two Playfair Algorithm And Caesar Chiper Algorithm Using City Post Code

Sewindu Putro[1], Sumbogo Wisnu Pamungkas[2], dan Dony Ariyus[3]

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

e-mail: sewindup@gmail.com[1)], Sumbogo8122@students.amikom.ac.id[2)], dony.a@amikom.ac.id[3)]

ARTICLEINFO

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

Keywords:
Playfair Cipher, Caesar Chiper, Steganography

ABSTRACT

Privacy and data security is one of the most important aspects that need to be addressed, especially in this digital age where all desktop and mobile computing devices can be connected to one another in a virtual world that causes virtually impossible to protect the message to its destination. The purpose of this study is a modification of the Playfair cipher algorithm and caesar cipher with the postal code of the city, aims to produce a ciphertext that is more complex and not easily solved. In this penelian also implement LSB steganography method so that the message content more secure and not readily known by those who do not have an interest. From the test results of this study showed that by modifying the Playfair cipher algorithm and caesar cipher with city postal code in the encoding, produce ciphertext more complicated to be returned to the original message by parties who have no interest. Applying LSB steganography method makes the observer is not aware of the information that is pasted on the image that acts as a message.

1. Introduction

Privacy and data security is one of the most important aspects that need to be addressed, especially in this digital age where all desktop and mobile computing devices can be connected to one another in a virtual world that causes virtually impossible to protect the message to its destination. Hackers often infiltrate into the device to conduct cybercrime example by attempting to steal data or change the data or the original message.

To maintain the security aspects of data and for security reasons to maintain the confidentiality of messages or data, then comes techniques - message encoding techniques or better known as cryptography.Cryptography is the science and art of maintaining the security of a message when the message is sent from one place to another [1]. Message or data will be concatenated into a code - a code that has no meaning and is not understood by a person or a computer, so if there are other parties who are not eligible, then they will not know the true meaning of the message. In the process of encoding the plaintext into a ciphertext is called encryption and reverse the process of ciphertext into a plaintext is called decryption origin. There are several cryptographic techniques including the Playfair cipher and caesar cipher.

*Playfair cipher*is an encryption or decryption process performed on the letters in pairs and use a 5x5 matrix. All in Playfair cipher alphabet laid out in the matrix except the letter J is replaced with the letter I [2]. Caesar Cipher itself is a cipher that is shifting. The Caesar Cipher cipher text obtained from the plaintext alphabet, by shifting the letters in plaintext with a certain number of letters [3].

*steganography*is the science of hiding a form of text messages in other media, so that the hidden text messages can be fused with the media. The media here can be text, images, audio, and video [4].

Referring to some previous studies that Design For Security Applications Folder With Playfair algorithm, aims to create an application that is used to secure a method to apply a text file with Playfair [5]. Playfair Cipher Algorithm Implementation For Security File Encryption Key In Text With Rijndael algorithm, aimed at the implementation of Playfair cipher algorithm that is used to secure the data [6]. 2326662 Cipher Algorithm Modifications By Ordering Array Matrix, aims to improve the ability of data

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

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 412-420 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

security by changing the size of a 6x6 matrix with the hope to be stronger than the standard Playfair [7].

Based on these studies, this research author will modify the Playfair cipher algorithm and caesar cipher with the postal code of the city, aims to produce a ciphertext that is more complex and not easily solved. In this study presented also apply steganographic message that the content be more secure and not easily known by the party that has no interest.

2. Method

The method used in this study is menkombinasikan Playfair cipher algorithm with a Caesar Cipher. In this study also modifying the algorithm by using ZIP Code.

A. Flow Encryption

Flow encryption is an overview of the process of encryption algorithms to be designed, for mengetahuii groove encryption process can be seen in Figure 1.

