Journal of Informatics Management and Information Technology
ISSN XXXX-XXXX (Media Online)
Vol 1, No 1, Januari 2021
Hal 13-22
https://hostjournals.com/jimat

Penyembunyian Pesan Teks Tersandi dengan Algoritma Massey Omura Pada Gambar Berdasarkan Metode Stegano F5

Herianata Barasa

Program Studi Teknik Informatika Universitas Budi Darma, Medan, Indonesia
Email: heryianata1223@gmail.com

Abstrak−Pada era komputerisasi saat ini mengamankan data merupakan hal yang sangat penting dilakukan terutama pada data yang bersifat rahasia. Karena jika sempat terjadi pembobolan data misalnya pada pesan yang berisi teks rahasia maka akan merugikan yang berkepentingan. Oleh sebab itu dibutuhkan suatu sistem yang dapat mengamankan pesan teks tersebut. Semakin ketat pengamanan data tersebut maka semakin kecil kemungkinan untuk dibobol. Dalam penelitian ini penulis akan mengkombinasikan dua buah metode dalam pengamanan pesan teks. Yakni metode *Massey Omura* dan Metode *Stegano* F5. Penulis akan menggunakan metode *Massey Omura* untuk menyandikan pesan yang kemudian disembunyikan pada gambar dengan metode *Stegano* F5. Algoritma *Massey Omura* merupakan salah satu algoritma yang bekerja dengan dengan konsep kunci asimetris dan dikembangkan berdasarkan konsep protokol tiga-*pass*. Protokol *three-pass* bekerja dengan konsep bahwa setiap pihak (penerima dan pengirim pesan) menggunakan kunci mereka sendiri untuk melakukan proses mengenkripsi dan mendekripsi pesan. Salah satu keuntungan dari algoritma *Massey Omura* ialah kesulitan menghitung logaritmik diskrit yang mirip dengan algoritma kunci publik lainnya seperti RSA, dan lainnya. Dan Stegano F5 merupakan versi yang sangat awal untuk menanamkan file ke dalam gambar BMP, GIF, atau JPEG warna asli. Penggabungan algoritma Massey Omura dengan metode Stegano F5, akan menjadikan sangat kecil kemungkinan pihak lain dapat membobol pesan yang bersifat rahasia.

Kata Kunci: Dekripsi; Enkripsi; Pengamanan Data; Massey Omura; Stegano F5

Abstract−In the current era of computerization, securing data is a very important thing to do, especially on confidential data. Because if there was data breach, for example in messages containing secret text, it would be detrimental to those concerned. Therefore we need a system that can secure these text messages. The tighter the data security is, the less likely it is to be compromised. In this study the authors will combine two methods in securing text messages. Namely the Massey Omura method and the Stegano F5 method. The author will use the Massey Omura method to encode messages which are then hidden in the image using the Stegano F5 method. The Massey Omura algorithm is an algorithm that works with the concept of asymmetric keys and is developed based on the concept of a three-pass protocol. The three-pass protocol works with the concept that each party (recipient and sender of the message) uses their own key to encrypt and decrypt messages. One of the advantages of the Massey Omura algorithm is the difficulty of calculating discrete logarithmic which is similar to other public key algorithms such as RSA, and others. And Stegano F5 is a very early version for embedding files into native color BMP, GIF, or JPEG images. The combination of the Massey Omura algorithm with the Stegano F5 method, will make it very unlikely that other parties can break into confidential messages.

Keywords: Decryption; Encryption; Data Security; Massey Omura; Stegano F5

1. PENDAHULUAN

Perkembangan teknologi saat ini sangat bermanfaat bagi masyarakat baik tua maupun kaum muda. Dengan semakin berkembangnya dunia komunikasi, maka semakin banyak pertukaran informasi yang terjadi dengan berbagai media komunikasi. Dalam melakukan beberapa pertukaran informasi perlu adanya perlindungan terhadap informasi seperti pesan teks yang bersifat rahasia, misalnya pesan yang berisi rencana tindakan kriminal. Pesan teks itu dapat diamankan dengan teknik kripto, namun kelemahannya mudah menimbulkan kecurigaan bila dilihat hasilnya[1], sehingga perlu dioptimalkan keamanannya.

Dalam penelitian ini file yang akan diamankan berupa pesan teks menggunakan metode *Massey Omura*. Algoritma Mas*sey Omura* adalah salah satu algoritma yang bekerja dengan konsep asimetris dan dikembangkan berdasarkan konsep protocol tiga-*pass. Protocol three-pass* bekerja dengan konsep bahwa setiap (penerima dan pengirim pesan) menggunakan kunci mereka sendiri untuk melakukan proses mengenkripsi dan mendekripsi pesan.

Teknik lain yang dapat digunakan untuk mengamankan *file* adalah *steganografi*. Kata *steganografi* terdiri dari 2(dua) penggalan kata yaitu steganos dan *graphein* yang berarti "tulisan tersembunyi"[2]. Stegano sendiri merupakan suatu ilmu yang mempelajari bagaimana cara menyembunyikan suatu pesan rahasia pada suatu media sehingga hanya pihak terkait saja yang mengetahui isi pesan rahasia tersebut. Steganografi menyediakan format media digital untuk penyisipan pesan yang beragam seperti format *image* (*jpeg, bitmap, dan gif*), format *audio (wav, voc, dan mp3)*, dan format lain seperti teks *file*, html, pdf, dan lain-lain[2].

