PENGAMANAN DOKUMEN TEKS MENGGUNAKAN ALGORITMA KRIPTOGRAFI MODE OPERASI *CIPHER BLOCK CHAINING* (CBC) DAN STEGANOGRAFI METODE *END OF FILE* (EOF)

Reza Dwi Oktaf Purnama[1], Heru Lestiawan, M.Kom.[2]
[1,2]Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Nakula I No.5-11 Semarang, 50131, (024) 3517261
E-mail : 111201105994@mhs.dinus.ac.id [1], hlestiawan@gmail.com[2]

Abstrak

Perkembangan teknologi informasi dan komunikasi memudahkan setiap orang untuk saling terhubung satu sama lain, hal ini menyebabkan pertukaran data maupun informasi dapat dengan mudah dilakukan. Kemudahan akses informasi ini memberi pengaruh dengan adanya ancaman yang dapat membahayakan informasi tersebut, misalnya berupa interupsi, penyadapan, maupun modifikasi informasi. Sebagai contoh sebuah perusahaan ingin mengirimkan sebuah dokumen penting atau pesan kepada mitra bisnisnya tetapi perusahaan ingin agar dokumen/pesan tersebut aman dari ancaman penyadapan yang dapat dilakukan oleh pihak lain. Kriptografi dan steganografi merupakan teknik pengamanan pesan diharapkan dapat tetap menjaga kerahasiaan isi dari informasi dan memberikan keyakinan pada penerima bahwa informasi tersebut memang berasal dari pengirim yang tepat begitu pula, metode yang digunakan dalam penelitian ini adalah mode operasi Cipher Block Chaining dan metode End Of File dengan menggunakan bahasa pemrograman Java. Penggabungan teknik pengamanan kriptografi dan steganografi akan meningkatkan keamanan pesan atau informasi dan menjamin kerahasiaan serta mengurangi resiko informasi dapat dilihat oleh pihak lain. Aplikasi pengamanan dokumen teks yang dibangun dapat mengamankan pesan/informasi dengan baik. Karena pesan berhasil teracak dan citra yang dihasilkan tidak menampakkan perbedaaan kualitas citra yang terlaku jauh dibandingkan dengan citra asli.

Kata Kunci: *ancaman, kriptografi, steganografi, Cipher Block Chaining, End Of File.*

Abstract

The development of information and communication technologies to facilitate each person are connected to each other, this means that data exchange as well as information can easily be carried. Accessibility this information make a difference with the threat that could jeopardize the information, for example of interruption, tapping, and modification information. For example, a company wants to send an important document or message to its business partners, but the company wants documents / messages are safe from the threat of eavesdropping can be done by others. Cryptography and steganography is a security techniques message is expected to maintain the confidentiality of the contents of the information and provide assurance to the recipient that the information actually came from the sender right as well, the method used in this study is the operating mode Cipher Block Chaining and methods End Of File with using the Java programming language. Incorporation of security cryptography and steganography techniques will improve the security of a message or information and guarantee the confidentiality and reduce the risk of information can be viewed by others. Text document security applications built to secure the message / information properly. Because the resulting image did not show differences in the quality of the image that terlaku far compared with the original image.

Keywords: *threat, cryptography, steganografy, ciphers block chaining, end of file.*

1. PENDAHULUAN

1.1 Latar Belakang

Ilmu pengetahuan dan teknologi khususnya bidang informatika berkembang semakin pesat dan membawa dunia ke era yang tanpa batas. Sejalan dengan itu, perkembangan teknologi informasi dan komunikasi memudahkan setiap orang untuk saling terhubung satu sama lain, yang mana hal ini menyebabkan pertukaran data maupun informasi dapat dengan mudah dilakukan. Seiring dengan perkembangan tersebut, muncul berbagai media yang dapat digunakan untuk mengakses dan mengelola informasi.

