Analisis Penerapan Modifikasi Algoritma Vigenere Cipher, Caesar Cipher, Vernam Cipher dan Hill Cipher Untuk Penyisipan Pesan Dalam Gambar

Analysis of Application of Modification of Vigenere Cipher Algorithm, Caesar Cipher, Vernam Cipher and Hill Cipher for Message Insertion in Images

Siti Fatonah[1], Anisa Yulandari[2], Dony Ariyus[3]
[1,2,3]MTI Universitas Amikom Yogyakarta
E-mail: [1]fatonah476@gmail.com@,[2]anisa.y@amikom.ac.id,[3]dony.a@amikom.ac.id

Abstrak

Saat ini informasi merupakan elemen yang sangat penting dalam kehidupan manusia. Menjaga keamanan informasi plaintext dapat dilakukan melalui proses enkripsi dalam kriptografi. Penelitian sebelumnya, berbagai algoritma yang dapat digunakan untuk melakukan enkripsi maupun dekripsi dalam kriptografi. Penelitian ini melakukan pengamanan pesan dengan menyisipkan pesan pada sebuah gambar menggunakan algoritma steganografi LSB (least Significant Bit) pada pesan yang telah dienkripsi menggunakan modifikasi algoritma vigenere cipher, hill cipher, vernam cipher dan hill cipher. Hasil penelitian ini pesan dapat disembunyikan dalam gambar dengan meletakkan pesan pada bit terakhir gambar.

Kata Kunci*—kriptografi, steganografi, keamananinformasi*

Abstract

Information is a very important element in human life. Maintaining the security of plaintext information can be done through encryption in cryptography. Previous research, various algorithms that can be used to encrypt and decrypt cryptography. This study secures messages by inserting messages on an image using the least significant LSB steganography algorithm on messages that have been encrypted using a modified vigenere cipher algorithm, hill cipher, vernam cipher and hill cipher. The results of this study message can be hidden in the image by placing a message on the last bit of the image..

Keywords*—cryptography, steganography, information security*

1. PENDAHULUAN

Algoritma kriptografi telah banyak sekali diciptakan untuk menyembunyikan pesan. Algoritma kriptografi saat ini dapat dikelompokan menjadi algoritma klasik dan algoritma modern. Bentuk umum algoritma klasik yaitu cipher subtitusi dan cipher transposisi. Cipher subtitusi dilakukan dengan mengganti (substitusi) suatu huruf pada plaintext menjadi huruf lain pada chipertext. Jenis substitusi dalam kriptografi antara lainCipher Abjad Tunggal, Cipher Substitusi Homofonik, Cipher Abjad Majemuk, dan Polygram Substitution Cipher. Contoh algoritma kriptografi klasik dengan bentuk cipher substitusi yaitu Vigenere Cipher, Caesar Cipher, dan Hill Cipher[1]. Dalam kriptografi, vigenere cipher merupakan salah satu jenis

algoritma klasik berbasis karakter. Proses enkripsi dalam algoritma vigenere cipher dengan merubah plaintext menggunakan kunci tertentu yang berulang sepanjang plaintext sehingga diperoleh ciphertext. Algoritma vigenere cipher memiliki kelemahan yaitu adanya perulangan karakter sehingga mudah diserang dengan analisis frekuensi dan metode kaskisi. Cara tersebut dapat mengetahui panjang huruf yang digunakan sebagai kunci pada vigenere cipher. Sehingga diperlukan modifikasi pada vigenere cipher untuk mengatasi kelemahan tersebut. Modifikasi vigenere cipher dalam penelitian ini dilakukan dengan menambahkan angka 0-9 pada kolom dan baris[3].

Pada algoritma Caesar cipher, setiap huruf pada plaintext digantikan huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Dalam caesar cipher pergeseran pada tiap karakter dilakukan sesai dengan kunci yang diberikan[4]. Modifikasi caesar cipher dalam penelitian ini yaitu dengan merubah setiap plaintext kedalam biner kemudian dilakukan pergeseran sebanyak 3 digit.