Untuk menghindari kecurigaan *steganografi* dapat diterapkan pada media yang umum digunakan pada pertukaran data digital, yaitu media citra digital. Gambar adalah sebuah perpaduan antara titik, garis, bidang dan warna untuk mencitrakan sesuatu. Pada kehidupan sehari-hari masyarakat sering *sharing* gambar melalui media *chatting.* Format citra digital yang digunakan yaitu citra dengan format JPEG. Citra JPEG yang telah disisipi pesan rahasia tidak terlihat berbeda secara kasat mata, maka dari itu mengurangi tingkat kecurigaan pihak yang tidak bertanggung jawab. Format JPEG (*Joint Photographic Experts Group*) saat ini format yang paling umum menyimpan data gambar. Kompresi dengan JPEG menggunakan beberapa proses, yaitu DCT (*Descrete Cosine Transform*), kuantisasi, dan penyandian entropi (*Huffman Coding*).

ISSN XXXX-XXXX (Media Online)
Vol 1, No 1, Januari 2021
Hal 13-22
https://hostjournals.com/jimat

Pada penelitian ini penulis menggunakan metode F5 yang merupakan perbaikan dari algoritma F3 dan F4 oleh peneliti yang sama yaitu Andreas Westfeld. Kelebihan dari algoritma adalah penyebaran pesan lebih merata keseluruh media citra penampung (*cover-image*) karena menggunakan permutasi sehingga keberadaan pesan sulit untuk dideteksi, selain itu F5 menawarkan kapasitas penyimpanan data besar dengan proporsi pesan yang ditampung sebesar 13% dari citra penampungnya. Algoritma F5 dapat mencegah serangan statistik *Permutative Stradding* dan *Matric Encoding*.

2. METODOLOGI PENELITIAN

2.1 Keamanan Data

Keamanan data salah satu aspek terpenting dari sebuah sistem komunikasi. Apalagi dalam komunikasi data dan informasi pada era komputerisasi sekarang dibutuhkan sistem keamanan data untuk melindungi data dan informasi. Kemajuan sistem komunikasi. Informasi saai ini sudah menjadi komoditas yang sangat penting bahkan ada yang mengatakan bahwa kita telah berada disebuah *information-based society*, hal ini dimungkinkan karena adanya perkembangan pesat dalam teknologi komputer dan telekomunikasi atau sering disebut *end computing* yang mendorong penggunaan komputer adalah meningkatnya pengetahuan manusia tentang komputer yang banyaknya mengakses informasi yang tersedia, prangkat keras yang murah dan mudahnya ditemukan dipasaran.

Banyak hal yang perlu diperhatikan dalam hal keamanan komunikasi data salah satunya adalah penyadapan yang dilakukan pihak ketiga untuk kepentingan data, terjadinya pencurian data tanpa sepengetahuan pemilik. Sehingga manusia untuk menyembunyikan data dengan melakukan enkripsi terhadap data rahasia dengan mengunakan berbagai macam cara diantaranya adalah steganografi merupakan ilmmu yang mempelajari tentang penyisipan atau penyembunyian data, kriptografi adalah ilmu yang mempelajari tentang penyandian atau keamanan data dengan membuat kunci data.

2.2 Kriptografi

Kriptografi (*Cryptography*) berasal dari bahasa Yunani yaitu "*Cryptos*" artinya "*secret*"(rahasia) dan "*graphein*" artinya "*writing*" (tulisan). Jadi, Kriptografi berarti "*secret writing*"(tulisan rahasia). Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan yang dikirim sipengirim sampai dengan aman pada si penerima pesan.

3. HASIL DAN PEMBAHASAN

Asumsikan pengirim dan penerima sedang *online* dan menggunakan aplikasi obrolan. Keduanya telah menyetujui bilangan prima lebih besar dari 256, misalnya, p = 97.
Bangkitkan bilangan prima 97 dan dilakukan pengecekan apakah bilangan tersebut merupakan bilangan prima atau bukan dengan cara berikut:

a. Pilih sebuah bilangan a dimana 1<a<97.
b. Misalkan nilai random yang terpilih untuk nilai a adalah 2.
c. Hitung nilai L (*Legendre*), dimana $L = a^{(p-1)/2} \bmod p$, dimana p = 97.
   $L = a^{(p-1)/2} \bmod p$
   $= 2^{(97-1)/2} \bmod 97$
   $= 1$

Maka : 97 adalah prima

1. Pengirim memilih eA, dimana 1 <eA <p - 1 dan eA *co-prime* dengan p – 1
   a. Asumsikan eA = 5 , karena 5 adalah *co-prime* dengan 97. Nilai eA digunakan dalam proses enkripsi.
   b. Pengirim menghitung kebalikan dari eA berdasarkan persamaan (1), dan menyimpan dalam dA. Asumsikan dA = 77, digunakan dalam proses enkripsi.
2. Penerima menghitung eB, di mana 1 <eB <p - 1 dan eB *co-prime* dengan p-1
   a. Asumsikan eB = 11, karena 11 adalah *co-prime* dengan 97. Nilai eB digunakan dalam proses enkripsi.
   b. Penerima menghitung kebalikan dari eB berdasarkan persamaan (3), dan menyimpan dalam dB Diasumsikan dB = 35 mod 97 = 1 memenuhi syarat. Nilai dB digunakan dalam proses dekripsi.