Kemudahan akses informasi ini memberi pengaruh dengan adanya ancaman-ancaman yang dapat membahayakan informasi tersebut, misalnya berupa interupsi, penyadapan, maupun modifikasi informasi. Hal ini dapat mempengaruhi tingkat keamanan dari pesan/ informasi yang berakibat pada keamanan data dan memunculkan kekhawatiran bagi pengirim dan penerima informasi apakah pesan/informasi yang dikirimkan masih aman atau sudah mengalami perubahan. Sebagai contoh sebuah perusahaan ingin mengirimkan sebuah dokumen penting ataupun pesan kepada mitra bisnisnya tetapi perusahaan ingin agar dokumen/pesan tersebut aman dari ancaman penyadapan yang dapat dilakukan oleh pihak lain. Oleh karena itu dilakukan proses pengamanan terhadap dokumen/pesan untuk menjaga kerahasian dari dokumen atau pesan/informasi tersebut.

Keamanan terhadap pesan/informasi adalah hal yang sangat penting, bisa dibayangkan apabila informasi yang menjadi rahasia penting dapat bocor dan disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, kriptografi yang merupakan salah satu teknik pengamanan pesan diharapkan dapat tetap menjaga kerahasiaan isi dari informasi dan memberikan keyakinan pada penerima pesan bahwa informasi tersebut memang berasal dari pengirim yang tepat begitu pula sebaliknya pengirim yakin bahwa penerima informasi adalah pihak yang tepat [1]. Dalam perkembangannya banyak algoritma kriptografi yang dapat diaplikasikan untuk mengamankan pesan atau informasi, salah satunya adalah algoritma kriptografi mode operasi Cipher Block Chaining (CBC).

Pengaplikasian teknik pengamanan kriptografi dapat mengamankan sebuah pesan atau informasi, namun kemampuan untuk memecahkan kriptografi juga mengalami perkembangan yang pesat, banyak metode kriptografi yang telah terpecahkan. Salah satu metode yang dapat ditambahkan untuk meningkatkan pengamanan informasi adalah metode steganografi.

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia (hiding message) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia [3]. Penyembunyian atau penyisipan informasi dapat diterapkan pada berbagai media seperti gambar, suara dan video. Metode steganografi yang dapat digunakan untuk penyembunyian atau penyisipan pesan salah satunya adalah dengan menggunakan metode End Of File (EOF).

Penggabungan teknik pengamanan kriptografi dan steganografi akan meningkatkan keamanan pesan atau informasi dan menjamin kerahasiaan informasi, serta mengurangi resiko informasi dapat dilihat oleh pihak lain. Sehingga penulis melakukan penelitian dengan menggabungkan teknik keamanan pesan kriptografi dan steganografi. Topik tugas akhir ini adalah “Pengamanan Dokumen Teks Menggunakan Algoritma Kriptografi

Mode Operasi Cipher Block Chaining (CBC) Dan Steganografi Metode End Of File (EOF)".

Berdasarkan latar belakang masalah yang telah diuraikan tersebut, maka dapat diambil perumusan masalah yaitu bagaimana mengamankan dokumen teks yang berisi pesan/informasi menggunakan algoritma kriptografi mode operasi Cipher Block Chaining (CBC) dan teknik steganografi metode End Of File (EOF) dalam memberikan keamanan terhadap pesan atau informasi?.

Berdasarkan rumusan masalah yang telah dijelaskan, maka ruang lingkup penelitian dibatasi pada :

a. Proses enkripsi dan dekripsi pesan dengan menggunakan algoritma kriptografi mode operasi Cipher Block Chaining (CBC) pada file berekstensi txt.
b. Proses steganografi pesan atau informasi yang telah dienkripsi dengan menyisipkan pesan kedalam file citra dengan format *.jpg, dan *.png dengan menggunakan metode End Of File (EOF).
c. Implementasi algoritma kriptografi mode operasi Cipher Block Chaining (CBC) dan steganografi End Of File (EOF) dalam aplikasi pengamanan informasi menggunakan software Java Netbeans.

