P-ISSN: 2548-9704
E-ISSN: 2686-0880

IMPLEMENTASI ALGORITMA OTP DAN STEGANOGRAFI EOF DALAM PENYISIPAN PESAN TEKS PADA CITRA

Muhammad Arief [1], Magdalena Simanjuntak[2], I Gusti Prahmana[3]

Mahasiswa Program Studi Teknik Informatika, STMIK KAPUTAMA Binjai
Jl. Veteran No. 4A-9A, Binjai 20714, Sumatera Utara
www.kaputama.ac.id // e-mail: info@kaputama.ac.id

ABSTRAK

Penggunaan informasi media citra mempunyai beberapa kelemahan, salah satunya adalah mudahnya dimanipulasi oleh pihak-pihak tertentu dengan bantuan teknologi yang berkembang sekarang ini. Upaya yang dapat dilakukan dalam peningkatan pengamanan pengiriman informasi citra adalah kriptografi, yaitu ilmu dan seni untuk menjaga keamanan pesan. Pada penelitian ini diterapkan metode *One Time Pad* dan *Stegnografi End Of File* yang bertujuan untuk memperoleh *cipher* yang lebih kuat dengan menyisipkan pesan kedalam citra sehingga susah untuk di sadap. Algoritma *One Time Pad* untuk mengenkripsi dan dekripsi, *Stegnografi End Of File* yang digunakan untuk mengencoding dan mendecoding citra. Hasil dari penelitian ini menunjukkan bahwa dengan menerapkan algoritma *One Time Pad* dan *Stegnografi End Of File* dapat mengamankan pesan yang disisipkan kedalam citra dan mengamankan kunci untuk kebutuhan data. Waktu proses encoding dan decoding di pengaruhi oleh banyaknya pesan yang akan dirahasiakan.

Kata Kunci: Citra, Kriptografi, *One Time Pad*, Pesan, *Stegnografi End Of File.*

1. LATAR BELAKANG MASALAH

Keamanan data dan kerahasiaan data merupakan hal yang sangat penting dalam proses pertukaran pesan ataupun informasi. Hal tersebut diperlukan untuk mengatasi penyadapan ataupun modifikasi pesan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Tanpa adanya jaminan keamanan data dan kerahasiaan data, orang lain dapat dengan mudah mendapatkan pesan atau informasi melalui jaringan internet. Berbagai macam teknik keamanan telah dikembangkan untuk melindungi kerahasiaan data supaya tidak digunakan oleh orang yang tidak berhak, salah satunya adalah teknik Kriptografi. Kriptografi adalah suatu cabang ilmu yang berguna untuk menjaga keamanan dan kerahasiaan data dengan cara mengubah bentuk awal data ke bentuk yang tidak dapat dimengerti lagi maknanya.

Data yang bersifat rahasia perlu di buatkan penyimpanan dan pengiriman yang aman. Data yang telah di enkripsi tidak dapat di buka oleh pihak-pihak yang tidak mengetahui kunci yang digunakan untuk mengenkripsi dan mendekripsi file tersebut. Dengan begitu data akan terproteksi dan akan terhindar dari pihak-pihak yang tidak berkepentingan dan tidak bertanggung jawab yang ingin merusak atau melihat isi data tersebut.

Pada penelitian ini algoritma yang digunakan untuk penyisipan pesan adalah OTP (*One Time Pad*) dan *Steganografi* EOF (*End of File*). Kedua algoritma ini akan digunakan untuk menyisipkan pesan ke dalam citra dan penyisipan pesan akan dibandingkan baik dari segi kecepatan penyisipan, keamanan hasil pesan, lama extraksi pesan.