3.1 Proses Enkripsi Pada Massey Omura

Secara umum, ada tiga proses dalam algoritma *massey-omura* yaitu proses menghasilkan kunci publik dan kunci privat, proses enkripsi dan dekripsi. Langkah-langkah algoritma *Massey-Omura*, adalah:

1. Penerima dan pengirim telah menyetujui nilai prima (p) yang lebih besar (mis.>256)
2. Pengirim (langkah pertama)
   a. Menentukan nilai yang digunakan untuk melakukan proses enkripsi pertama. Diasumsikan eA di mana 1 <eA <p - 1 dan eA adalah co-prime dengan p - 1
   b. Hasilkan kunci dekripsi dengan mencari kebalikan dari nilai eA berdasarkan persamaan: dA x eA (mod p - 1) = 1 (1)

ISSN XXXX-XXXX (Media Online)
Vol 1, No 1, Januari 2021
Hal 13-22
https://hostjournals.com/jimat

c. Lakukan proses enkripsi pertama ke pesan untuk menghasilkan C1 berdasarkan pada persamaan: C1 = MeA mod p (2)
d. Hasil cipher (C1) dikirim ke penerima.

3. Penerima (langkah kedua)
   a. Menentukan nilai yang digunakan untuk melakukan proses enkripsi kedua. Diasumsikan eB di mana 1 <eB <p - 1 dan eA adalah co-prime dengan p - 1
   b. Hasilkan kunci dekripsi dengan mencari kebalikan dari nilai dB berdasarkan pada persamaan: dB x eB (mod p - 1) = 1 (3)
   c. Lakukan proses enkripsi kedua ke C1 untuk menghasilkan C2 berdasarkan pada persamaan: $C2 = C1^{eB}$ mod p (4)
   d. C2 dikirim ulang ke pengirim.
4. Pengirim (langkah ketiga)
   a. Terima C2 dari penerima
   b. Enkripsi C2 (langkah enkripsi ketiga) dan tetapkan sebagai C3, berdasarkan pada persamaan: $C3 = C2^{dA}$ mod p (5)
   c. Kirim ulang C3 (sandi akhir) ke penerima
5. Penerima (langkah keempat)
   a. Terima C3 (sebagai pesan yang telah dienkripsi) dari pengirim
   b. Dekripsi C3 (pesan dari pengirim) berdasarkan pada persamaan: $M = C3^{dB}$mod p (6)

c. Hasil proses dekripsi C3 adalah pesan asli dari pengirim.

Anggap pengirim mengirim pesan ke penerima menggunakan aplikasi obrolan dan pesan aslinya adalah "HERIANATA"

1. Pengirim mengonversi karakter pesan ke nilai ASCII, jadi:
   H = 72 E = 69 R = 82 I = 73 A = 65 N = 78A = 65 T = 84 A = 65
2. Enkripsi setiap karakter pesan berdasarkan persamaan (2).
   Untuk H: 72^5 mod 97 = 44
   Untuk E: 69^5 mod 97 = 51
   Untuk R: 82^5 mod 97 = 38
   Untuk I: 73^5 mod97 = 9
   Untuk A: 65^5 mod 97 = 2
   Untuk N: 78^5 mod 97 = 20
   Untuk A : 65^5 mod 97 = 2
   Untuk T : 84^5 mod 97 =23
   Untuk A : 65^5 mod 97 =26
   Jadi, dihasilkan C1 = 44,51,38, 9, 2, 20, 2, 23, 26, jikadikonversi ke karakter C1 = , , 3, &, AT, STX, DC4, STX, ETB, STX.
3. Pengirim mengirim C1 ke penerima.
4. Receiver mengenkripsi C1 berdasarkan persamaan (4)
   Untuk ,: 44^{11} mod 97 = 49
   Untuk 3: 51^{11} mod 97 = 77
   Untuk & :38^{11} mod 97 = 83
   Untuk AT :9^{11} mod 97 = 43
   Untuk STX :2^{11} mod 97 = 11
   Untuk DC4 : 20^{11} mod 97 =55
   Untuk STX :2^{11} mod 97 =11
   Untuk ETB :23^{11} mod 97 =90
   Untuk STX :26^{11} mod 97 =84
   Jadi , menghasilkan C2 = 49, 77, 83, 43, 11, 55, 11, 90, 84.
5. Penerima mengirim C2 ke pengirim
6. Pengirim mengenkripsi C2 berdasarkan pada persamaan (5) dan menghasilkan C3
   Untuk 49^{77} mod 97 =3
   Untuk 77^{77} mod 97 =19
   Untuk 83^{77} mod 97 =68
   Untuk 43^{77} mod 97 =93
   Untuk 11^{77} mod 97 =66
   Untuk 55^{77}mod 97 =63
   Untuk 11^{77} mod 97 =66
   Untuk 90^{77} mod 97 =10
   Untuk 84^{77} mod 97 =76
   Jadi, dihasilkan C3 = 3, 19, 68, 93, 66, 63, 66, 10, 76jika dikonversi ke karakter akan dihasilkan C3 = ETX, DC3, D,], B, ?, B, LF, L.
7. C3 adalah sandi dari pesan asli dari pengirim yang akan dikirim ke penerima.