Tujuan dari penelitian ini adalah mengamankan dokumen yang berisi pesan/informasi dari pengirim ke penerima agar informasi yang disampaikan masih terjaga keaslian dan kerahasiannya dengan menggunakan algoritma kriptografi mode operasi Cipher Block Chaining (CBC) dan steganografi metode End Of File (EOF).

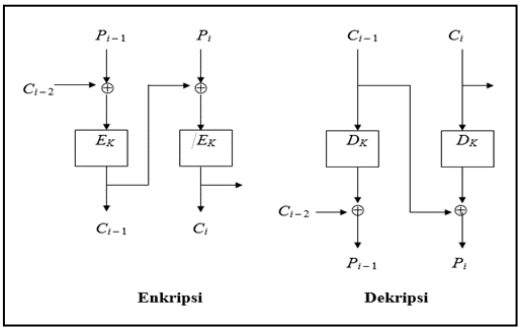
1.2 Landasan Teori

A. Kriptografi

Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi [4]. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter.

B. Mode Operasi Cipher Block Chaining (CBC)

Mode operasi ini menerapkan mekanisme umpan balik (feedback) pada sebuah blok, yang dalam hal ini hasil enkripsi blok sebelumnya di-umpan-balikkan ke dalam enkripsi blok yang current. Caranya, blok plainteks yang current di-XOR-kan terlebih dahulu dengan blok cipherteks hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi.



Gambar 1. Enkripsi dan Dekripsi Mode Operasi CBC

Untuk menghasilkan blok cipher pertama, IV (initialization vector) digunakan untuk menggantikan blok cipherteks sebelumnya. Sebaliknya pada dekripsi, blok plainteks pertama diperoleh dengan cara meng- XOR-kan IV dengan hasil dekripsi terhadap blok cipherteks pertama [2]. Secara matematis, enkripsi dengan mode CBC dinyatakan sebagai berikut :

$$Ci = EK(Pi \text{ xor } Ci - 1)$$

dan dekripsi sebagai

Pi = DK(Ci) xor Ci – 1

C. Steganografi

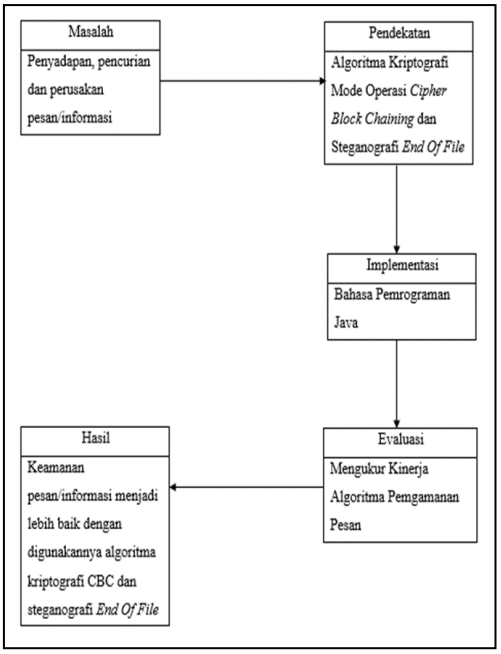
Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia (hiding message) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Steganografi membutuhkan dua properti yaitu wadah penampung dan data rahasia yang akan disembunyikan. Wadah penampung menggunakan media digital misalnya gambar, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suar, teks, atau video. Steganografi bertujuan untuk menghilangkan kecurigaan dengan cara menyamarkan pesan tersebut.

D. Metode End of File (EOF)

Metode End of File (EOF) merupakan salah satu metode yang digunakan dalam steganografi. Teknik ini menggunakan cara dengan menyisipkan data pada akhir file. Sehingga, tidak akan mengganggu kualitas data awal yang akan disisipkan pesan [6]. Namun hal ini akan mengakibatkan ukuran file bertambah, karena ukuran file sebelumnya akan ditambah dengan ukuran file pesan yang disisipkan ke dalam media penampung.