Algoritma vernam cipher diciptakan oleh Mayor J. Maugbornedan G. Vernam yang merupakan algoritma berjenis symetric key, algoritma ini menggunakan stream cipher yang berasal dari hasi XOR antara bit plaintext dan bit key. Dalam metode ini plaintext diubah ke dalam kode ASCII dan kemudian dilakukan operasi XOR terhadap kunci yang sudah diubah ke dalam kode ASCII (Sholeh, 2011). Modifikasi algoritma vernam cipher dalam penelitian ini yaitu dengan merubah plaintext dengan bilangan biner hasil dari proses enkripsi pada metode sebelumnya yaitu pada caesar cipher kemudian dilakukan operasi XOR terhadap kunci yang sudah diubah ke dalam bilangan biner.

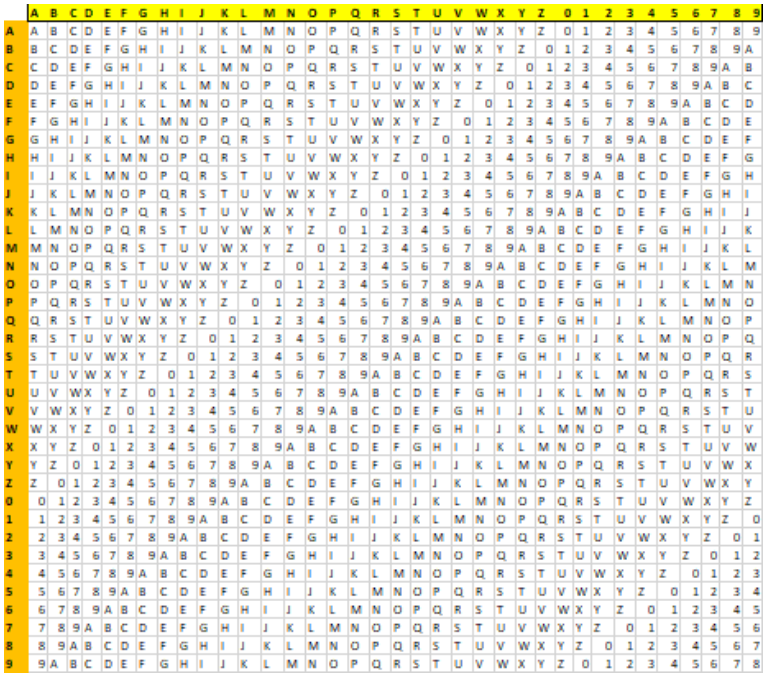
Algoritma hill cipher termasuk algorima kriptografi klasik yang termasuk dalam sistem kriptografi kriptografi polialfabetik dengan menggunakan 26 huruf dalam bahasa Inggris, yang berkorespondensi dengan 0 sampai 25. Hill cipher terdapat beberapa kekurangan karena algoritmanya dirancang hanya dapat mengenkripsi karakter alfabet saja. Ciphertext yang dihasilkan dari proses enkripsi hill cipher berupa karakter abjad dan jumlah elemen ciphertext sama dengan jumlah elemen plaintext[6]. Dalam penelitian ini metode hill cipher dilakukan perhitungan padamatriksp (pergeseran) dengan ordo 2*2denganblokmatriks plaintextberordo 1*2 kemudian hasil perkalian matrik dilakukan konversi ke karakter dan hex. Hasil konversi yang berupa hex akan menjadi inputan dalam melakukan menyembunyian pesan dalam gambar menggunakan algoritma steganografi LSB.

2. METODE PENELITIAN

2.1. Metode Vigenere Cipher

Vigenere cipher merupakan suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso yang berbasis karakter, maka kunci yang digunakan biasanya berupa kata atau kalimat [1]. Teknik untuk menghasilkan ciphertext dilakukan dengan melakukan substitusi angka maupun bujur sangkar Vigenere. Pada bujur sangkar Vigenere, setiap baris yang diperoleh dengan Caesar cipher dan setiap kolom menunjukan kunci. Vigenere cipher menggunakan suatu kunci yang memiliki panjang tertentu. Panjang kunci tersebut bisa lebih pendek maupun sama panjang dengan plaintext, jika kunci lebih pendek dari plaintext maka kunci tersebut akan dilakukan perulangan sepanjang plaintext tersebut [3].