ISSN XXXX-XXXX (Media Online)
Vol 1, No 1, Januari 2021
Hal 13-22
https://hostjournals.com/jimat

3.2 Penyisipan Pesan Pada Gambar

Berikut ini diuraikan contoh algoritma *Massey Omura* dalam mengamankan sebuah teks dan disisipkan dengan metode *stegano* F5 pada sebuah gambar berwarna.

Gambar 1. *Plain Image* Dengan Resolusi 1544 x 1027

Berdasarkan *plain image* diatas, akan diambil 8 x 8 pixel sebagai sampel dalam perhitungan manual. Lima *pixel* tersebut akan diambil nilai desimal warna pada setiap elemen warna *pixel*nya.

Gambar 2. *Plain Image* Sampel Sebanyak 8 Pixel

Nilai elemen warna dari delapan *pixel plain image* sampel diatas diambil dengan menggunakan *software* matlab, sehingga diperoleh:

70	81	80	110	150	172	167	92
100	73	61	103	135	141	127	94
138	122	92	95	121	137	101	84
141	148	130	108	111	124	91	82
154	144	146	135	113	105	93	79
162	143	148	150	127	98	104	107
161	156	164	163	128	67	69	98
152	162	178	168	125	64	45	49

Gambar 3. Matriks Original

Proses transformasi DCT dimulai dengan membagi *citra* menjadi beberapa blok dengan ukuran 8 x 8 piksel/blok, blok-blok piksel tersebut masing-masing diproses menjadi 64 koefisien DCT. Berikut adalah rumus yang digunakan untuk memproses 1 blok 8 x 8 piksel dengan DCT :

$$F(u,v) = \frac{C(u)C(u)}{4} \sum_{i}^{7}{}_{u} . \sum_{j}^{7}{}_{v} \cos\frac{(2i+1)u\pi}{16} \cos\frac{(2j+1)v\pi}{16} f(i,j) \quad \text{.....(1)}$$

Keterangan :

$f(i,j)$ = matrix input dengan panjang i, dengan lebar j

$F(u, v)$ = hasil proses det dengan panjang u, dan lebar v

DCT hanya dapat memproses koefisien yang nilainya antara -127 dan 127. Oleh karenanya, masing – masing koefisien dari *matrix* sebelumnya dikurangi 128 sehingga mendapatkan hasil sebagai berikut:

-58	-47	-48	-18	22	44	39	-36
-28	-55	-67	-25	7	13	-1	-34
10	-6	-36	-33	-7	9	-27	-44
13	20	2	-20	-17	-4	-37	-46
26	16	18	7	-15	-23	-35	-49
34	15	20	22	-1	-30	-24	-24
33	28	36	35	0	-61	-99	-30
24	34	50	40	-3	-64	-83	-79

Gambar 4. Matriks M

Kemudian menghitung nilai matriks DCT untuk matriks T dan matriks *transpose* untuk matriks T’ dengan rumus :

ISSN XXXX-XXXX (Media Online)
Vol 1, No 1, Januari 2021
Hal 13-22
https://hostjournals.com/jimat

$$T(i,j) = \begin{cases} \frac{1}{\sqrt{N}} & Jika\ i = 0 \\ \sqrt{\frac{2}{N}}\ \cos\frac{(2j+1)i\pi}{2N} & Jika\ i \neq 0 \end{cases}$$

Dengan menggunakan rumus matriks diatas dapat dihitung nilai matriks T mulai dari T (0,0) sampai T (7,7) sebagai berikut:

T (0,0) = $\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{8}}$ = 0,03536
T (0,1) = $\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{8}}$ = 0,03536
T (0,2) = $\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{8}}$ = 0,03536
T (0,3) = $\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{8}}$ = 0,03536
T (0,4) = $\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{8}}$ = 0,03536
T (0,5) = $\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{8}}$ = 0,03536
T (0,6) = $\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{8}}$ = 0,03536
T (0,7) = $\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{8}}$ = 0,03536
T (1,0) = $\sqrt{\frac{2}{8}}$ Cos $\frac{(2.0+1)1.180^0}{2.8}$ = 0,4909
T (1,1) = $\sqrt{\frac{2}{8}}$ Cos $\frac{(2.1+1)1.180^0}{2.8}$ = 0,4157
T (1,2) = $\sqrt{\frac{2}{8}}$ Cos $\frac{(2.2+1)1.180^0}{2.8}$ = 0,2778
T (1,3) = $\sqrt{\frac{2}{8}}$ Cos $\frac{(2.3+1)1.180^0}{2.8}$ = 0,0975
T (1,4) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.4+1)1.180^0}{2.8}$ = -0,0975
T (1,5) = $\sqrt{\frac{2}{8}}$ Cos $\frac{(2.5+1)1.180^0}{2.8}$ = -0,2778
T (1,6) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.6+1)1.180^0}{2.8}$ = -0,4157
T (1,7) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.7+1)1.180^0}{2.8}$ = -0,4904
T (2,0) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.0+1)2.180^0}{2.8}$ = 0,4619
T (2,1) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.1+1)2.180^0}{2.8}$ = 0,1913
T (2,2) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.2+1)2.180^0}{2.8}$ = -0,1913
T (2,3) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.3+1)2.180^0}{2.8}$ = -0,4619
T (2,4) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.4+1)2.180^0}{2.8}$ = -0,4619
T (2,5) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.5+1)2.180^0}{2.8}$ = -0,1913
T (2,6) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.6+1)2.180^0}{2.8}$ = 0,1913
T (2,7) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.7+1)2.180^0}{2.8}$ = 0,4619
T (3.0) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.0+1)3.180^0}{2.8}$ = 0,4157
T (3.1) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.1+1)3.180^0}{2.8}$ = -0,0975
T (3.2) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.2+1)3.180^0}{2.8}$ = -0,4904
T (3.3) = $\sqrt{\frac{2}{8}}$Cos $\frac{(2.3+1)3.180^0}{2.8}$ = -0,2778