E. Kerangka Pemikiran

Kerangka pemikiran pada penelitian Penerapan Algoritma Kriptografi Mode Operasi Cipher Block Chaining (CBC) Dan Steganografi Metode End Of File (EOF) Untuk Pengamanan Pesan Pada Media File Citra dapat digambarkan melalui diagram berikut :



Gambar 2. Kerangka Pemikiran

2. METODE PENELITIAN

2.1 Instrumen Penelitian

A. Peralatan

1. Kebutuhan Perangkat Keras

Seperangkat PC atau laptop dengan spesifikasi minimal sebagai berikut :

- Prosessor Pentium 4 atau lebih.
- Harddisk 160 GB.
- Memori DDR 1 GB atau lebih.

B. Kebutuhan Perangkat Lunak

1. Sistem Operasi Microsoft Windows XP

Kebutuhan minimal sistem operasi pada penelitian ini yaitu Microsoft Windows XP, karena untuk pembuatan sistem aplikasi dengan menggunakan bahasa pemrograman Java sudah dapat berjalan pada sistem operasi ini, tetapi tidak menutup kemungkinan digunakannya sistem operasi terbaru yang lebih baik.

2. Software NetBeans IDE

Bahasa pemrograman yang digunakan dalam

perancangan sistem pada penelitian ini adalah Java. Netbeans digunakan untuk menulis, meng-compile, mencari kesalahan dan menyebarkan program netbeans yang ditulis dalam bahasa pemrograman java. Netbeans merupakan sebuah aplikasi Integrated Development Environment (IDE) yang berbasiskan Java dari Sun Microsystems yang berjalan di atas swing.

2.2 Metode Pengumpulan Data

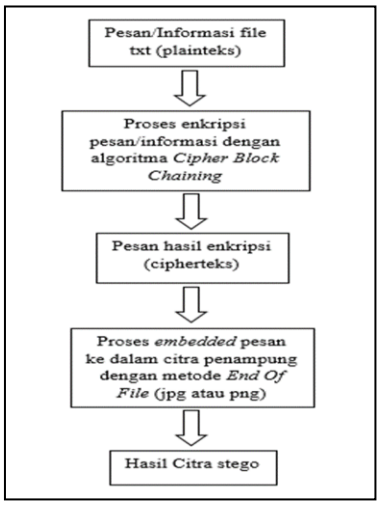
Data yang dikumpulkan dalam penelitian ini merupakan data sekunder. Data diperoleh dari telaah pustaka dan dokumen yang didapatkan penulis dari pustaka-pustaka yang mendukung, informasi dari internet, buku-buku dan artikel dari jurnal yang terkait dengan penelitian yang dilakukan oleh penulis.

2.3 Teknis Analisis Data

- Proses enkripsi dan dekripsi pesan/informasi menggunakan algoritma kriptografi mode operasi Cipher Block Chaining (CBC).
- Proses penyisipan pesan/informasi kedalam wadah penampung file citra dan proses ekstraksi pesan dari file citra menggunakan metode steganografi End Of File (EOF).
- Melakukan penilaian terhadap kualitas file citra penampung setelah disisipkan pesan dan menilai aplikasi pengamanan pesan secara keseluruhan.

2.4 Metode Yang Diusulkan

A. Prosedur Encode Data Yang diusulkan
   1. Inputkan file berekstensi txt yang berisi pesan/informasi (plaintext) yang akan dienkripsi dengan minimal 8 karakter pesan (64 bit).
   2. Proses enkripsi pesan dengan menambahkan kunci dengan panjang 8 karakter (64) kunci dengan menggunakan algoritma kriptografi mode operasi Cipher Block Chaining.
   3. Inputkan file citra sebagai wadah penampung pesan dengan format file *.jpg, atau *.png.
   4. Pesan yang telah terenkripsi kemudian disisipkan kedalam file citra penampung pada proses stego dengan metode steganografi End Of File.
   5. Hasil akhir adalah file citra yang telah disisipkan pesan/informasi (stego image).