2. LANDASAN TEORI

P-ISSN: 2548-9704
E-ISSN: 2686-0880

2.1 Kriptografi

Kriptografi telah menjadi bagian penting dalam dunia teknologi informasi, terutama dalam bidang komputer. Hampir semua penerapan teknologi informasi menggunakan kriptografi sebagai alat untuk menjamin keamanan dan kerahasiaan data atau informasi. Karena itu kriptografi menjadi suatu ilmu yang berkembang pesat dan dalam waktu singkat banyak muncul algoritma-algoritma baru yang dianggap lebih unggul daripada algoritma pendahulunya

Sedangkan definisi dalam buku-buku terbaru menyatakan kriptografi merupakan ilmu mengenai metode untuk mengirimkan pesan secara rahasia sehingga hanya penerima yang dimaksud yang dapat menghapus dan membaca pesan tersebut atau memahaminya. Pengertian lain kriptografi yaitu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Kata *graphy* dalam kata *cryptography* itu sendiri sudah menyiratkan sebuah seni.

Jadi, kriptografi adalah suatu ilmu sekaligus seni yang bertujuan untuk menjaga keamanan suatu pesan (*cryptography is the art and science of keeping messages secure*). Secara umum, kriptografi adalah teknik pengamanan informasi dimana informasi diubah dengan kunci tertentu melalui enkripsi sehingga menjadi informasi baru yang tidak dapat dimengerti oleh orang yang tidak berhak menerimanya, dan informasi tersebut hanya dapat di ubah kembali oleh orang yang berhak menerimanya melalui dekripsi (Nurdin, 2017).

2.2 Algoritma OTP (*One Time Pad*)

One-time pad (OTP) adalah suatu cipher aliran yang melakukan setiap enkripsi dan dekripsi satu karakter setiap kali. Algoritma ini ditemukan oleh Major Joseph Mauborgne pada tahun 1917 sebagai perbaikan dari algoritma Vernam cipher untuk menghasilkan keamanan yang lebih sempurna. Mauborgne mengusulkan penggunaan *one-time pad* (pad = kertas bloknot) yang berisi deretan karakter-karakter kunci yang dibuat secara acak. Satu pad hanya digunakan sekali (*one-time*) saja untuk menyandikan suatu pesan, setelah itu pad yang telah digunakan dihancurkan supaya tidak dipakai kembali untuk mengenkripsi pesan yang lain (Fahlevi et al., 2020).

Algoritma *One Time Pad* mempunyai cara kerja dimana penerima pesan mempunya salinan kunci yang sama dan kunci tersebut hanya dipakai satu kali (*one time*) untuk enkripsi dan dekripsi dan setelah digunakan maka pad (kertas *blocknot*)harus segera dihancurkan agar tidak bisa dipakai lagi untuk enkripsi dan dekripsi pesan yang lain.Pengirim dan penerima harus sama sama memiliki satu set materi kunci yang besar dan juga acak, selama kombinasi dari semua pesan yang pernah dikirimkan (Fauzi et al., 2017)

Jadi secara teori alasan OTP tidak dapat dipecahkan jika kuncinya secara sempurna diacak, dirahasiakan dan hanya dipakai sekali saja. Pada algoritma OTP mempunyai panjang kunci yang sama dengan panjang *plaintext.*Sehingga tidak ada kebutuhan untuk mengulang penggunaaan kunci selama proses enkripsi. Pada algoritma OTP mempunyai panjang kunci yang sama dengan panjang *plaintext.* Sehingga tidak ada kebutuhan untuk mengulang penggunaaan kunci selama proses enkripsi (Fauzi et al., 2017)

2.1.1 Teknik Enkripsi Pada Algoritma OTP (*One Time Pad*)

$$Ci = (Pi + Ki) \bmod 256$$

Keterangan :
Ci = Cipherteks (Ciphertext)
Pi = Plainteks (Plaintext)
Ki = kunci (Key)

2.1.2 Teknik Dekripsi Pada Algoritma OTP (*One Time Pad*)

$$Ci=(Pi – Ki) \bmod 256$$

Keterangan :
Ci = Cipherteks (Ciphertext)

P-ISSN: 2548-9704
E-ISSN: 2686-0880

Pi = Plainteks (Plaintext)
Ki = kunci (Key)

2.3 Steganografi

Steganografi (*steganography*) adalah teknik menyembunyikan data rahasia di dalam wadah (media) digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang. Steganografi membutuhkan dua properti yaitu, wadah penampung dan data rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara (audio), teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video.