Dalam penelitian ini dilakukan modifikasi terhadap algoritma vigenere cipher yaitu dengan menambahkan angka 0-9 pada setiap baris dan kolomnya. Berikut ini adalah bujursangkar vigenere yang telah dimodifikasi.



Gambar 1. Modifikasi vigenere cipher

Contoh modifikasi vigenere cipher adalah sebagai berikut :
Plaintext : AMIKOM
Key : YOGYA
Ciphertext :Y0O8OA

2.2. Metode Caesar Cipher

Metode enkripsi dalam caesar cipher ini merupakan enkripsi berjenis subtitusi, dimana setiap huruf pada plaintextnya diganti dengan huruf lain. Misalnya dengan pergeseran 2 langkah, A akan digantikan dengan C, dan B akan digantikan dengan D dan begitu seterusnya [4].

Proses enkripsi dalam penelitian ini dilakukan dengan merubah setiap huruf pada plaintext (ciphertext hasil dari metode vigenere cipher) dengan bilangan biner kemudian dilakukan pergeseran 3 digit ke kanan pada setiap hurufnya.

Proses enkripsi pada metode caesar cipher adalah sebagai berikut :

Plaintext : Y0O8OA
Pergeseran : 3 bit ke kanan
Merubah Plaintext dan kunci pergeseran menjadi data biner sebagai berikut :

Biner : 01011001 00110000 01001111 00111000 01001111 01000001

Kemudian lakukan proses enkripsi data dengan melakukan pergeseran pada bilangan biner plaintext sebanyak 3 digit ke arah kanan. Berikut adalah hasil konversi ke dalam bilangan biner :

Plaintext	:	Y	0	O	8	O	A
Biner	:	01011001	00110000	01001111	00111000	01001111	01000001
Hasil	:	00101011	00000110	11101001	00000111	11101001	00101000

2.3. Vernam Cipher

Pada tahun 1917 Mayor J. Maugbornedan G. Vernam menciptakan algoritma kriptografi yang disebutVernam Cipher. Vernam cipher merupakan algoritma berjenis symetric key atau kunci

simetris yang artinya kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan stream cipher yang berasal dari hasi XOR antara bit plaintext dan bit key. Dalam metode ini plaintext diubah kedalam kode ASCII dan kemudian dilakukan operasi XOR terhadap kunci yang sudah diubah ke dalam kode ASCII (Sholeh, 2011).

Modifikasi algoritma vernam cipher dalam penelitian ini yaitu dengan merubah plaintext dengan bilangan biner hasil dari proses enkripsi pada metode sebelumnya yaitu pada caesar cipher kemudian dilakukan operasi XOR terhadap kunci yang sudah diubah ke dalam bilangan biner.

Proses XOR dengan kunci YOGYA adalah sebagai berikut :

00101011	00000110	11101001	00000111	11101001	00101000
01011001⊕	01001111⊕	01000111⊕	01011001⊕	01000001⊕	01011001⊕
01110010	01001001	10101110	01011110	10101000	01110001

Hasil XOR dengan kunci YOGYA kemudian diubah ke dalam bentuk desimal

Tabel 1. Hasil convert Desimal

Hasil XOR	Desimal
01110010	114
01001001	73
10101110	174
01011110	94
10101000	168
01110001	113