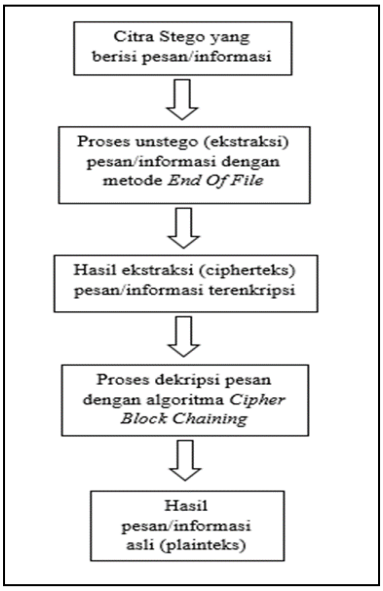


Gambar 3. Prosedur Encode Yang Diusulkan

B. Prosedur Decode Yang Diusulkan
   1. Inputkan citra stego yang berisi pesan/informasi yang akan dilakukan proses ekstraksi.
   2. Proses unstego citra dengan metode End Of File untuk mengambil pesan yang telah disisipkan pada file citra.
   3. Pesan yang telah berhasil di-

unstego (ekstraksi) masih dalam bentuk ciphertext.

4. Proses dekripsi untuk mengetahui pesan asli dengan menggunakan algoritma kriptografi mode operasi Cipher Block Chaining.
5. Pesan/infomasi asli (plaintext) dihasilkan dari proses dekripsi.



Gambar 4. Prosedur Decode Yang Diusulkan

3. HASIL DAN PEMBAHASAN

3.1 Analisis Algoritma Mode Operasi Cipher Block Chaining

A. Cara kerja mode operasi *Cipher Block Chaining*

1. Proses Enkripsi
   - Bagi plainteks menjadi blok yang telah ditentukan ukurannya, pada perangkat lunak ini tiap blok berukuran 64 bit.
   - Tiap blok yang telah dibagi kemudian di-XOR-kan dengan IV.
   - Kemudian hasil yang telah didapatkan di-XOR-kan kembali dengan kunci.
   - Hasil operasi XOR tersebut digeser 1 bit ke kiri.
   - Hasil tersebut menjadi IV untuk blok berikutnya.
   - Proses diulang sampai blok terakhir.

Contoh Enkripsi :
Plainteks (P) : U
Kunci (K) : K
IV/C0 : 00000000
Maka
P : 01010101
K : 01001011
C0 : 00000000

U = 01010101
C1 diperoleh sebagai berikut :
P1 xor C0 = 01010101 xor 00000000 = 01010101
Kemudian hasil yang diperoleh di-XOR dengan kunci
01010101 xor 01001011 = 00011110
Geser ke kiri 1 bit
0001 menjadi 0010 dan 1110 menjadi 1101
Maka C1 = 00101101 atau dalam hexa = 2D

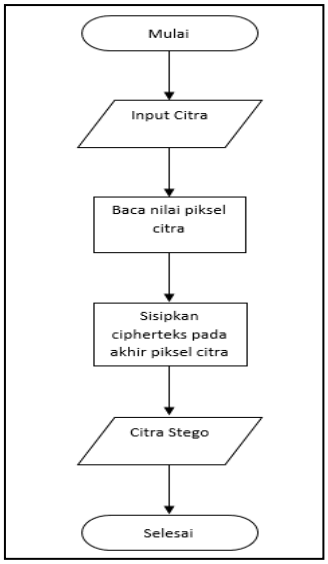
2. Proses Dekripsi
   - Proses dekripsi dilakukan dari blok paling akhir.
   - Hasil pembagian blok kemudian digeser 1 bit ke kanan.
   - Kemudian hasil pergeseran tersebut di-XOR-kan dengan kunci.
   - Kemudian hasil tersebut di-XOR-kan kembali dengan blok cipherteks sebelumnya.
   - Proses diulang sampai blok paling awal, blok paling awal di-XOR-kan dengan IV.