Penggunaan steganografi antara lain bertujuan untuk menyamarkan eksistensi (keberadaan) data rahasia sehingga sulit dideteksi, dan melindungi hak cipta suatu produk. Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi, data yang telah disandikan (*chiphertext*) tetap tersedia, maka dengan steganografi cipherteks dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya. Data rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti keadaan aslinya.

Kriteria yang harus diperhatikan dalam penyembunyian data adalah:

1. Fidelity
   Mutu citra penampung tidak jauh berubah.Setelah penambahan data rahasia, citra hasil steganografi masih terlihat denganbaik. Pengamat tidak mengetahui kalau didalam citra tersebut terdapat data rahasia.
2. Robustness.
   Data yang disembunyikan harus tahan (*robust*) terhadap berbagai operasi manipulasi yang dilakukan pada citra penampung, seperti pengubahan kontras,
   penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan (cropping), enkripsi, dan sebagainya. Bila pada citra penampung dilakukan operasioperasi pengolahan citra tersebut, maka data yang disembunyikan seharusnya tidak rusak (tetap valid jika diekstraksi kembali).
3. Recovery.
   Data yang disembunyikan harus dapat diungkapkan kembali (*reveal*). Karena tujuan steganografi adalah data hiding, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut (Minarni & Fernando, 2020)

2.4 *End of file* (EOF)

Metode EOF merupakan salah satu metode yang digunakan dalam steganografi. Metode ini menggunakan cara dengan menyisipkan data pada akhir *file*. Sehingga, tidak akan mengganggu kualitas data awal yang akan disisipkan pesan. Namun, ukuran *file* setelah disisipkan pesan rahasia akan bertambah. Sebab, ukuran *file* yang telah disisipkan pesan rahasia sama dengan ukuran *file* sebelum disisipkan pesan rahasia yang disisipkan. Untuk mengenai data yang disisipkan pada akhir *file*, diperlukan suatu tanda pengenal atau simbol pada awal dan akhir data yang akan disisipkan.

EOF menggunakan karakter yang berbeda sebagai penanda awal penyisipan pesan dan penanda akhir penyisipan pesan. Metode EOF menggunakan kelemahan indera manusia yang tidak sensitif sehingga seakan-akan tidak ada perbedaan yang terlihat antara sebelum atau sesudah pesan disisipkan (Maharani et al., 2016).

2.4.1 Teknik Encoding *End Of File* (EOF)

Adapun langkah-langkah encoding menggunakan *End Of File*:

1. Proses encoding dimulai dengan pesan yang akan disisipkan. Pesan diubah kedalam bentuk biner denganrepresentasi 1 atau 0.
2. Kemudian disisipkan angka 1 didepan rangkaian biner tersebut.langkah selanjutnya rangkaian biner tersebut dikonversikan

P-ISSN: 2548-9704
E-ISSN: 2686-0880

menjadi bilangan decimal dan meghasilkan sebuah bilangan yang dinamakan dengan *m.*