ISSN XXXX-XXXX (Media Online)
Vol 1, No 1, Januari 2021
Hal 13-22
https://hostjournals.com/jimat

T (3.4) = $\sqrt{\frac{2}{8}}\text{Cos}\ \frac{(2.4+1)3.180^0}{2.8}$ = 0,2778

T (3.5) = $\sqrt{\frac{2}{8}}\text{Cos}\ \frac{(2.5+1)3.180^0}{2.8}$ = 0,4904

T (3.6) = $\sqrt{\frac{2}{8}}\text{Cos}\ \frac{(2.6+1)3.180^0}{2.8}$ = 0,0975

T (3.7) = $\sqrt{\frac{2}{8}}\text{Cos}\ \frac{(2.7+1)3.180^0}{2.8}$ = -0,4157 Sampai ke- T (7,7).

Dari perhitungan diatas maka diperoleh nilai untuk matriks T sebagai berikut:

0,3536	0,3536	0,3536	0,3536	0,3536	0,3536	0,3536	0,3536
0,4904	0,4157	0,2778	0,0975	−0,0975	−0,2778	−0,4157	−0,4904
0,4619	0,1919	−0,1913	−0,4619	−0,4619	−0,1913	0,1913	0,4619
0,4157	−0,0975	−0,4904	−0,2778	0,2778	0,4904	0,0975	−0,4157
0,3536	−0,3536	−0,3536	0,3536	0,3536	−0,3536	−0,3536	0,3536
−0,2778	−0,4904	0,0975	0,4157	−0,4157	−0,0975	−0,4904	−0,2778
0,1913	−0,4619	0,4619	−0,1913	−0,1913	0,4619	−0,4619	0,1913
0,0975	−0,2778	0,4157	−0,4904	0,4904	−0,4157	0,2778	−0,0975

Gambar 5. Matriks Transform

0,3536	0,4904	0,4619	0,4157	0,3536	−0,2778	0,1913	0,0975
0,3536	0,4157	0,1919	−0,0975	−0,3536	−0,4904	−0,4619	−0,2778
0,3536	0,2778	−0,1913	−0,4904	−0,3536	0,0975	0,4619	0,4157
0,3536	0,0975	−0,4619	−0,2778	0,3536	0,4157	−0,1913	−0,4904
0,3536	−0,0975	−0,4619	0,2778	0,3536	−0,4157	−0,1913	0,4904
0,3536	−0,2778	−0,1913	0,4904	−0,3536	−0,0975	0,4619	−0,4157
0,3536	−0,4157	0,1913	0,0975	−0,3536	−0,4904	−0,4619	0,2778
0,3536	−0,4904	0,4619	−0,4157	0,3536	−0,2778	0,1913	−0,0975

Gambar 6 Matriks Transpose

Berikutnya adalah tahap menghitung matriks D, dimana matriks D akan digunakan untuk kuantisasi lanjutan. Dengan rumus, D = T.M.T^t

-58	-58	-58	-58	-58	-58	39	-36
-28	-55	-67	-25	7	13	-1	-34
10	-6	-36	-33	-7	9	-27	-44
13	20	2	-20	-17	-4	-37	-46
26	16	18	7	-15	-23	-35	-49
34	15	20	22	-1	-30	-24	-24
33	28	36	35	0	-61	-99	-30
24	34	50	40	-3	-64	-83	-79

0,3536	0,3536	0,3536	0,3536	0,3536	0,3536	0,3536	0,3536
0,4904	0,4157	0,2778	0,0975	-0,0975	-0,2778	-0,4157	-0,4904
0,4619	0,1919	-0,1913	-0,4619	-0,4619	-0,1913	0,1913	0,4619
0,4157	-0,0975	-0,4904	-0,2778	0,2778	0,4904	0,0975	-0,4157
0,3536	-0,3536	-0,3536	0,3536	0,3536	-0,3536	-0,3536	0,3536
-0,2778	-0,4904	0,0975	0,4157	-0,4157	-0,0975	-0,4904	-0,2778
0,1913	-0,4619	0,4619	-0,1913	-0,1913	0,4619	-0,4619	0,1913
0,0975	-0,2778	0,4157	-0,4904	0,4904	-0,4157	0,2778	-0,0975