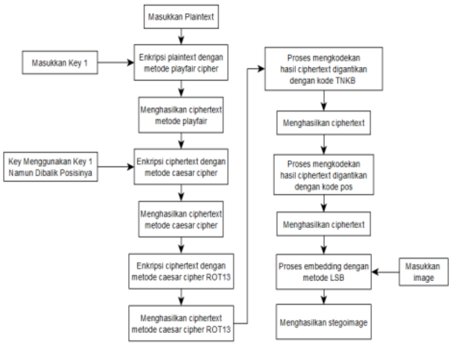

Fig 1. Flow Encryption

In Figure 1 is the flow of encryption do. Langah first set up messages to be kept secret (plaintext). Next determine the key 1 (key) and the encryption is done using methods*Playfair cipher* generating ciphertext from Playfair cipher method. Furthermore, the Caesar Cipher encryption method by using key 1 but reversed sequence positions produce ciphertext from Caesar Cipher method. Furthermore, the encryption method generates ciphertext of ROT13 ROT13 method. The next process coding ciphertext results by the number sign motor vehicles produce ciphertext in the form of motor vehicle number sign code. The next process coding results produce ciphertext ciphertext zip code in the form of a zip code. then prepares media to be pasted image insertion and incoming messages on penyisipkan ciphertext steganography is in the image using the LSB. Generate stego image that is the image that has been inserted message

B. Flow Decryption

Flow decryption is an overview of the decryption process of the algorithm that will be designed, for mengetahuii flow of the decryption process can be seen in Figure 2.

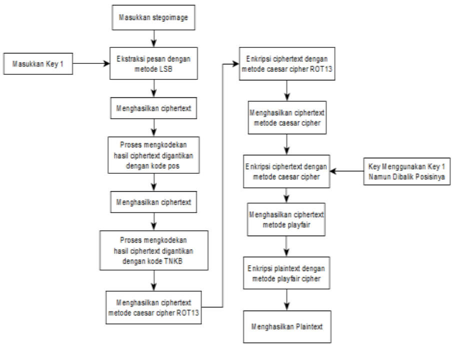

Fig 2. Flow Decryption

In figure 2 is the flow of decryption is done. The first langah prepare stego image will open the messages within it. Next maasukkan key 1 (key) and do ekstransi messagein the image using the LSB method of generating ciphertext. then do the encoding results with zip code generating ciphertext ciphertext in the form of a zip code. The next process coding ciphertext results by the number sign motor vehicles produce ciphertext in the form of motor vehicle number sign code. Furthermore, the encryption

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

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 412-420 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

method generates ciphertext of ROT13 ROT13 method. Furthermore, the Caesar Cipher encryption method by using key 1 but reversed sequence positions produce ciphertext from Caesar Cipher method. Furthermore, the Playfair cipher encryption method generates plaintext (hidden message).

C. Playfair Cipher

*Playfair cipher*is an encryption or decryption process performed on the letters in pairs and use a 5x5 matrix. All in Playfair cipher alphabet laid out in the matrix except the letter J is replaced with the letter I. In Playfair cipher key used must not contain letters or characters of the same. In the first row inserted key, then forwarded to the next alphabet in sequence [2]. In a mathematical formula, the encryption process using the Playfair cipher message, namely:

a) If two (2) letters contained in the same row lock, then using the formula:
E1 = (x + 1, y)

b) If two (2) letters are on the same key columns, then using the formula:
E1 = (x, y + 1)

c) If two (2) letters are not in the same column or the same line, then:

1. If Y1 <Y2 then using the formula:
The first letter: E1 = (x, y + (m - 1))
the second letter : E1 = (x, y - (m - 1))

2. If Y1> Y2 then using the formula:
The first letter: E1 = (x, y - (m - 1))
the second letter : **E1 = (x, y + (m - 1))**

With information E1 = Result Encryption, Y1 = Y axis coordinates first letter, Y2 = second letter Y axis coordinates, x = Coordinate X axis, y = Coordinate Y-axis, and m = Number of columns matrix formed by the intersection of two letters plaintext.

D. Caesar Cipher

*Caesar Cipher*is a cipher that is shifting. The Caesar Cipher cipher text obtained from the plaintext alphabet, by shifting the letters in plaintext with a certain number of letters [3]. In a mathematical formula, the process of message encryption using cipher caesar namely:

En = (X + K) mod 26

With information En = Result Encryption, X = plaintext ,and K = Shift.

E. *ROT13*

ROT13 is a derivative of caesar cipher. The way it works is by moving forward from the initial letters as much as 13 times in the order in alfabetn [8]. In a mathematical formula, the process of message encryption using ROT13 method are:

C = ROT13 (P)

With the description of the C = Results Encryption. ROT13 = Rotate 13. P = plaintext.