3. Menghitung jumlah warna yang terdapat pada berkas RGB yang menjadi objek steganografi dan akan menghasilkan sebuah bilangan. Bilangan tersebut dinamakan dengan In, maka apabila *m>n!-1* maka pesan yang akan disisipkan berukuran terlalu besar sehingga proses penyisipan tidak dapat dilakukan.
4. Warna dalam palet warna diurutkan sesuai dengan urutan "natural". Setiap warna dengan format RGB dikonversikan kedalam bilangan integer dengan aturan (Merah * 65536 + Hijau * 256 + Biru). Kemudian diurutkan berdasarkan besar bilangan integer yang mewakili warna tersebut.
5. Setelah itu lakukan proses iterasi terhadap variable *i* adalah 1 sampai n. Setiap warna dengan urutan *n – i* dipindahkan ke posisi baru yaitu m mod i, kemudian *m* dibagi dengan *i*.
6. Kemudian palet warna yang baru hasil iterasi pada langkah ke-4 dimasukkan kedalam palet warna berkas RGB. Apabila ada tempat yang diisi oleh dua buah warna, maka warna sebelumnya yang menempati tempat tersebut akan digeser satu tempat ke samping.
7. Apabila ternyata besar dari palet warna yang baru lebih kecil dari 256 maka palet warna akan diisi dengan warna terakhir dari palet warna sebelumnya.
8. Kemudian berkas RGB akan dikompresi ulang dengan palet warna yang baru, untuk menghasilkan berkas yang baru (Maharani et al., 2016).

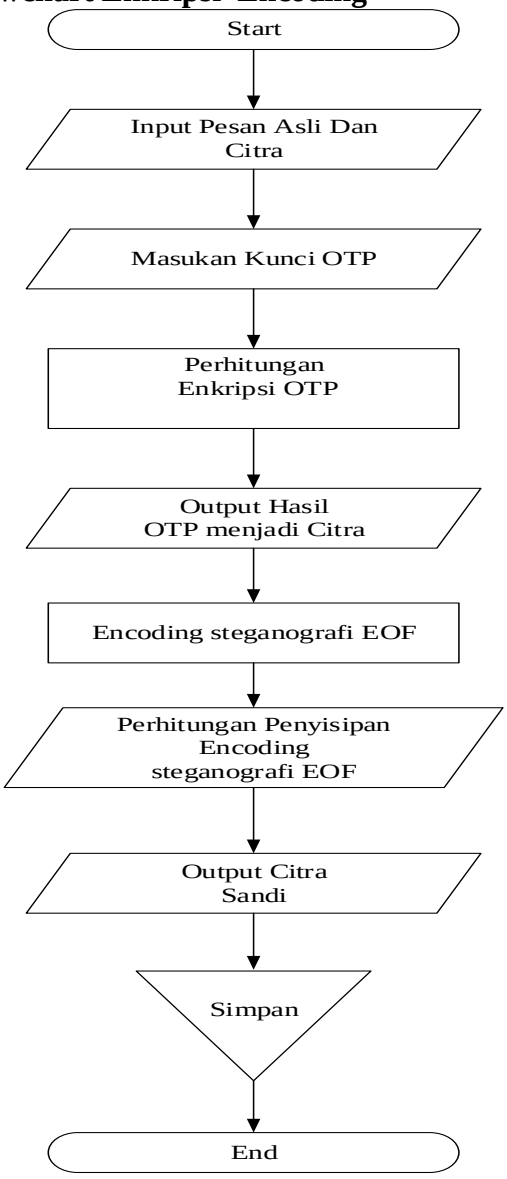
2.4.2 Teknik Decoding *End Of File* (EOF)

Langkah- langkah proses decoding atau mengekstrak pesan dari citra yang telah disisipi pesan dengan EOF adalah sebagai berikut:

1. Menghitung pixel citra yang sudah disisipi pesan kemudian di ubah menjadi bilangan decimal.
2. Melakukan pencarian pesan penanda yang telah disisipkan dalam stegoimage
3. Pesan decimal di ambil dan dipisahkan dengan penanda
4. Pesan decimal di konversikan ke bentuk karakter (Minarni & Fernando, 2020).