Gambar 7. Perkalian Matriks T dengan M

T(0,0)=(-58*0,3536)+(47*0,2778)+(48*0,4619)+(18*0,4157)+(22*0,3536)+(44*-0,2278)+(39*0,1913)+(-36*0,0975)
= 20.1912

T(0,1)=(-58*0,3536)+(47*0,4157)+(48*0,1919)+(18*0,0975)+(22*0,3536)+(44*-0,4904)+(39*0,4619)+(-36*0,2778)
= 47,330

T(0,2)=(-58*0,3536)+(47*0,2778)+(48*0,1913)+(18*0,4904)+(22*0,3536)+(44*-0,975)+(39*-0,4619)+(-36*-0,4157)
= 58,187

T(0,3)=(-58*0,3536)+(47*0,0975)+(48*0,4619)+(18*0,2778)+(22*0,3536)+(44*-0,4157)+(39*-0,1913)+(-36*0,4904)
= 12,2

T(0,4)=(-58*0,3536)+(47*0,0975)+(48*0,4619)+(18*0,2778)+(22*0,3536)+(44*-0,4157)+(39*-0,1913)+(-36*0,4904)
= 12,2

T(0,5)=(-58*0,3536)+(47*0,2778)+(48*0,1913)+(18*0,4904)+(22*0,3536)+(44*-0,0975)+(39*0,4619)+(-36*-0,4157)
= 48,603

Lakukan perhitungan tersebut sampai dengan T(7,7), setelah dilakukan perhitungan tersebut, maka akan terdapat hasil seperti gambar pada tabel berikut ini:

20,19	47,33	58,18	12,2	12,2	48,60	-31,84	63,16
11	-30,32	-34,10	58,08	58,08	-43,10	13,83	36,34
-14,27	-7,12	-41,54	14,55	-7,26	-36,38	-15,70	7,66
-21,23	53,08	-22,25	36,46	36,46	-22,25	-2,93	-12,43
5,09	38,03	-33,15	35,47	-30,93	33,22	35,56	5,91
22,14	26,92	-16,91	3,07	-4,59	140,01	10,48	17,76
61,90	-49,09	47,05	41,32	-22,68	77,63	-41,27	22,46
-12,72	88,27	-6.19	-108,2	-14,24	-14,24	-10,77	6,82

Gambar 8. Nilai Hasil DCT

ISSN XXXX-XXXX (Media Online)
Vol 1, No 1, Januari 2021
Hal 13-22
https://hostjournals.com/jimat

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	58	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Gambar 9. Matriks Quantisasi

Untuk mendapatkan hasil DCT terkuantisasi, lakukan pembagian hasil perhitungan DCT dengan matriks quantisasi. Sehingga diperoleh hasil sebagai berikut:

1,2	4,3	6	0,7	1	2	-1	1,03
1	-3	-2,4	3,05	2,2	-1	0,2	1
-1,01	-1	-3	1	-0,1	-1	-0,2	0,1
-2	3,1	-1,01	1,2	1	-0,2	-0,03	-0,2
0,2	2	-1	1	-0,4	0,3	4	-0,07
1	1	-0,3	0,04	-0,05	1,3	0,09	0,1
1,2	-1	0,6	0,4	-0,2	1	-0,3	0,2
-0,1	1	-0,06	-1,1	-0,1	-0,1	-0,1	0,06

Gambar 10. Matriks Hasil DCT Terkuantisasi

Untuk tahap penyisipan cari terlebih dahulu informasi posisi bit yang akan diganti dari linier D. Dengan rumus:

$$b(i,j)\begin{cases} i > 0; C(i,j) \bmod 2 \\ i < 0; (c-1) \bmod 2 \end{cases}$$

Sampel *chiper* yang akan disipkan diambil 5 digit yang diubah kedalam bentuk biner.
Chiper:
ETX = 0000 0011
DC3 = 0001 0011
D = 0100 0100
] = 0101 1101
B =0100 0010
Disisipkan ke citra yang telah diubah dalam bentuk biner:

D1 = 0111 0000
D2 = 1000 0001
D3 = 1000 0000
D4 = 1000 0000
D5 = 1010 0000
D6 = 1011 1001
D7 = 1011 0111 1
D8 = 1001 0010
D9 = 0 0000 0000
D10 = 0111 0011
D11 = 0110 0000
D12 = 1 0000 0011
D13 = 1 0011 0101
D14 = 1 0100 0001
D15 = 1 0010 1111
D16 = 1001 0100
D17 = 1 0011 1000
D18 = 1 0010 0010
D19 = 1001 0011
D20 = 1001 0100
D21 = 1 0010 0001
D22 = 1 0011 0110
D23 = 1 0000 0001
D24 = 1000 0100

D25 = 1 0100 0011
D26 = 1 0100 0000
D27 = 1 0010 0000
D28 = 1 0000 1000
D29 = 1 0001 0011
D30 = 1 0010 0000
D31 = 1001 0001
D32 = 1000 0011
D33 = 1 0101 0101
D34 = 1 0100 0100
D35 = 1 0100 0111
D36 = 1 0011 0101
D37 = 1 0001 0111
D38 = 1 0000 0101
D39 = 1001 0011
D40 = 0111 1000
D41 = 1 0110 0010
D42 = 1 0100 0111
D43 = 1 0100 1000
D44 = 1 0101 0000
D45 = 1 0010 0111
D46 = 1001 1000
D47 = 1 0000 0100
D48 = 1 0000 0111