Contoh Dekripsi :
C1 = 00101101
Geser 1 bit ke kanan
0010 menjadi 0001 dan 1101 menjadi 1110
Kemudian di-XOR-kan dengan kunci
00011110 xor 01001011 = 01010101
Hasil yang diperoleh kemudian di-XOR kembali dengan C0
01010101 xor 00000000 = 01010101
maka 01010101 = U

3.2 Analisis Metode End Of File

Teknik ini menggunakana cara dengan menyisipkan data pada akhir file. Sehingga, tidak akan mengganggu kualitas data awal yang akan disisipkan pesan [6]. Namun hal ini akan mengakibatkan ukuran file bertambah, karena ukuran file sebelumnya akan ditambah dengan ukuran file pesan yang disisipkan ke dalam media penampung. Teknik ini sendiri ditujukan agar tidak mengurangi kualitas dari gambar induk sebelum dan sesudah penyisipan.

A. Proses Embedding
- Inputkan cipherteks yang akan disisipkan.
- Inputkan file citra yang akan dijadikan sebagai wadah penampung pesan.
- Baca nilai piksel dari citra.
- Tambahkan cipherteks pada akhir piksel citra.
- Ubah menjadi citra baru.



Gambar 5. Flowchart penyisipan pesan

Misalkan terdapat citra RGB dengan ukuran 8x8 yang memiliki nilai setiap piksel seperti berikut :

Tabel 1. Matriks piksel citra RGB

104	38	55	104	96	96	77	92
80	93	60	60	60	51	56	94
91	79	16	62	90	69	73	87
97	98	70	52	60	63	52	99
85	83	37	18	82	88	51	56
87	84	56	65	68	39	106	101
69	37	44	74	80	68	99	99
66	62	60	32	105	88	71	77

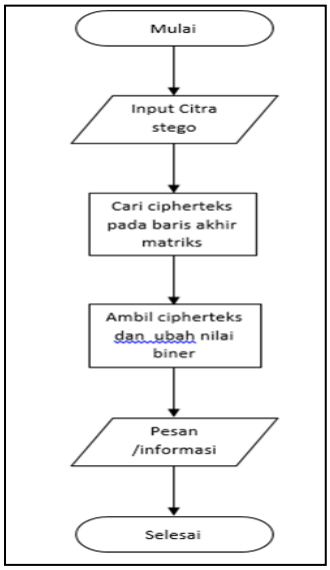
Kemudian citra tersebut akan disisipkan cipherteks " 45 68 140 19 11 38 ". cipherteks akan ditambahkna sebagai nilai akhir dari piksel citra RGB. Maka didapatkan matriks piksel baru :

Tabel 2. Matriks piksel citra RGB telah disisipkan cipherteks

104	38	55	104	96	96	77	92
80	93	60	60	60	51	56	94
91	79	16	62	90	69	73	87
97	98	70	52	60	63	52	99
85	83	37	18	82	88	51	56
87	84	56	65	68	39	106	101
69	37	44	74	80	68	99	99
66	62	60	32	105	88	71	77
45	**68**	**140**	**19**	**11**	**38**		

B. Proses Ekstraksi

- Inputkan citra yang terdapat pesan cipherteks (stego image).
- Baca nilai piksel stego image yang terdapat pada baris akhir matriks piksel citra.
- Ambil cipherteks pada baris akhir matriks piksel citra yang terdapat pada stego image kemudian ubah nilai biner.
- Pesan/informasi rahasia.



Gambar 6. Flowchart ekstraksi pesan

Citra RGB 8x8 yang telah disisipkan cipherteks (stego image) dengan nilai setiap piksel file citra RGB seperti pada tabel.

Tabel 3. Matriks piksel citra RGB telah disisipkan cipherteks

104	38	55	104	96	96	77	92
80	93	60	60	60	51	56	94
91	79	16	62	90	69	73	87
97	98	70	52	60	63	52	99
85	83	37	18	82	88	51	56
87	84	56	65	68	39	106	101
69	37	44	74	80	68	99	99
66	62	60	32	105	88	71	77
45	**68**	**140**	**19**	**11**	**38**		

Kemudian baca dan ambil nilai piksel pada stego image yang terdapat pada baris terakhir matriks piksel citra.