3.3 ANALISA DAN PEMBAHASAN

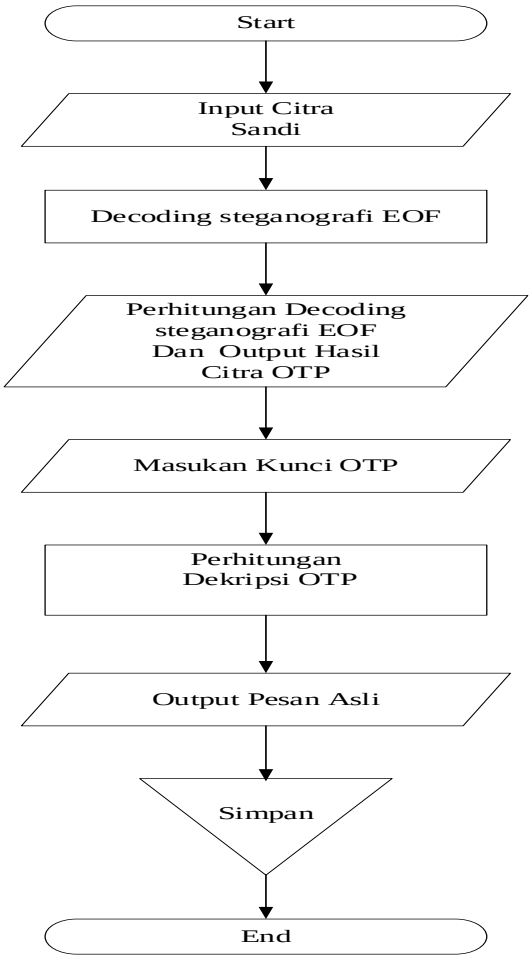
3.1 Flowchart Enkripsi Encoding



Gambar 1 Flowchart Enkripsi Encoding

P-ISSN: 2548-9704
E-ISSN: 2686-0880

3.2 Flowchart Decoding Dekripsi



Gambar 2 Flowchart Decoding Dekripsi

3.3 Perhitungan Enkripsi Pesan Algoritma OTP (*One Time Pad*)

Pada proses enkripsi menyembunyikan pesan bertujuan untuk mengubah pesan asli *(plaintext)* ke bentuk yang rahasia *(ciphertext)*. Contoh perhitungan dengan menggunakan algoritma OTP (*One Time Pad*) adalah sebagai berikut:

Input Pesan : saya sedang skripsi
Kunci : wisuda
char = s = 115
(115 + 119) Mod 256 = 234 = ê
char = a = 97
(97 + 105) Mod 256 = 202 = Ê
char = y = 121
(121 + 115) Mod 256 = 236 = ì
char = a = 97
(97 + 117) Mod 256 = 214 = Ö
char = = 32
(32 + 100) Mod 256 = 132 = „
char = s = 115
(115 + 97) Mod 256 = 212 = Ô
char = e = 101
(101 + 119) Mod 256 = 220 = Ü
char = d = 100
(100 + 105) Mod 256 = 205 = Í
char = a = 97
(97 + 115) Mod 256 = 212 = Ô
char = n = 110
(110 + 117) Mod 256 = 227 = ã
char = g = 103
(103 + 100) Mod 256 = 203 = Ë
char = = 32
(32 + 97) Mod 256 = 129 = •
char = s = 115
(115 + 119) Mod 256 = 234 = ê
char = k = 107
(107 + 105) Mod 256 = 212 = Ô
char = r = 114
(114 + 115) Mod 256 = 229 = å
char = i = 105
(105 + 117) Mod 256 = 222 = Þ
char = p = 112
(112 + 100) Mod 256 = 212 = Ô
char = s = 115
(115 + 97) Mod 256 = 212 = Ô
char = i = 105
(105 + 119) Mod 256 = 224 = à
char = = 32
(32 + 105) Mod 256 = 137 = ‰
char = = 32
(32 + 115) Mod 256 = 147 = “
Kesimpulan = êÊìÖ„ÔÜÍÔãË• êÔåÞÔÔà‰“