2.4. Metode Hill Cipher

Algoritma hill cipher termasuk algorima kriptografi klasik yang termasuk dalam sistem kriptografi kriptografi polialfabetik dengan menggunakan 26 huruf dalam bahasa Inggris, yang berkorespondensi dengan 0 sampai 25 [6]. Pada metode hill cipher dilakukan pembuatan matrik p yaitu matrik dari pergeseran pada metode caesar cipher (pergeseran 3) sebagai berikut :

$$p = \begin{bmatrix} p & p-1 \\ p+1 & p+2 \end{bmatrix}$$

$$p = \begin{bmatrix} 3 & 3-1 \\ 3+1 & 3+2 \end{bmatrix}$$

$$p = \begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix}$$

Kemudian dilakukan perhitungan pada matriks p (pergeseran) dengan blok matriks plaintext sebagai berikut :

$$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 114 \\ 73 \end{bmatrix} = \begin{bmatrix} 488 \\ 821 \end{bmatrix} \bmod 255 = \begin{bmatrix} 233 \\ 56 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 174 \\ 94 \end{bmatrix} = \begin{bmatrix} 710 \\ 1166 \end{bmatrix} \bmod 255 = \begin{bmatrix} 200 \\ 146 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 168 \\ 113 \end{bmatrix} = \begin{bmatrix} 730 \\ 1237 \end{bmatrix} \bmod 255 = \begin{bmatrix} 220 \\ 217 \end{bmatrix}$$

Kemudian ubah bilangan decimal hasil perhitungan matriks di atas menjadi karakter dan bilangan hexadecimal.

Tabel 2. Hasil konversi desimal

Decimal	Hex	Karakter
233	E9	é
56	38	8
200	c8	È
146	92	
220	0D	
217	D9	

Jadi ciphertext untuk kata “AMIKOM” dengan kunci “YOGYA” mengahasilkan é8È

Proses dekripsi pesan dilakukan dengan melakukan perkalian invers matrik p dengan blok matrik ciphertext.

$p = \begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix}$ $_{det}k = (3*5) – (2*4)$

invers modulo:	Mencari p=n sehinggahasil x
7^{-1} mod 255	adalahbilanganbulat.
7x=1 mod 255	k=0; x=(1+255*0)/7 = 1/7
7x=1+255k	k=1; x=(1+255*1)/7 = 36.6
x =(1+255k)/7	k=2; x=(1+255*2)/7 = 73

Sehingga invers dari 7 mod 255 ekuivalen dengan 73 mod 255 yaitu 73.

Invers modulo determinan digunakan untuk mencari invers matriks.

$p = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ maka k^{-1}= determinan $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Sehingga :

$$p^{-1} = 73 \begin{bmatrix} 5 & -2 \\ -4 & 3 \end{bmatrix} = \begin{bmatrix} 365 & -146 \\ 218 & 219 \end{bmatrix} \text{ mod } 255 \rightarrow \begin{bmatrix} 110 & 109 \\ 218 & 219 \end{bmatrix}$$

Setelah matrik p di-invers, maka selanjutnya adalah mengalikan matrik p dengan ciphertext.

$$\begin{bmatrix} 110 & 109 \\ 218 & 219 \end{bmatrix} \begin{bmatrix} 233 \\ 56 \end{bmatrix} = \begin{bmatrix} 31734 \\ 63058 \end{bmatrix} \text{ mod } 255 = \begin{bmatrix} 114 \\ 73 \end{bmatrix}$$

$$\begin{bmatrix} 110 & 109 \\ 218 & 219 \end{bmatrix} \begin{bmatrix} 200 \\ 146 \end{bmatrix} = \begin{bmatrix} 37914 \\ 75574 \end{bmatrix} \text{ mod } 255 = \begin{bmatrix} 174 \\ 94 \end{bmatrix}$$

$$\begin{bmatrix} 110 & 109 \\ 218 & 219 \end{bmatrix} \begin{bmatrix} 220 \\ 217 \end{bmatrix} = \begin{bmatrix} 47853 \\ 95483 \end{bmatrix} \text{ mod } 255 = \begin{bmatrix} 168 \\ 113 \end{bmatrix}$$

Kemudian lakukan konversi desimal ke biner sebagai berikut :

Tabel 3. Hasil Konversi Desimal ke Biner

Desimal	Biner
114	01110010
73	01001001
174	10101110
94	01011110
168	10101000
113	01110001

Kemudian hasil konversi biner dilakukan XOR dengan kunci sebagai berikut :