F. Motorized Vehicle registration number (TNKB)

The number sign motor vehicle is a motor vehicle regident sign that serves as proof of the legitimacy of operating a motor vehicle in the form of plates with the specifications issued by the Police and containing an area code, registration number, as well as the validity period and mounted on a motor vehicle [9]. This Baerikut sign listing numbers of motor vehicles for each city:

Table 1.
List of Motor Vehicle registration number

TNKB	City	TNKB	City	TNKB	City	TNKB	City
A	Banten	H	Semarang	O	Field	V	Riau
B	Jakarta	I	Madiun	P	Besuki	W	Sidoarjo
C	Surakarta	J	Bali	Q	Jambi	X	Flores
D	duo	K	Starch	R	Banyumas	Y	Papuan
E	Cirebon	L	Surabaya	S	Bojonegoro	Z	Sumedang
F	Bogor	M	Madura	T	Karawang	-	-
G	Pekalongan	N	Poor	U	Yogyakarta	-	-

In Table 1 there are some letters that are not on the number of vehicles, the letter C, I, J, O, Q, U, V, X, and Y. From these letters then replace letters with numbers of other vehicles such as C becomes AD, I into AE, J to DK, O becomes BK, Q becomes BH, U becomes AB, V to BM, EB mendai X and Y into DS.

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

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 412-420 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

G. Postal code

Post code is a code that serves to define or facilitate the delivery of mail or goods in different regions within a country [10]. Here is a list of zip codes:

Table 2.
List Postal Standards

City	Postal code	City	Postal code	City	Postal code	City	Postal code
Banten	42 191	Semarang	50 111	Field	20028	Riau	28124
Jakarta	10110	Madiun	63 111	Besuki	68 356	Sidoarjo	61211
Surakarta	57 116	Bali	80 351	Jambi	36111	Flores	86 212
duo	40111	Starch	59111	Banyumas	53 172	Papuan	98 871
Cirebon	45 111	Surabaya	60111	Bojonegoro	62 111	Sumedang	45311
Bogor	16 111	Madura	53 265	Karawang	41 311	-	-
Pekalongan	51 111	Poor	57139	Yogyakarta	55000	-	-

H. Steganography

*steganography*is the science of hiding a form of text messages in other media, so that the hidden text messages can be fused with the media. The media here can be text, images, audio, and video [4]. In steganography there are several methods, one of which uses the method of Least Significant Bit (LSB). Least Significant Bit (LSB) is one method of steganography most simple and easy to implement. This method uses a digital image as the cover medium. In the arrangement of bits in a byte (where 1 byte = 8 bits), there is the most significant bit is the Most Significant Bit (MSB) and least significant bit is the Least Significant Bit (LSB). For example 11010010 bytes, the number of bits 1 that underlined is the MSB bit and bit rate of 0 which is underlined is the LSB [11].

3. result

3.1. Encryption process

In this encryption process, the first time a plaintext encryption by using methods Playfair cipher, then the results will be encrypted ciphertext again using the method of Caesar Cipher.

a) Playfair Cipher

The first encryption process is done by using the method of Playfair cipher. Here is an example of the plaintext used "GRADUATION IMMEDIATELY" and the key that will be used "AMIKOM YK". The next step removes the same character on the key that will be used, so the key is changed to "AMIKOY". The next process create 5x5 matrix keys, as in figure 3.

A (0,0)	M (0,1)	I (0,2)	K (0,3)	O (0,4)
Y (1,0)	B (1,1)	C (1,2)	D (1,3)	E (1,4)
F (2,0)	G (2,1)	H (2,2)	L (2,3)	N (2,4)
P (3,0)	Q (3,1)	R (3,2)	S (3,3)	T (3,4)
U (4,0)	V (4,1)	W (4,2)	X (4,3)	Z (4,4)

Fig 3. Process Playfair Cipher Encryption

The next step expands the matrix by adding a sixth row and the sixth column, as in Figure 4:

A (0,0)	M (0,1)	I (0,2)	K (0,3)	O (0,4)	A (0,5)
Y (1,0)	B (1,1)	C (1,2)	D (1,3)	E (1,4)	Y (1,5)
F (2,0)	G (2,1)	H (2,2)	L (2,3)	N (2,4)	F (2,5)
P (3,0)	Q (3,1)	R (3,2)	S (3,3)	T (3,4)	P (3,5)
U (4,0)	V (4,1)	W (4,2)	X (4,3)	Z (4,4)	U (4,5)
A (5,0)	M (5,1)	I (5,2)	K (5,3)	O (5,4)	