3.4 Encoding Penyisipan Pesan Citra *Steganografi End Of File*

P-ISSN: 2548-9704
E-ISSN: 2686-0880

Gambar 3 Toga Wisuda

Pada proses encoding penyisipan pesan bertujuan untuk menyembunyikan pesan rahasia *(ciphertext).* Contoh perhitungan dengan menggunakan *Stegenografi End Of File* adalah sebagai berikut:

pixel(0 , 360)
Red = ê = 11101010 = 234
Green = Ê = 11001010 = 202
Blue = ì = 11101100 = 236

pixel(1 , 360)
Red = Ö = 11010110 = 214
Green = „ = 10000100 = 132
Blue = Ô = 11010100 = 212
pixel(2 , 360)
Red = Ü = 11011100 = 220
Green = Í = 11001101 = 205
Blue = Ô = 11010100 = 212
pixel(3 , 360)
Red = ã = 11100011 = 227
Green = Ë = 11001011 = 203
Blue = • = 10000001 = 129
pixel(4 , 360)
Red = ê = 11101010 = 234
Green = Ô = 11010100 = 212
Blue = å = 11100101 = 229
pixel(5 , 360)
Red = Þ = 11011110 = 222
Green = Ô = 11010100 = 212
Blue = Ô = 11010100 = 212
pixel(6 , 360)
Red = à = 11100000 = 224
Green = ‰ = 10001001 = 137
Blue = “ = 10010011 = 147

3.5 Decoding Penyisipan Pesan Citra *Steganografi End Of File.*

Pada proses Decoding penyisipan pesan bertujuan untuk menampilkan pesan yang tidak rahasia *(plaintext).* Contoh perhitungan dengan menggunakan *Stegenografi End Of File* adalah sebagai berikut:

pixel(0 , 361)
Red = 234 = 11101010 = ê
Green = 202 = 11001010 = Ê
Blue = 236 = 11101100 = ì
pixel(1 , 361)
Red = 214 = 11010110 = Ö
Green = 132 = 10000100 = „
Blue = 212 = 11010100 = Ô
pixel(2 , 361)
Red = 220 = 11011100 = Ü
Green = 205 = 11001101 = Í
Blue = 212 = 11010100 = Ô
pixel(3 , 361)
Red = 227 = 11100011 = ã
Green = 203 = 11001011 = Ë
Blue = 129 = 10000001 = •
pixel(4 , 361)
Red = 234 = 11101010 = ê
Green = 212 = 11010100 = Ô
Blue = 229 = 11100101 = å
pixel(5 , 361)
Red = 222 = 11011110 = Þ
Green = 212 = 11010100 = Ô
Blue = 212 = 11010100 = Ô
pixel(6 , 361)
Red = 224 = 11100000 = à
Green = 137 = 10001001 = ‰
Blue = 147 = 10010011 = “

3.6 Perhitungan Dekripsi Pesan Algoritma OTP (*One Time Pad*)

Pada proses Dekripsi bertujuan untuk mengubah pesan rahasia *(ciphertext)* ke bentuk yang asli (*plaintext*). Contoh perhitungan dengan menggunakan algoritma OTP (*One Time Pad*) adalah sebagai berikut:

Input : êÊìÖ„ÔÜÍÔãË• êÔåÞÔÔà‰“
Kunci : wisuda
char = ê = 234
(234 - 119) Mod 256 = 115 = s
char = Ê = 202
(202 - 105) Mod 256 = 97 = a
char = ì = 236

P-ISSN: 2548-9704
E-ISSN: 2686-0880

(236 - 115) Mod 256 = 121 = y
char = Ö = 214
(214 - 117) Mod 256 = 97 = a
char = „ = 132
(132 - 100) Mod 256 = 32 =
char = Ô = 212
(212 - 97) Mod 256 = 115 = s
char = Ü = 220
(220 - 119) Mod 256 = 101 = e
char = Í = 205
(205 - 105) Mod 256 = 100 = d
char = Ô = 212
(212 - 115) Mod 256 = 97 = a
char = ã = 227
(227 - 117) Mod 256 = 110 = n
char = Ë = 203
(203 - 100) Mod 256 = 103 = g
char = • = 129
(129 - 97) Mod 256 = 32 =
char = ê = 234
(234 - 119) Mod 256 = 115 = s
char = Ô = 212
(212 - 105) Mod 256 = 107 = k
char = å = 229
(229 - 115) Mod 256 = 114 = r
char = Þ = 222
(222 - 117) Mod 256 = 105 = i
char = Ô = 212
(212 - 100) Mod 256 = 112 = p
char = Ô = 212
(212 - 97) Mod 256 = 115 = s
char = à = 224
(224 - 119) Mod 256 = 105 = i
char = ‰ = 137
(137 - 105) Mod 256 = 32 =
char = “ = 147
(147 - 115) Mod 256 = 32 =
Kesimpulan = saya sedang skripsi