D49 = 1 0110 0001
D50 = 1 0101 0110
D51 = 1 0110 0100
D52 = 1 0110 0011
D53 = 1 0010 1000
D54 = 0110 0111
D55 = 0110 1001
D56 = 1001 1000
D57 = 1 0101 0010
D58 = 1 0110 0010
D59 = 1 0111 1000
D60 = 1 0110 1000
D61 = 1 0010 0101
D62 = 0110 0100
D63 = 0100 0101
D64 = 0100 1001

ISSN XXXX-XXXX (Media Online)
Vol 1, No 1, Januari 2021
Hal 13-22
https://hostjournals.com/jimat

56	129	128	128	160	185	367	146
0	115	96	259	309	321	303	148
312	290	147	148	289	310	257	132
323	320	288	264	275	288	145	131
341	324	655	309	279	261	147	120
354	327	328	336	295	152	260	263
353	342	356	355	296	103	105	152
338	354	576	293	293	100	69	1

Gambar 11. Matriks *SteganoImage*

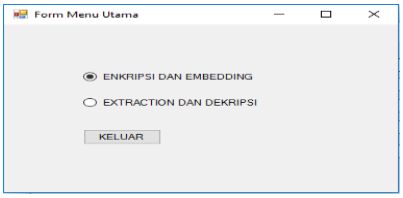
Nilai *pixel* akhir dari *citra cover* dirubah menjadi 1 sebagai penanda bahwa citra cover tersebut telah tersisipkan pesan. Pada *citra cover* yang telah disisipi pesan atau disebut *steganoimage* terjadi perubahan warna seperti gambar 3.15 dibawah ini:

Gambar 12. *Citra Steganoimage*

3.3 Implementasi Program

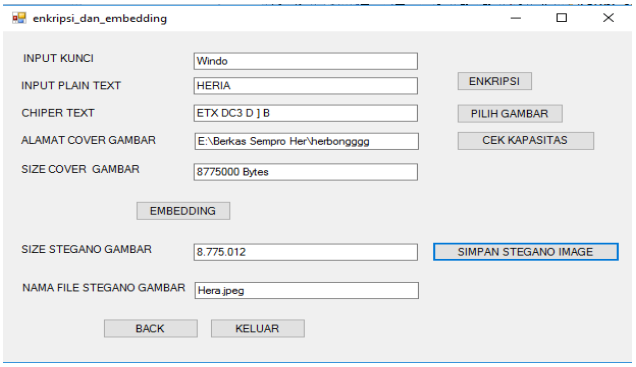
a. Form Menu Utama

Menu pilihan yang disediakan *form* menu utama adalah, *form* dekripsi dan *embedding*, *form Extraction* dan deskripsi seperti pada gambar 13 dibawah ini :



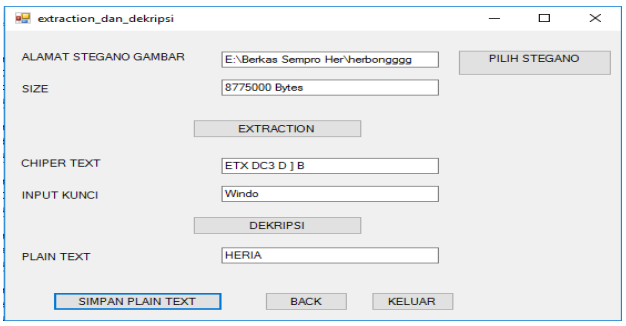
Gambar 13. Tampilan *form* Menu Utama

b. Form Menu Enkripsi dan Embedding



Gambar 14. *Form* Enkripsi dan *Embedding*

c. Form Extraction dan Dekripsi



Gambar 14. *Form Extraction* dan Dekripsi

3.4 Pengujian Sistem

Berdasarkan hasil pengujian system yang dilakukan maka didapatkan hasil dimana ukuran *gambar* asli dengan *steganoimage* mengalami perubahan yang siknifikan karena teks yang disisipkan hanya pada nilai bit gambar tertentu, berikut merupakan beberapa tabel hasil pengujian sistem yaitu pengujian proses penyisipan dan *extraction*.

1. Pengujian Proses *Embedding*
   Dalam proses pengujian *embedding* penyusun mengambil tiga sampel sebagai bahan untuk pengujian pada tabel berikut:

No	Plainteks	Size	Kunci Enkripsi	Chiperteks	Cover Image	Size	Steganoimage	Size	Ket
1	HERIA	13 Byte	Windo	ETX DC3 D] B	Hera.jpg	8775000 Bytes	Hera.jpg	8.875.101 2 Bytes	Sukses
2	SUZAN E	20 Byte	Mokkol	DC B T B] ^	Zane.jpg	456000 Bytes	Zane.jpg	405000 Bytes	Gagal
3	Ayam	15 Byte	Kokok	B ^ B J	Aya.jpg	150000 Bytes	Aya.jpg	160000 Bytes	Sukses

Gambar 15. Proses Pengujian *Embedding*

Setelah dilakukan proses *embedding* dengan menggunakan tiga *gambar* yang berbeda dan *plainteks* yang berbeda, maka pada pengujian sampel didapatkan hasil prosesnya gagal karena jumlah bit gambar yang bernilai 456000 dan 406000 lebih sedikit dari jumlah biner *cipherteks* yang akan disisipkan, proses *embedding* akan berjalan lancar apabila jumlah bit pada gambar yang bernilai 456000 dan 406000 minimal sama banyaknya dengan nila bit *cipherteks* yang akan disisipkan.