01110010	01001001	10101110	01011110	10101000	01110001
01011001⊕	01001111⊕	01000111⊕	01011001⊕	01000001⊕	01011001⊕
00101011	00000110	11101001	00000111	11101001	00101000

Hasil XOR terhadap kunci digeser ke kiri sebanyak 3 bit

Tabel 4. Pergeseran Bit

Hasil XOR	Hasil Pergeseran
00101011	01011001
00000110	00110000
11101001	01001111
00000111	00111000
11101001	01001111
00101000	01000001

Kemudian hasil XOR yang sudah digeser di lakukan konversi ke tabel ASCII

Tabel 5. Hasil Konversi ke ASCII

Hasil XOR	Karakter ASCII
01011001	Y
00110000	0
01001111	O
00111000	8
01001111	O
01000001	A

Dari hasil konversi yang diperoleh kemudian di dekripsikan mengggunakan tabel vigenere cipher sehingga diperoleh plaintext sebagai berikut :

Tabel 6. Hasil Proses Vigenere Cipher

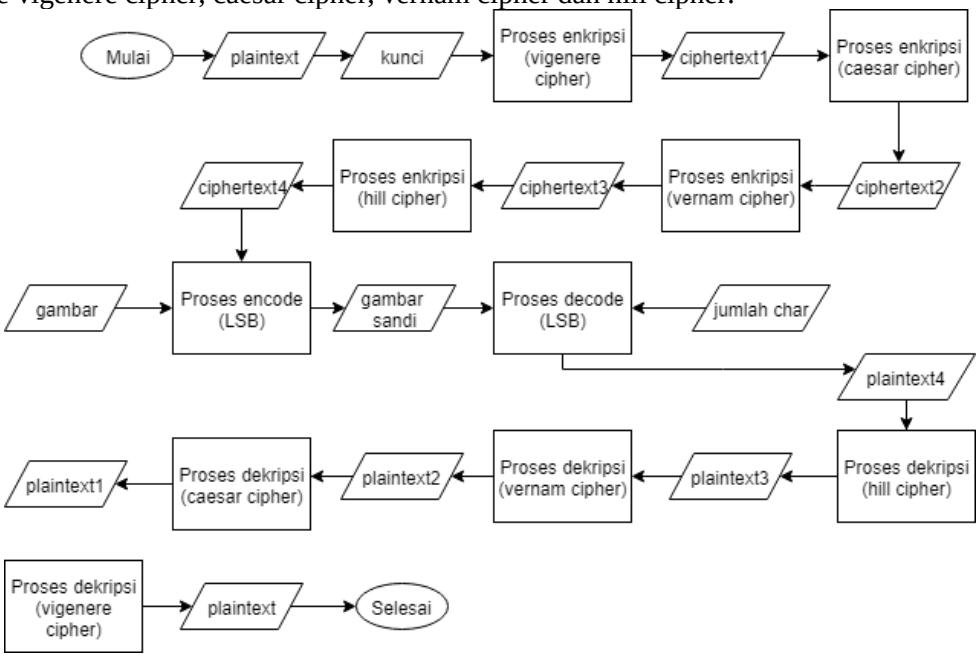
Karakter ASCII	Plaintext
Y	A
0	M
O	I
8	K
O	O
A	M

2.5. LSB (Least Significant Bit)

Dalam sistem steganografi terdapat dua langkah proses yaitu peoses penyembunyian (embedding) dan proses ekstraksi data dari berkas. Penyembunyian data dapat dilakukan dengan mengganti bit – bit data di dalam segmen citra dengan bit – bit data rahasia. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), terdapat bit yang paling berarti atau most significant bit (MBS) dan bit yang paling kurang berarti atau least significant bit (LBS).Bit yang cocok untuk diganti yaitu bit LSB karena perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya [2].Dalam penelitian ini penyembunyian pesan dilakukan dengan menyisipkan pesan pada bit terakhir pada gambar.

