TEKNIK PENGAMANAN DATA DENGAN STEGANOGRAFI METODE END OF FILE (EOF) DAN KRIPTOGRAFI VERNAM CIPHER

Agustinus Baretto Petrus Anggen[1)], Mohammad Irwan Ukkas[2)], Reza Andrea[3)]

[1.]Program Studi Teknik Informatika, STMIK Widya Cipta Dharma
[1.]Jl. M.Yamin No.25, Samarinda, 75123
E-Mail : agustinus.anggen@gmail.com[1)], irwan212@yahoo.com[2)], reza.andrea@gmail.com[3)]

ABSTRAK

Teknik Pengamanan Data Dengan Steganografi Metode End of File (EoF) dan Kriptografi Vernam Cipher, merupakan aplikasi yang dibuat untuk mempermudah pengamanan file-file penting yang rawan dicuri ataupun hilang. Proses pengamanan data diharapkan dapat mencegah pencurian atau penyadapan data yang dilakukan oleh hacker, cracker, carder, phreaker, dan sebagainya.

Tujuan dari penelitian ini adalah untuk menyembunyikan data-data penting dengan menggunakan teknik steganografi dan juga dikunci dengan teknik kriptografi agar data tidak bocor kepada pihak-pihak yang tidak bertanggung jawab.

Dari hasil implementasi, disimpulkan bahwa dengan penggunaan teknik pengamanan data ini dapat membantu dalam proses pengamanan data-data penting dari pihak yang tidak bertanggung jawab.

***Kata Kunci**: Enkripsi, Dekripsi, Steganografi, Kriptografi, End of File, Vernam Cipher*

1. PENDAHULUAN

Steganografi merupakan salah satu cara yang sangat efektif untuk mengamankan data (selain pengirim dan penerima yang sah). Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari bidang jenis teknik untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah *file*. *File* yang digunakan sebagai induk untuk menyembunyikan file yang disisipkan(*plain file)* disebut dengan *file spoof*. Dalam perkembangan ilmu steganografi sekarang ini, terdapat berbagai macam metode yang dapat digunakan untuk menyembunyikan *file* tersebut. Salah satu contohnya adalah metode *End of File* (EoF).

Kriptografi juga dapat digunakan untuk mengamankan data-data penting pada sebuah *file*. Data yang terkandung dalam *file* disandikan atau dienkripsi untuk diubah menjadi simbol tertentu sehingga hanya orang tertentu saja yang dapat mengetahui isi dari data tersebut. Dalam perkembangan ilmu kriptografi masa sekarang ini, telah banyak tercipta algoritma-algoritma yang dapat digunakan untuk mengubah data asli (*plain text*) menjadi simbol tertentu (*cipher text*). Salah satu contohnya adalah algoritma *Vernam Cipher*. Algoritma ini termasuk dalam algoritma kriptografi modern dan merupakan algoritma *stream chiper*.

Proses pengamanan data dengan menggunakan steganografi dan kriptografi diharapkan dapat mencegah terjadinya pencurian atau penyadapan data yang dilakukan oleh *hacker*, *cracker*, *carder*, *phreaker*, dan sebagainya.

Berdasarkan keunggulan dari kedua algoritma tersebut, maka peneliti menganalisa kemampuan gabungan dari *vernam cipher* dan *end of file* untuk mengamankan file.

2. RUANG LINGKUP PENELITIAN

2.1 Rumusan Masalah

Berkaitan dengan latar belakang di atas, maka ada hal yang menjadi rumusan dalam masalah ini, yaitu sebagai berikut :

1. Bagaimana menerapkan steganografi untuk menyisipkan dan merahasiakan *plain file* didalam *file spoof*?
2. Bagaimana menerapkan *vernam cipher* untuk enkripsi *file* dengan kunci berupa karakter ASCII?
3. Bagaimana hasil perbandingan dan estimasi waktu dalam penerapan steganografi dan *vernam cipher?*

2.2 Batasan Masalah

Adapun batasan masalah dari penilitian ini adalah :

1. Metode Steganografi untuk *End of File* terbatas hanya untuk *file* dengan format gambar .bmp.
2. *Vernam Chiper* untuk enkripsi file berupa kunci karakter ASCII.
3. Pengujian yang digunakan adalah *black box, dan white box*.
4. *Plain file* tidak dapat lebih besar dari *file spoof*.