2. Pengujian Proses *Extraction*
   Pengujian proses *extraction* merupakan proses pengambilan biner dari dalam bit gambar, proses pengujian ini diambil lima sampel yang sebelumnya telah dilakukan *embedding* dengan kunci dan *plaintext* yang berbeda seperti tabel berikut.

No	Nama Steganoimage	Size	Kunci Steganoimage	Plainteks	Kunci Extraction	Size	Ket
1	Hera.jpg	8.875.101 Bytes	Windo	HERIA	Windo	13 Byte	Sukses
2	Aya.jpg	150000 Bytes	Kokok	Ayam	Kokok	15 Byte	Sukses
3	Bunga.jpg	140000 Bytes	-	-	-	13 Byte	Gagal
4	Zane.jpg	456000 Bytes	Mokkol	SUZANE	-	20 Byte	Gagal

Gambar 16. Tabel Proses Pengujian *Extraction*

Dari hasil pengujian *extraction* pada tabel diatas terdapat *extraction* yang gagal, hal ini diakibatkan nilai biner *cipherteks* lebih banyak dari jumlah nilai gambar sehingga *embedding* tidak berjalan lancar, kata kunci yang digunakan saat *extraction* salah sehingga pengujian *extraction* tidak dapat berjalan dengan lancar Setiap *embedding* yang dilakukan dan sukses maka proses pengujian *extraction* juga sukses, jika *embedding* gagal maka *extraction* juga gagal.

4. KESIMPULAN

Kesimpulan yang diperoleh berdasarkan implementasi dan pengujian yang telah dilakukan algoritma *Massey Omura* dapat menyandikan sebuah *file* dengan konsep *Three-pass Protocol.* Metode F5 dapat digunakan untuk menyisipkan pesan rahasia kedalam citra berwarna dengan format .jpg. Citra yang dihasilkan (*stego-image*) secara kasat mata tidak jauh berbeda antara *cover-image* dan *stego-image*. Waktu *encode* pesan bergantung dengan resolusi *cover-image*. Semakin besar resolusi *cover-image*, maka dibutuhkan waktu *encode* pesan lebih lama. *Stego-image* tidak tahan terhadap berbagai manipulasi citra, seperti pemberian efek *Blur*, merotasi *citra*, merubah ukuran (*scalling*), dan memotong citra (*cropping*). Stego-image akan gagal ketika di-*decode* untuk mengambil pesan.

REFERENCES

[1] A. Massey-omura, M. Reza, M. A. Budiman, and D. Arisandi, “Simulasi Pengamanan File Teks Menggunakan,” vol. 1, no. 1, pp. 20–27, 2012.
[2] T. Zebua, R. K. Hondro, and E. Ndruru, “Message Security on Chat App based on Massey Omura Algorithm,” vol. 1, no. 2, pp. 16–23, 2018.
[3] I. Pendahuluan, “PENGAMANAN APLIKASI CHATTING MENGGUNAKAN METODE,” vol. 12, no. September, pp. 295–300, 2017.
[4] R. Munir, “ALGORITMA ENKRIPSI CITRA DIGITAL DENGAN KOMBINASI DUA CHAOS,” *Chaos*, 2012.
[5] P. M. Perangkat Lunak Enkripsi Pesan Dengan Metode Paillier Cryptosystem Reinhard Simbolon, R. M. Simbolon, and K.

Kunci, "PERANCANGAN PERANGKAT LUNAK ENKRIPSI PESAN DENGAN METODE PAILLIER CRYPTOSYSTEM," *Pelita Inform. Budi Darma*, 2013.

[6] A. Rohmanu, "Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End Of File Ajar Rohmanu," *J. Inform. SIMANTIK*, vol. 1, no. 2, pp. 1–11, 2017.

[7] V. M. Amal and A. R. Yohannis, "Aplikasi Steganografi," pp. 77–88.

[8] G. D. A, R. M. Rumani, M. Nasrun, and S. Prodi, "IMPLEMENTASI KRIPTOGRAFI DAN STEGANOGRAFI PADA MEDIA GAMBAR MENGGUNAKAN ALGORITMA BLOWFISH DAN METODE LEAST SIGNIFICANT BIT CRYPTOGRAPHY AND STEGANOGRAPHY IMPLEMENTATION IN IMAGE USING BLOWFISH ALGORITHM AND LEAST SIGNIFICANT BIT METHOD," vol. 2, no. 2, pp. 3762–3769, 2015.

[9] M. Magdalena, N. A. Putra, and E. P. Widiyanto, "Implementasi Algoritme F5 untuk Penyisipan Pesan Rahasia pada Citra Digital," pp. 1–14.

[10] D. Suhartono, A. G. Salman, and C. Octavianus, "Aplikasi Penyembunyian Pesan Pada Citra Jpeg Dengan Algoritma F5 Dalam Perangkat Mobile Berbasis Android," vol. 2012, no. Snati, pp. 15–16, 2012.

[11] E. Pramunanto, Y. Perwira, A. Putra, and A. Zaini, "Penulisan Pesan Tersembunyi Pada Citra JPEG dengan Metode F5," vol. 10, no. 2, pp. 1–8, 2012.

[12] T. N. Sianturi and R. G. Hutagaol, "Penyisipan Pesan Rahasia Kedalam Audio Menggunakan Algoritma F5," pp. 890–893, 2019.