Fig 4. Process Playfair Cipher Encryption Adds Sixth Line

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 412-420 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

If the matrix has been created, then the first step plaintext split into 2 letter (in pairs). So changed as follows:

plaintext = IMMEDIATELY WISUDA ➔ GE SE WI RA SU DA

The next stage is to do the encryption process every 2 letter corresponding to the key matrix that has been made in accordance with the three existing rules. The results were as follows:

1. SE➔ The letters are not in the same column or the same row and Y1 <Y2, then the result:
   S (3.3) ➔ E1 = (3, 3+ (2-1)) = (3,4) = T E (1.4) ➔ E1 = (1, 4- (2-1)) = (1,3) = D
2. GE➔ The letters are not in the same column or the same row Y1 <Y2, then the result:
   G (2,1) ➔ E1 = (2, 1 + (4-1)) = (2,4) = N E (1.4) ➔ E1 = (1, 4- (4-1)) = (1,1) = B
3. RA ➔ The letters are not in the same column or the same row Y1> Y2, then the result:
   R (3,2) ➔ E1 = (3, 2- (3-1)) = (3,0) = P A (0,0) ➔ E1 = (0, 0+ (3-1)) = (0,2) = I
4. WI ➔ The letters contained in the rows of keys are the same, then the result is:
   W (4.2) ➔ E1 = (4 + 1, 2) = (5,2) = I I (0.2) ➔ E1 = (0 + 1, 2) = (1,2) = C
5. SU ➔ The letters are not in the same column or the same row Y1> Y2, then the result:
   S (3.3) ➔ E1 = (3, 3- (4-1)) = (3,0) = P U (4,0) ➔ E1 = (4, 0+ (4-1)) = (4,3) = X
6. DA ➔ The letters are not in the same column or the same row Y1> Y2, then the result:
   D (1.3) ➔ E1 = (1, 3- (4-1)) = (1,0) = Y A (0,0) ➔ E1 = (0, 0+ (4-1)) = (0,3) = K

So that the ciphertext of the encryption process Playfair cipher method into TD NB PI IC YK PX.

b) Caesar Cipher

The next encryption process that is the result of the algorithm Playfair cipher ciphertext encrypted again using Chiper Caesar algorithm by using a key on Playfair cipher algorithm that direverse. So that initially AMIKOY be YOKIMA. Because it uses a key that created itself, so his key now becomes 0. The composition of the alphabet for the calculation of Caesar Chiper algorithm that can be seen in Table 1:

Table 1.
Caesar Cipher

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Key	Y	O	K	I	M	A	B	C	D	E	F	G	H	J	L	N	P	Q	R	S	T	U	V	W	X	Z

The first step of the method further Playfair cipher ciphertext converted into an integer, it is obtained:

T = 19; D = 3; N = 13; B = 1; P = 15; I = 8; I = 8; C = 2; P = 15; X = 23; Y = 24; K = 10;

The second step is to do the encryption on each of each letter:

T ➔ □ (T) = 19 □□□ 26 = 19 = S
D ➔ □ (D) = 3 □□□ 26 = 3 = I
N ➔ □ (N) = 13 □□□ 26 = 13 = J
B ➔ □ (B) = 1 □□□ 26 = 1 = O

P ➔ □ (P) = 15 26 = 15 = □□□ □
I ➔ □ (I) = 8 □□□ 26 = 8 = D
I ➔ □ (I) = 8 □□□ 26 = 8 = D
C ➔ □ (C) = 2 □□□ 26 = 2 = K

P ➔ □ (P) = 15 □□□ 26 = 15 = N
X ➔ □ (X) = 23 □□□ 26 = 23 = W
Y ➔ □ (Y) = 24 □□□ 26 = 24 = X
K ➔ □ (□) □□□ 26 = 10 = 10 = F

So that after the encryption process using methods caesar cipher, ciphertext transformed into SI JO DK ND NW XF.

c) ROT13

The next stage is the result of the method caesar ciphertext cipher encryption process is carried out again using ROT31 or shift number 13. The encryption process is done by dividing the alphabet into two sections and reflects each individual letter. The results of this reflection is the ciphertext letter that will be used to further process. Reflections of each letter can be seen in Table 3.