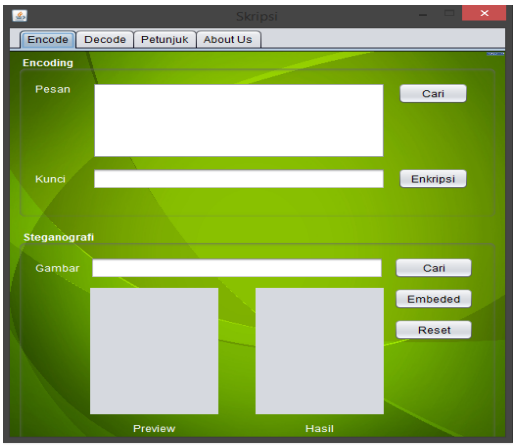
Tabel 4. Matriks piksel stego image pada baris terakhir

45	**68**	**140**	**19**	**11**	**38**

3.3 Implementasi

Aplikasi kriptografi dan steganografi ini dimulai dengan menekan tombol "ENTER" yang berada di tampilan awal aplikasi untuk menuju ke tampilan antar muka selanjutnya yang berisi sub menu aplikasi.

Gambar 7. Tampilan awal aplikasi



Gambar 8. Menu aplikasi

Pada halaman selanjutnya berisi menu yang ada pada aplikasi, yaitu menu encode, menu decode, menu petunjuk, dan menu about us.

3.4 Hasil Pengujian Aplikasi

Pengujian aplikasi dilakukan dengan menggunakan metode random sampling

yaitu dengan mengambil sample masing masing 40 sample pesan dan 40 sample gambar yang terdiri dari 20 sample gambar *.jpg dan 20 sample gambar *.png.

File pesan dan file gambar kemudian diujikan pada aplikasi untuk melihat hasil akhir dari proses kriptografi dan proses steganografi. Dalam pengujian yang dilakukan, penulis memasukkan kunci yang sama untuk setiap pengujian, kunci yang digunakan adalah “semangat”.

Masing-masing data kemudian diujikan pada aplikasi. Pengujian dilakukan untuk melihat proses enkripsi yang bertujuan untuk mengacak pesan agar pesan tidak dapat dibaca kemudian hasil proses enkripsi dilakukan juga uji proses steganografi yang bertujuan agar pesan rahasia dapat disembunyikan pada media penampung.

Setelah dilakukan pengujian, semua data yang diujikan pada aplikasi berhasil melewati proses kriptografi (enkripsi dan dekripsi). Data pesan/informasi yang berada pada dokumen txt setelah dilakukan proses enkripsi menjadi data acak yang tidak bisa dibaca, kemudian untuk proses dekripsi data acak tersebut dapat dikembalikan seperti semula.

Pada proses steganografi, data pesan berhasil disisipkan kedalam gambar penampung dan proses pengungkapan kembali atau ekstraksi pesan berhasil dilakukan terhadap gambar penampung, ini memenuhi unsur steganografi yang baik yaitu Recovery. Hal ini menunjukkan aplikasi pengamanan pesan dapat digunakan untuk mengamankan pesan atau informasi.

Pengujian juga dilakukan pada citra stego yang mengalami pengubahan dengan dilakukan rotasi 90 derajat ke kanan, 90 derajat kekiri dan rotasi 180 derajat untuk dilakukan proses decode apakah pesan berhasil dieksraksi atau tidak.