4. PEMBAHASAN DAN IMPLEMENTASI

4.1 Pembahasan

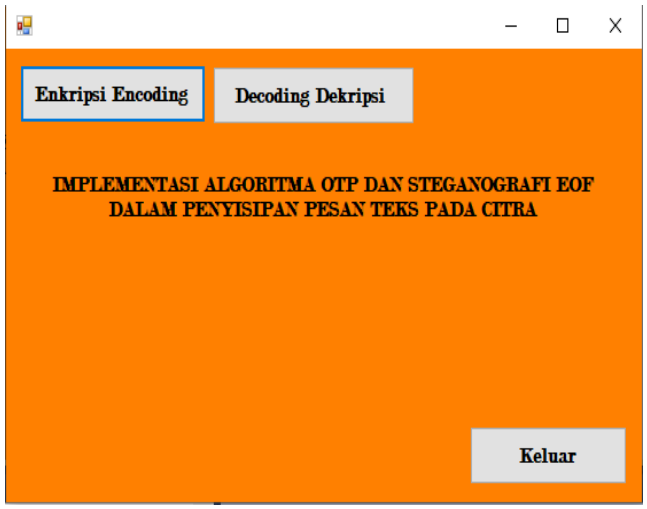
Aplikasi penyisipan pesan pada citra menggunakan metode Algoritma OTP (*One Time Pad*) dan algoritma *Steganografi* EOF (*End Of File)* ini di bangun dengan tujuan menjaga kepemilikan agar tetap aman dari tindakan pencurian. Hal ini di lakukan dengan cara mengenkrip data tersebut dan dapat di dekripsi sebagai pembuktian kepemilikan dari pesan tersebut. Proses enkripsi dan dekripsi harus menggunakan aplikasi dan kunci yang sama.

4.2 Pembahasan Langkah Kerja Aplikasi

Tampilan dari sistem perbaikan citra yang telah dirancang menggunakan aplikasi pemerograman *Visual Basic 2010*, dengan penerapan algoritma OTP *(One Time Pad)* dan *Steganografi* EOF (*End Of File*) dalam penyisipan pesan pada citra, yaitu sebagai berikut:

a. Tampilan Halaman Utama

Tampilan dibawah ini merupakan tampilan menu utama Algoritma OTP Steganografi EOF. Adapun tampilanya yaitu seperti pada gambar dibawah ini :



Gambar 4 Tampilan Halaman Utama

b. Tampilan Halaman Enkripsi Encoding

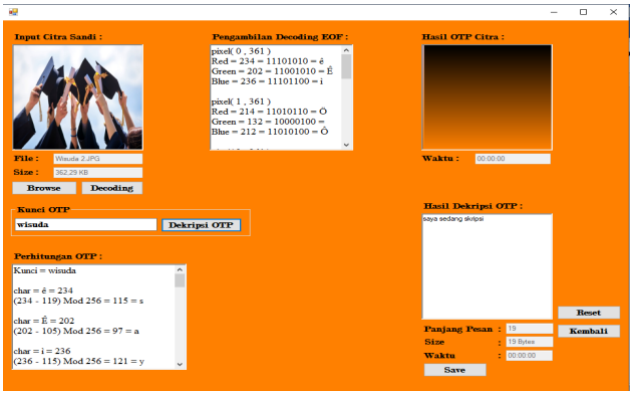
Tampilan form Menu Algoritma OTP Steganografi EOF seperti pada gambar dibawah ini:

P-ISSN: 2548-9704
E-ISSN: 2686-0880

Gambar 5 Tampilan Halaman Enkripsi Encoding

c. Tampilan Halaman Decoding Dekripsi

Tampilan form Menu Algoritma OTP Steganografi EOF seperti pada gambar dibawah ini:



Gambar 6 Tampilan Halaman Decoding Dekripsi

1. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil perancangan dan pembuatan program aplikasi kriptografi menggunakan algoritma OTP (*One Time Pad*) dan *Steganografi* EOF (*End of File*) ini dapat di ambil kesimpulan sebagai berikut:

1. Dalam penyisipan pesan kedalam citra berhasil di terapkan dan mampu melakukan proses enkripsi *encoding* dan *decoding* dekripsi Semakin banyak pesan tersebut maka waktu proses enkripsi *encoding* dan *decoding* dekripsi akan membutuhkan waktu yang lebih lama, Hasil pengujian pada sistem di dapatkan bahwa pesan yang telah mengalami proses enkripsi *encoding* dan *decoding* dekripsi dengan algoritma OTP (*One Time Pad*) dan *Steganografi* EOF (*End of File*), memiliki isi informasi yang sama dengan pesan asli yang telah di sisipkan.
2. Penyisipan pesan pada citra dengan menggunakan algoritma OTP (*One Time Pad*) dan *Steganografi* EOF (*End of File*) untuk merahasiakan pesan berjalan dengan baik. pesan berhasil di sisipkan kedalam citra dengan cara proses enkripsi *encoding* dan *decoding* dekripsi, percobaan yang dilakukan pada OTP (*One Time Pad*) dan *Steganografi* EOF (*End of File*).

5.2 Saran

Adapun saran penulis usulkan dalam pengembangan aplikasi ini adalah sebagai berikut:

1. Sistem yang di buat dalam penelitian ini hanya berbasis desktop, di harapkan pada penelitian berikutnya mampu menerapkan pada perangkat lain seperti android, IOS dan yang lainnya.
2. Aplikasi enkripsi *encoding* dan *decoding* dekripsi masih jauh dari kata sempurna, maka di harpakan kepada pembaca untuk menambah fitur lainnya maka program ini lebih baik dan sempurna.
3. Untuk penelitian lebih lanjut di harapkan dapat mengembangkan sistem yang telah ada untuk dapat melakukan enkripsi encoding dan decoding dekripsi.

DAFTAR PUSTAKA

[1]. Fahlevi, M. R., Ridha, D., Putri, D., & Doni, R. (2020). Teknik Keamanan File Teks Menggunakan Kriptografi Dengan Algoritma One Time Pad Cipher. 4(September), 588–597.

[2]. Fauzi, A., Maulita, Y., & Novriyenni. (2017). Perancangan Aplikasi Keamanan Pesan Menggunakan Algoritma Elgamal Denganmemanfaatkan Algoritma One Time Pad Sebagai Pembangkit Kunci. Jurnal Teknik Informatika Kaputana (JTIK), 1(1),

P-ISSN: 2548-9704
E-ISSN: 2686-0880

1–9.

[3]. Maharani, S., Maula, I., & Arifin, Z. (2016). Steganografi Video Menggunakan Metode End of File (Eof). SCAN - Jurnal Teknologi Informasi Dan Komunikasi, 11(3), 49–56.

[4]. Minarni, M., & Fernando, A. G. (2020). IMPLEMENTASI ALGORITMA END OF FILE (EoF) PADA STEGANOGRAFI CITRA. Jurnal TeknoIf, 8(1), 25. https://doi.org/10.21063/jtif.2020.v8.1.25-31

[5]. Nurdin, A. P. N. (2017). Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia. Jesik, 3(1), 1–11. nnurdin69@gmail.com