3. BAHAN DAN METODE

3.1 Kriptografi

Kriptografi berasal dari kata ‘‘Crypto’’ yang bearti rahasia dan “graphy” yang bearti tulisan. Jadi dapat dikatakan bahwa kriptografi adalah tulisan yang

tersembunyi. Dengan adanya tulisan yang tersembunyi ini, orang-orang tidak mengetahui bagaimana tulisan tersebut disembunyikan dan tidak mengetahui bagaimana cara membaca maupun menerjemahkan tulisan tersebut (Ariyus, 2008).

William Stallings mendefinisikan kriptografi sebagai "the art of science of keeping message secure". Kriptografi berbasis pada algoritma pengkodean data informasi yang mendukung kebutuhan dari dua aspek keamanan informasi, yaitu secrecy (perlindungan terhadap kerahasiaan data informasi) dan authenticity (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan. Kriptografi menjadi dasar bagi keamanan komputer dan jaringan karena merupakan sarana bagi distribusi data dan informasi. Sehingga data dan informasi tersebut harus diamankan agar hanya orang-orang yang berhak mengaksesnya yang dapat mengetahui maupun menggunakan data tersebut. Salah satu cara yang paling banyak digunakan dalam mengamankan data adalah dengan kriptografi. Data-data tersebut diamankan dengan sedemikian rupa oleh pengirim sehingga orang lain tidak dapat mengenali data tersebut. Pembakuan penulisan pada kriptografi dapat ditulis dalam bahasa matematika.

3.2 Vernam Cipher

Vernam cipher merupakan algoritma kriptografi yang ditemukan oleh Mayor J. Maugborne dan G. Vernam. Algoritma ini merupakan algoritma berjenis symmetric key yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara stream cipher dimana cipher berasal dari hasil XOR antara bit plaintext dan bit key. Algoritma Vernam cipher diadopsi dari one-time pad cipher, dimana dalam hal ini karakter diganti dengan bit (0 atau 1). Dengan kata lain, Vernam Cipher merupakan versi lain dari one-time pad cipher (Wicaksono, 2011).

Dalam proses enkripsi, cipherteks diperoleh dengan melakukan penjumlahan modulo 2 satu bit plainteks dengan satu bit kunci, seperti terlihat pada rumus di bawah ini :

$c_1 = (p_1 + k_1) \bmod 2$

Dimana :

C_1 = cipher teks $p1$ = plainteks $k1$ = kunci

Sedangkan dalam proses dekripsi, untuk mendapatkan kembali plainteks, diperoleh dengan melakukan penjumlahan modulo 2 satu bit cipherteks dengan satu bit kunci :

$p_1 = (c_1 - k_1) \bmod 2$

Pada cipher aliran, bit hanya mempunya dua buah nilai, sehingga proses enkripsi hanya menyebabkan dua keadaan pada bit tersebut, yaitu berubah atau tidak berubah. Dua keadaan tersebut ditentukan oleh kunci enkripsi yang disebut dengan aliran-bit-kunci (keystream). Oleh karena operasi penjumlahan modul 2 identik dengan operasi bit dengan operator XOR, maka persamaan dapat ditulis secara sederhana sebagai berikut:

$c_1 = p_1 \text{ XOR } k_1$

Sedangkan pada proses pendekripsian dituliskan:

$p_1 = c_1 \text{ XOR } k_1$

Dalam operator logika XOR, hasil akan T (benar) apabila salah satu dari kedua operand (tetapi tidak keduanya) bernilai T atau 1. Atau dengan kata lain, apabila diaplikasikan dalam bit maka operator XOR akan menghasilkan 1 jika dan hanya jika salah satu operand bernilai 1.

3.3 Steganografi

Steganografi berasal dari bahasa Yunani yaitu Steganós yang berarti menyembunyikan dan Graptos yang artinya tulisan sehingga secara keseluruhan artinya adalah tulisan yang disembunyikan. Secara umum steganografi merupakan seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia dengan segala cara sehingga selain orang yang dituju, orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut (Edisuryana 2013).

Istilah steganografi termasuk penyembunyian data digital dalam file-file komputer. Contohnya, si pengirim mulai dengan file gambar biasa, lalu mengatur warna setiap pixel ke-100 untuk menyesuaikan suatu huruf dalam alphabet (perubahannya begitu halus sehingga tidak ada seorangpun yang menyadarinya jika ia tidak benar- benar memperhatikannya). Pada umumnya, pesan steganografi muncul dengan rupa lain seperti gambar, artikel, daftar belanjaan, atau pesan-pesan lainnya. Pesan yang tertulis ini merupakan tulisan yang menyelubungi atau menutupi. Contohnya, suatu pesan bisa disembunyikan dengan menggunakan tinta yang tidak terlihat diantara garis-garis yang kelihatan. Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia (teks atau gambar) di dalam file-file lain yang mengandung teks, image, bahkan audio tanpa menunjukkan ciri- ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari file semula. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya. Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.