Table 3.
ROT13

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

So that would be obtained ciphertext as follows:

plaintext = SI JO DK ND NW XF

C = ROT13 (S) = F
C = ROT13 (I) = V
C = ROT13 (J) = W
C = ROT13 (O) = B

C = ROT13 (N) = A
C = ROT13 (D) = Q
C = ROT13 (D) = Q
C = ROT13 (K) = X

C = ROT13 (N) = A
C = ROT13 (W) = J
C = ROT13 (X) = K
C = ROT13 (F) = S

So that the ciphertext be: FV WB QX AQ AJ KS.

d) Conversion From Aphabet be Postcode

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

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 412-420 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Then after the ciphertext is finished, the next stage is to convert each letter into the code number of the vehicle. After that replaces the letter of vehicle number in accordance with the city code of the city of origin of origin Furthermore the vehicle number converted by zip code license hometown. So ciphertext FV WB QX AQ AJ KS hometown converted to the number of vehicles as shown in Table 4:

Table 4. Conversions No. Vehicles Become a City Name

No. Vehicle	F	V	W	B	A	Q	Q	X	A	J	K	S
City name	Bogor	Riau	Sidoarjo	Jakarta	Banten	Jambi	Jambi	Flores	Banten	Bali	Starch	Bojonegoro

Next is converting from every town with the postal code of the city. The conversion result can be seen in the table5.

Table 5.
Conversion Name City Being Postal

City name	Bogor	Riau	Sidoarjo	Jakarta	Banten	Jambi	Jambi	Flores	Banten	Bali	Starch	Bojonegoro
Postal code	16 111	28124	61211	10110	42 191	36111	36111	86 212	42 191	80 351	59111	62 111

So the result chipertextnya into 1611128124 61211101104219136111 36111862124219180351591116 2 111.

3.2. Decryption

a. Conversion From Aphabet be Postcode

Of ciphertext zip code is separated every 5 digits. This is done because the number of digits of the postal codes of each respective city amounted to 5 digits. So from every postcode converted into a city name. The conversion result can be seen in Table 6.

Table 6.
Conversion Postal Being Name City

Postal code	16 111	28124	61211	10110	42 191	36111	36111	86 212	42 191	80 351	59111	62 111
City name	Bogor	Riau	Sidoarjo	Jakarta	Banten	Jambi	Jambi	Flores	Banten	Bali	Starch	Bojonegoro

The next step is to convert the city into a letter of the name of the vehicle number hometown. The conversion result into a number of vehicles the city name's home town can be seen in Table 7.

Table 7.
Conversion Name City Being No.Kendaraan

City name	Bogor	Riau	Sidoarjo	Jakarta	Banten	Jambi	Jambi	Flores	Banten	Bali	Starch	Bojonegoro
No. Vehicle	F	V	W	B	A	Q	Q	X	A	J	K	S

So we get the plaintext FVWBAQQXAJKS

b. ROT13

The next stage is the result of converting plaintext into a city name No. vehicle decryption process is done again using ROT31 or shift number 13. So the results become:

C = ROT13 (F) = S
C = ROT13 (V) = I
C = ROT13 (W) = J
C = ROT13 (B) = O
C = ROT13 (A) = N
C = ROT13 (Q) = D
C = ROT13 (Q) = D
C = ROT13 (X) = K
C = ROT13 (A) = N
C = ROT13 (J) = W
C = ROT13 (K) = X
C = ROT13 (S) = F

So ciphertext becomes: SI JO DK ND NW XF

c. Caesar Cipher

The next decryption process is the result of the algorithm ROT13 plaintext will decrypt it using caesar cipher algorithm by using a key that have previously been made, namely YOKIMA. Caesar cipher decryption formula is the same with the encryption formula, the difference is plaintext alphabet used is already inserted YOKIMA key. Here is a caesarean decryption calculation cipher:

Table 8.
Caesar Cipher Decryption

plaintext	Y	O	K	I	M	A	B	C	D	E	F	G	H	J	L	N	P	Q	R	S	T	U	V	W	X	Z
Key	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

S = 19; I = 3; J = 13; O = 1; N = 15; D = 8; D = 8; K = 2; N = 15; W = 23; X = 24; F = 10;