1. Rotasi 90 derajat kekanan

Gambar 9. Rotasi 90 derajat kekanan

2. Rotasi 90 derajat kekiri

Gambar 9. Rotasi 90 derajat kekiri

3. Rotasi 180 derajat

Gambar 10. Rotasi 180 derajat

Setelah dilakukan pengujian, citra stego yang telah mengalami pengubahan tidak berhasil untuk dilakukan ekstraksi. Aplikasi tidak menemukan adanya pesan yang disimpan karena susunan piksel telah berubah. Ini menunjukkan aplikasi tidak memenuhi unsur Robustness, data tidak tahan terhadap manipulasi yang dilakukan terhadap wadah penampung pesan.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Dari penelitian yang telah dilakukan maka penulis dapat menyimpulkan beberapa kesimpulan sebagai berikut :

1. Aplikasi pengamanan dokumen teks dapat mengamankan dokumen pesan/informasi dengan baik. Karena citra yang dihasilkan tidak menampakkan perbedaaan kualitas citra yang terlaku jauh.
2. Proses kriptografi (enkripsi dan dekripsi) pesan/informasi menggunakan metode Cipher Block Chaining dapat mengacak pesan menjadi pesan yang tidak terbaca dan dapat didekripsi kembali menjadi pesan asli.
3. Proses steganografi (embedded dan ekstraksi) dengan metode End Of File, pesan dapat disisipkan kedalam citra penampung dan pesan dapat diekstraksi dari citra penampung dapat dilakukan dengan baik, memenuhi unsur steganografi yang baik yaitu Recovery.
4. Citra stego yang dihasilkan dari proses stagnografi memiliki kualitas yang tidak banyak berubah setelah citra asli disisipkan pesan/informasi, hal ini memenuhi unsur steganografi yang baik yaitu Fidelity.
5. Namun setelah dilakukan pengujian dengan manipulasi rotasi 90 derajat kekanan, 90 derajat kekiri, dan rotasi 180 derajat terhadap citra stego menunujukkan hasil aplikasi tidak dapat membaca adanya pesan yang disisipkan, tidak memenuhi unsur Robustness, karena data tidak tahan terhadap manipulasi yang dilakukan.

4.2 Saran

Dari uraian kesimpulan diatas, maka penulis memberikan saran untuk pengembangan lanjutan dan penelitian selanjutnya yaitu sebagai berikut :

1. Pengembangan aplikasi pengamanan dokumen dapat dilakukan dengan file dokumen lainnya seperti *.doc, *pdf, dll. Atau dapat mengembangkan dengan menggunakan metode pengamanan kriptografi dan steganografi yang memberikan hasil lebih baik.
2. Untuk penelitian selanjutnya dapat dilakukan dengan menggunakan data atau metode yang lebih tahan terhadap manipulasi, agar memenuhi unsur Robustness sebagai steganografi yang baik.

DAFTAR PUSTAKA

[1] Cucu Tri Eka Yuliana, “Implementasi Algoritma Kriptografi Blowfish dan Metode Steganografi End Of File (EOF) untuk Keamanan Data”, Skripsi Teknik Informatika Universitas Dian Nuswantoro, Semarang, 2014.

[2] Rinaldi Munir, Kriptografi. Bandung: Informatika, 2007.

[3] Dony Ariyus, Kriptografi Keamanan Data dan Komunikasi. Yogyakarta: Andi Offset, 2005.

[4] Sentot Kromodimoeljo, Teori & Aplikasi Kriptografi.: SPK IT Consulting, 2010.

[5] Nurli Hairiah, “Analisa Dan Implementasi Algoritma Cipher Block Chaining Dalam Penyandian Teks”, STMIK Budi Darma Medan, Medan.

[6] Henny Wandani, Muhammad Andri Budiman, and Amer Sharif, "Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem," Universitas Sumatera Utara , Medan.

[7] Paskalis Andrianus Nani, "Penerapan Enkripsi ALgoritma Blowfish Pada Proses Steganografi EOF," Universitas Katolik Widya Mandira, Kupang.

[8] Yayuk Anggraini, Dolly Virgian Shaka Yudha Sakti, “Penerapan Steganografi Metode End Of File (Eof) Dan Enkripsi Metode Data Encryption Standard (Des) Pada Aplikasi

Pengamanan Data Gambar Berbasis Java Programming", Universitas Budi Luhur, Jakarta, 2014.
[9] M. Shalahuddin dan Rosa A.S. Belajar Pemrograman dengan Bahasa Pemrograman C++ dan Java : dari Nol Menjadi Handal, Bandung : Informatika, 2010.