Pada metode steganografi cara ini sangat berguna jika digunakan pada cara steganografi komputer karena banyak format file digital yang dapat dijadikan media untuk menyembunyikan pesan. Format yang biasa digunakan diantaranya:

Format image : bitmap (bmp), gif, pcx, jpeg, dll.

Format audio : wav, voc, mp3, dll.

Format lain : teks, File, html, pdf, dll.

Kelebihan steganografi daripada kriptografi adalah pesan- pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya. Sebuah pesan steganografi (plaintext), biasanya pertama-tama dienkripsikan dengan

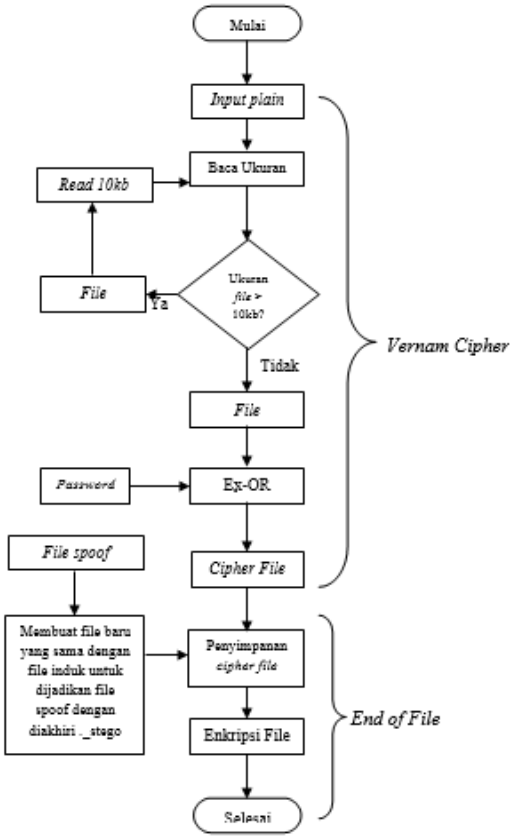
beberapa arti tradisional, yang menghasilkan ciphertext. Kemudian, covertext dimodifikasi dalam beberapa cara sehingga berisi ciphertext, yang menghasilkan stegotext. Contohnya, ukuran huruf, ukuran spasi, jenis huruf, atau karakteristik covertext lainnya dapat dimanipulasi untuk membawa pesan tersembunyi; hanya penerima (yang harus mengetahui teknik yang digunakan) dapat membuka pesan dan mendekripsikannya.

3.4 Metode End of File

Teknik yang digunakan pada digital watermarking beragam tetapi secara umum teknik ini menggunakan redundant bits sebagai tempat menyembunyikan pesan pada saat dilakukan kompresi data, dan kemudian menggunakan kelemahan indera manusia yang tidak sensitif sehingga pesan tersebut tidak ada perbedaan yang terlihat atau yang terdengar. Teknik EOF atau End Of File merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini menggunakan cara dengan menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam file tersebut. Teknik inilah yang akan digunakan penulis dalam penelitian ini. Dalam teknik ini, data disisipkan pada akhir file dengan diberi tanda khusus sebagai pengenal start dari data tersebut dan pengenal akhir dari data tersebut (Edisuryana, 2013).