2.6. Metode Penelitian

Tujuan penelitian ini adalah untuk menganalisis penyembunyian pesan pada sebuah gambar dengan proses enkripsi data menggunakan modifikasi dan kombinasi algoritma vigenere cipher, caesar cipher, vernam cipher dan hill cipher untuk meningkatkan keamnaan data. Untuk mencapai tujuan tersebut maka terdapat beberapa tahapan atau proses enkripsi dan dekripsi untuk meningkatkan keamanan pesan atau text. Berikut ini adalah proses kriptografi dengan modifikasi metode vigenere cipher, caesar cipher, vernam cipher dan hill cipher.



Gambar 2. Alur Proses Kriptografi Modifikasi

Pada gambar 2 proses kriptografi dengan kombinasi 4 metode yaitu vigenere cipher, caesar cipher, vernam cipher dan hill cipher dan proses penyembunyian pesan pada gambar menggunakan LSB. Proses pertama pesan asli (plaintext) dienkripsi menggunakan vigenere cipher dan menghasilkan pesan sandi (ciphertext1), setelah itu dienkripsi kembali menggunakan caesar cipher dan menghasilkan ciphertext2 kemudian dienkripsi kembali menggunakan vernam cipher menghasilkan ciphertext3 kemudian dienksipsi kembali menggunakan metode hill cipher menghasilkan ciphertext4 kemudian dilakukan proses penyembunyian pesan (encode) menggunakan steganografi LSB dengan memasukan gambar dan chipertext4 menghasilkan gambar sandi. Untuk proses encode gmbar dilakukan dengan memasukan gambar sandi dan memasukan jumlah karakter pesan yang disembunyikan menghasilkan ciphertext4 (hasil ekstrak), kemudian ciphertext4 dilakukan proses dekripsi menggunakan metode hill cipher menghasilkan plaintext3, selanjutnya hasil plaintext3 dilakukan proses dekripsi menggunakan metode vernam cipher menghasilkan plaintext2, kemudian plaintext2 dilakukan proses dekripsi menggunakan metode caesar chiper menghasilkan plaintext1, hasilnya kemudian dilakukan proses dekripsi kembali menggunakan metode vigenere cipher menghasilkan plaintext atau pesan asli.

3. HASIL DAN PEMBAHASAN

3.1 Proses Enkripsi

Proses kriptografi dengan modifikasi metode vigenere cipher, caesar cipher, vernam cipher dan hill cipher dilakukan dengan membuat pesan yang akan dienkripsi dan membuat sebuah kunci sebagai proses penyandian.

Contoh pesan yang akan dienkripsi adalah kata “sel” dengan kunci “3”. Tahap pertama yaitu melakukan enkripsi pesan menggunakan metode vigenere cipher. Adapun prosesnya adalah sebagai berikut :

Plaintext : sel→ karena berjumlah ganjil maka ditambahkan 1 karakter pada plaintext menjadi selg

Kunci : 3

Ciphertext1 : L7E9

Kemudian lakukan proses enkripsi pada ciphertext1dengan menggunakan metode caesar cipher dengan mengganti atau merubah ciphertext1 ke dalam bentuk biner kemudian lakukan pergeseran sebanayak 3 bit, dapat dilihat pada tabel 1.

Tabel 7. Konversi plaintext ke biner dan pergeseran

Ciphertxt1	Konversi Biner	Ciphertext2
L	01001100	10001001
7	00110111	11100110
E	01000101	10101000
9	00111001	00100111

Proses selanjutnya yaitu hasil ciphertext2 (hasil persegeran) dilakukan proses enkripsi menggunakan metode vernam cipher yaitu dilakukan proses XOR dengan kunci sebagai berikut :

10001001	11100110	10101000	00100111
00110011⊕	00110011⊕	00110011⊕	00110011⊕
10111010	11010101	10011011	00010100

Setelah didapatkan hasil XOR maka proses selanjutnya yaitu merubah data biner menjadi desimal sehingga menghasilkan ciphertext3 sebagai berikut :