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

S ➔ □ (S) = 19 □□□ 26 = 19 = T	N ➔ □ (N) = 15 □□□ 26 = 15 = P	N ➔ □ (N) = 15 □□□ 26 = 15 = P
I ➔ □ (I) = 3 □□□ 26 = 3 = D	D ➔ □ (D) = 8 □□□ 26 = 8 = I	W➔ □ (W) = 23 □□□ 26 = 23 = X
J ➔ □ (J) = 13 □□□ 26 = 13 = N	D ➔ □ (D) = 8 □□□ 26 = 8 = I	X ➔ □ (X) = 24 □□□ 26 = 24 = Y
O ➔ □ (O) = 1 □□□□ 26 = 1 = B	K ➔ □ (K) = 2 □□□ 26 = 2 = C	F ➔ □ (F) = 10 □□□ 26 = 10 = K

So that after the decryption process using methods caesar cipher, plaintext turns into TD NB PI IC YK PX.

d. Playfair Cipher

The next stage is to do the encryption process every 2 letter corresponding to the key matrix that has been made in accordance with the three existing rules. The results were as follows:

a. TD ➔ The letters are not in the same column or the same row and Y1> Y2, then the result:
T (3.4) ➔ E1 = (3, 4- (2-1)) = (3,3) = S D (1.3) ➔ E1 = (1, 3+ (2-1)) = (1,4) = E
b. NB ➔ The letters are not in the same column or the same row Y1> Y2, then the result:
N (2,4) ➔ E1 = (2, 4- (4-1)) = (2,1) = G B (1,1) ➔ E1 = (1, 1+ (4-1)) = (1,4) = E
c. PI ➔ The letters are not in the same column or the same row Y1 <Y2, then the result:
P (3,0) ➔ E1 = (3, 0 + (3-1)) = (3,2) = R I (0.2) ➔ E1 = (0, 2- (3-1)) = (0,0) = A
d. IC ➔ The letters contained in the rows of keys are the same, then the result is:
I (5.2) ➔ E1 = (5-1, 2) = (4,2) = W C (1,2) ➔ E1 = (1-1, 2) = (0,2) = I
e. PX ➔ The letters are not in the same column or the same row Y1 <Y2, then the result:
P (3,0) ➔ E1 = (3, 0 + (4-1)) = (3,3) = S X (4.3) ➔ E1 = (4, 3- (4-1)) = (4,0) = U
f. YK ➔ The letters are not in the same column or the same row Y1 <Y2, then the result:
Y (1,0) ➔ E1 = (1, 0 + (4-1)) = (1,3) = D K (0.3) ➔ E1 = (0, 3- (4-1)) = (0,0) = A

After the decryption process using the Playfair cipher algorithm, the obtained plain text "IMMEDIATE GRADUATION", submitted in accordance with the sender.

3.3. steganography

When the encryption process uses a modified algorithm that is designed, then the message will be inserted back in an image using steganography method LSB (Least Significant Bit).

3.4. Implementation of algorithms

The design of algorithms that have been created are then implemented using the Java programming language by using the software Android Studio.

4. Discussion

4.1. Interface Applications

a. Encryption Process Page Views

On page encryption process used to encrypt the original message into an image. The first process the user enters the messages to be encrypted and then enter the key, then click Encrypt after appearing cipher-text then click choose the image for the encryption process using steganographic methods. The results will be saved steganographic encryption download folder. Page views encryption process can be seen in Figure 5.

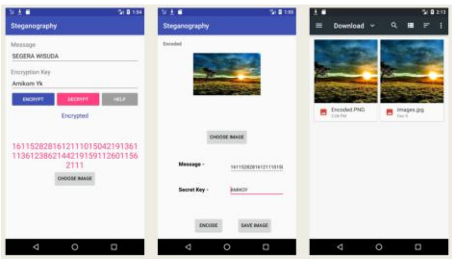

Fig 5. Encryption Process Page Views

b. Decryption Process Page Views

On page decryption process is used to perform the decryption of the image into the original message. The first process the user selects the image to be decrypted by clicking choose the image, select the image that will be later decrypted, after the image uploaded and then enter the key according to the key at the

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 412-420 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

time of the encryption process. Then if the decryption process is successful it will display the message successfully decoded. Then click OK it will display the original message.

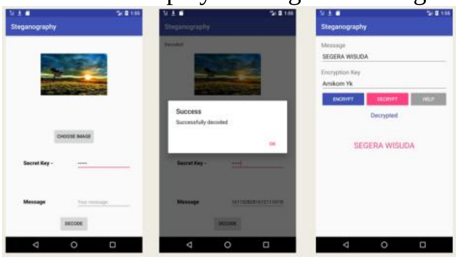

Fig 6. Decryption Process Display

4.2. Test result

Having successfully created a method which is designed in the form of apps then testing the insertion of the number of characters. File test in the extension .jpg image file. The test results are shown in Table 9.

Table 9.
Testing Insertion Number of Characters

examination	Key	number of Characters	So File Name	Initial File Size	Final File Size	Dimension Pictures	encryption	decryption
1	AMIKOMYK	13	encoded 13.PNG	28.5 Kb	270 Kb	661 x 464	succeed	succeed
2	AMIKOMYK	112	encoded 112.PNG	28.5 Kb	271 Kb	661 x 464	succeed	succeed
3	AMIKOMYK	560	encoded 560.PNG	28.5 Kb	276 Kb	661 x 464	succeed	succeed
4	AMIKOMYK	1120	encoded 1120.PNG	28.5 Kb	280 Kb	661 x 464	succeed	succeed
5	AMIKOMYK	10389	encoded 10389.PNG	28.5 Kb	338 Kb	661 x 464	succeed	succeed
6	AMIKOMYK	20 776	20776. encoded PNG	436 Kb	610 Kb	1980 x 1080	succeed	succeed

Then the researchers also sending pictures that have been encrypted to several social media and further testing decryption. The test results are shown in Table 10.

Table 10.
Decryption Testing Into Some Social Media

Social media	decryption
Posted By WhatsApp (image)	Not successful
Posted By WhatsApp (File)	succeed
Sent Via Email	succeed
Posted By Instagram	Not successful
Sent Through Facebook	Not successful

5. Conclusion

Based on research done by modifying the Playfair cipher algorithm and caesar cipher with city postal code in the encoding, resulting in a more complicated ciphertext is returned to the original message that does not have an interest. Applying LSB steganography method makes the observer is not aware of the information that is pasted on the image that acts as a message. Size image dimensions affect the success of the system to accommodate the number of characters that will do the encryption and decryption process. Semakain Great sized dimensions of the image, the greater the capacity to accommodate the number of characters in the image. The number of characters used in the encryption and decryption process affects the resulting file size. The more the number of characters, the greater the resulting file size.

6. Reference

[1] Pradipta, A., 2016, Implementasi Metode Caesar Cipher Alphabet Majemuk dalam Kriptografi untuk Pengamanan Informasi, Indonesian Journal on Networking and Security, Vol. 5, No. 3.

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

[2] Santi, R.C.N., 2010, Implementasi Algoritma Enkripsi Playfair pada File Teks, Jurnal Teknologi Informasi DINAMIK.Vol. XV, No.1.
[3] Harun,Mukhtar. 2018. *Sistem jaringan komputer untuk pemula*. Yogyakarta: Deepublish.
[4] Setiawan, W., dkk. 2012. Aplikasi Keamanan Pesan Menggunakan Algoritma Steganografi dan Kriptografi. jurnal Telematika. Vol.8, No.2.
[5] Kurniawan, Indra. 2019. Perancangan Aplikasi Untuk Keamanan Folder Dengan Algoritma Paly Fair. Jurnal Informatika Kaputama (JIK). Vol. 3, No.1.
[6] Santoso, Dedek Dwi,. dkk. 2018. Penerapan Algoritma Playfair Cipher Sebagai Penyandian Kunci Dalam Pengamanan File Teks Dengan Algoritma Rijndael. Jurnal Pelita Informatika. Vol. 17, No.1.
[7] Siambaton, Mhd Zulfansyuri,. dkk. 2018. Modifikasi Algoritma Playfair Cipher Dengan Pengurutan Array Pada Matriks. Jurnal Ilmu Komputer dan Informatika. Vol.2, No.1.
[8] Nugroho, Adi. 2009. Algoritma dan Struktur Data dengan C#. Yogyakarta: Andi Offset.
[9] Sinabela, Zhulhan Sentoso,. dkk. 2018. Perancangan Aplikasi Kode Pos Indonesia Berbasis Mobile Dengan Menerapakan Algoritma Zhu-Takaoka. Jurnal Konferensi Nasional Teknologi Informasi dan Komputer. Vol.2, No.1.
[10] KAPOLRI, 2012. Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2012 Tentang Registrasi dan Identifikasi Kendaraan Bermotor.
[11] Sadikin, R. .2012. Kriptografi untuk Keamanan Jaringan. Andi: Yogyakarta.