Taber 8. Hasil Konversi biner ke desimal

Biner	Desimal
10111010	186
11010101	213
10011011	155
00010100	20

Pada Tabel 3 dapat dilihat hasil ciphertext3 dengan ciphertext berupabilangan desimal yang akan diproses enkripsi kembali dengan metode Hill Cipher. Dalam metode Hill Cipher, ciphertext3digunakan dalam bentuk matriks di mana matriks yang digunakan adalah 1x2 dengan dilakukan prosers perkalian dengan matrik p (pergerseran) yaitu 3. Agar pergeseran 3 dapat digunakan maka rubah dalam bentuk matrik sebagai berikut :

$$p = \begin{bmatrix} p & p-1 \\ p+1 & p+2 \end{bmatrix}$$

$$p = \begin{bmatrix} 3 & 3-1 \\ 3+1 & 3+2 \end{bmatrix}$$

$$p = \begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix}$$

Proses perkalian dengan matrik p sebagai berikut :

$$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 186 \\ 213 \end{bmatrix} = \begin{bmatrix} 984 \\ 1809 \end{bmatrix} \bmod 255 = \begin{bmatrix} 219 \\ 24 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 155 \\ 20 \end{bmatrix} = \begin{bmatrix} 505 \\ 720 \end{bmatrix} \bmod 255 = \begin{bmatrix} 250 \\ 210 \end{bmatrix}$$

Kemudian ubah bilangan decimal hasil perhitungan matriks di atas menjadi karakter sebagai berikut :

Tabel 9. Konversi Desimal ke Hex

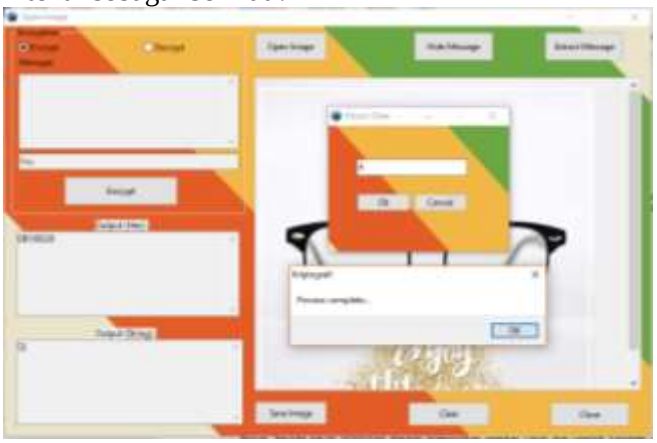
Desimal	Hex
219	DB
24	18
250	83
210	28

Gambar 3. Hasil Enkripsi Pesan

Proses selanjutnya yaitu melakukan encode menggunakan steganografi LSB, yaitu dengan memasukan hasil chipertext4 kedalam gambar sehingga menghasilkan gambar sandi sebagai berikut :

Gambar 4. Proses Encode

Proses decode pesan dilakukan dengan memasukan gambar sandi dan jumlah karakter pesan sehingga muncul plaintext4 sebagai berikut :



Gambar 5. Proses Decode

Untuk dekripsi pesan dilakukan dengan melakukanperkalianpada invers matrikspdenganblokmatrikciphertext4sebagaiberikut :

$$\begin{bmatrix}110 & 109\\218 & 219\end{bmatrix}\begin{bmatrix}219\\24\end{bmatrix} = \begin{bmatrix}2616\\52998\end{bmatrix} \bmod 255 = \begin{bmatrix}186\\213\end{bmatrix}$$

$$\begin{bmatrix}110 & 109\\218 & 219\end{bmatrix}\begin{bmatrix}250\\210\end{bmatrix} = \begin{bmatrix}50390\\100490\end{bmatrix} \bmod 255 = \begin{bmatrix}155\\20\end{bmatrix}$$

Kemudian melakukan konversi bilangan desimal ke bilangan biner sebagai berikut :

Tabel 10. Konversi Desimal ke Biner

Desimal	Biner
186	10111010
213	11010101
155	10011011
20	00010100

Kemudian hasil konversi bilangan biner dilakukan XOR dengan pergeseran yaitu 3 (dirubah ke dalam bentuk biner) sebagai berikut :

10111010	11010101	10011011	00010100
00110011⊕	00110011⊕	00110011⊕	00110011⊕
10001001	11100110	10101000	00100111

Hasil XOR kemudian digeser sebanyak 3 digit ke kanan sebagai berikut

Tabel 11. Hasil Pergeseran Biner

Hasil XOR	Hasil Pergeseran
10001001	01001100
11100110	00110111
10101000	01000101
00100111	00111001

Kemudian kunci yang sudah digeser dilakukan konversi ke tabel ASCII sehingga menghasilkan plaintext2 sebagai berikut :

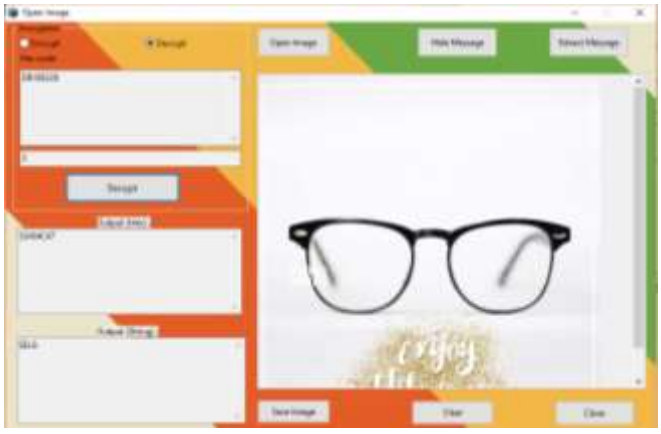
Tabel 12. Hasil konversi biner ke karakter

Biner	Karakter
01001100	L
00110111	7
01000101	E
00111001	9

Proses selanjutnya yaitu melakukan dekripsi hasil plaintext2 dengan metode vigenere cipher sehingga diperoleh ciphertext sebagai berikut :

Tabel 13. Hasil Dekripsi Vigenere Cipher

Karakter	Plaintext
L	S
7	E
E	L
9	G



Gambar 6. Hasil Proses Dekripsi

4. KESIMPULAN

Dari hasil penelitian dapat diambil beberapa kesimpulan antara lain :

1. Metode vigenere cipher, caesar cipher, vernam cipher dan hill cipher merupakan algoritma kriptografi klasik dan cukup kuat jika dilakukan modifikasi.
2. Kombinasi metode vigenere cipher, caesar cipher, vernam cipher dan hill cipher ini hanya membutuhkan 1 kunci untuk melakukan proses enkripsi dan dekripsi.
3. Proses steganografi dapat dilakukan dengan menyembunyikan pesan pada digit terakhir gambar pada RGB.

UCAPAN TERIMA KASIH

Terimakasih kepada seluruh pihak yang telah membantu dalam menyelesaikan penelitian ini, sehingga dapat dipublikasikan.

DAFTAR PUSTAKA

[1] Arrijal, I. M. A., Efendi, R., & Susilo, B. (2016). Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks. Jurnal Pseudocode, 3(1), 69-82.

[2] Hidayat, E. Y., & Hastuti, K. (2013). Analisis Steganografi Metode Least Significant Bit (LSB) dengan Penyisipan Sekuensial dan Acak Secara Kuantitatif dan Visual. Techno. Com, 12(3), 157-167.

[3] Octavianingrum, M., Siambaton, D. A., &Dewi, A. F. K. (2018). ModifikasiVigenere Cipher Dengan Kunci Geser Metode Enkripsi Blok. Prosiding Sendika, 4(1).

[4] Puspita, K., &Wayahdi, M. R. (2015, February). Analisis Kombinasi Metode Caesar Cipher, Vernam Cipher, Dan Hill Cipher Dalam Proses Kriptografi. In Jurnal Seminar Nasional Teknologi Informasidan Multimedia.

[5] Sholeh, M., & Hamokwarong, J. V. (2011). Aplikasi Kriptografi Dengan Metode Vernam Cipher dan Metode Permutasi Biner. Momentum, 7(2).

[6] Wowor, A. D. (2013). Modifikasi Kriptografi Hill Cipher Menggunakan Convert Between Base. SESINDO 2013, 2013.