4. RANCANGAN SISTEM/APLIKASI

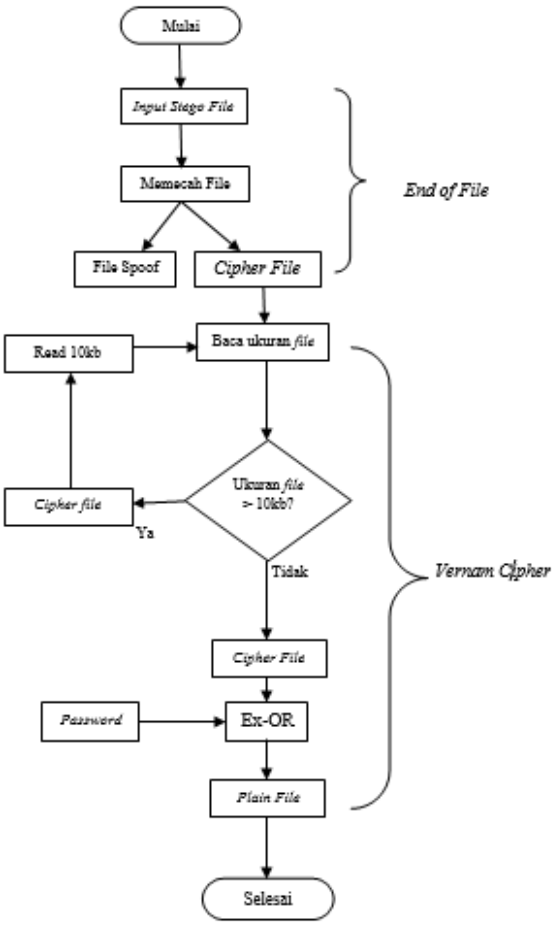
1. Flowchart Proses Enkripsi



Gambar 1 Flowchart Proses Enkripsi

Pada gambar 1 merupakan flowchart program yang menjelaskan tentang alur program proses enkripsi. Pertama ketika tombol steganografi di pilih, maka program akan memulai proses vernam cipher, dimana mulai dengan membaca format file dan dilanjutkan dengan ukuran gambar. Setelah itu file akan mulai diproses, yaitu dengan logika Ex-OR sampai syarat terpenuhi. Kemudian file yang disisipkan akan diproses lagi dengan logika Ex-OR dengan password yang telah diinput. Setelah selesai diproses, file akan menjadi file cipher yang tidak akan bisa dibaca tanpa password dibuka. Setelah itu program akan melanjutkan proses dengan metode end of file, dimana plain file yang telah diproses dengan vernam cipher tersebut disisipkan kedalam file induk yang telah dibuat baru dengan diberi tanda ._stego agar dapat terbaca ketika didekripsi. Setelah proses, maka file akan menjadi file spoof yang telah disisipkan dengan cipher file.

2. Flowchart Proses Dekripsi



Gambar 2 Flowchart Proses Dekripsi

Pada gambar 4.3 merupakan flowchart program yang menjelaskan alur ekstrak file dari file spoof yang telah di sisipkan file. Pertama setelah memilih tombol ekstrak file, maka akan memulai proses end of file dan masuk ke bagian menginput file spoof yang telah disisipkan. Dilanjutkan dengan membaca file tersebut, jika file lebih dari 10 kb, maka file tersebut akan dibaca 10000 byte dan sisanya akan di looping kedalam proses. Setelah proses, maka proses akan dilanjutkan dengan algoritma vernam cipher, dimana

cipher file tersebut akan didekripsi menggunakan password yang digunakan untuk enkripsi, dan akan menjadi plain file pada hasilnya.

5. Implementasi

1. Form Utama

Gambar 3 Form Utama

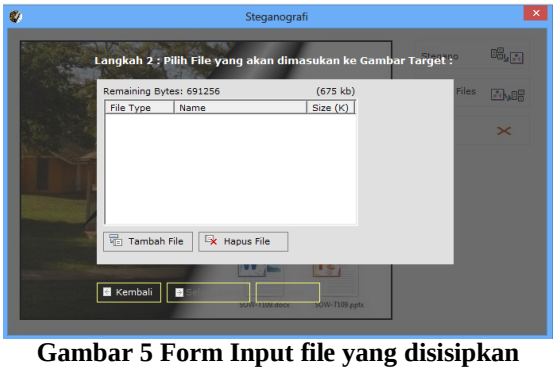
Pada gambar 3 adalah halaman utama untuk memulai memasuki program steganografi dan ekstrak file. *User* dapat memilih untuk memulai steganografi atau ekstrak file dari *file spoof* yang telah disisipkan file lain.

2. Form Input File Spoof

Gambar 4 Form Input File Spoof

Pada Gambar 4 adalah halaman steganografi dimana *user* dapat menginput file untuk dijadikan *file spoof* dalam proses steganografi dengan tombol "Tambah File". Setelah menambahkan file, kemudian user dapat melanjutkan proses steganografi dengan cara menekan tombol "Selanjutnya". File yang di *input* harus tipe *bitmap* (.bmp) file.

3. Form Input file yang disisipkan



Gambar 5 Form Input file yang disisipkan

Pada gambar 5 adalah halaman input file yang disisipkan pada file spoof. File yang di input nantinya akan disisipkan pada file spoof yang telah di input pada halaman sebelumnya dengan menekan tombol "Tambah File" pada halaman tersebut. User juga dapat menghapus file yang ingin di sisipkan dengan menekan tombol "Hapus File". User juga dapat kembali ke halaman sebelumnya dengan menekan tombol "Kembali", serta dapat memulai proses steganografi dengan menekan tombol "Selanjutnya".

4. Form Input Password

Gambar 6 Form Input Password

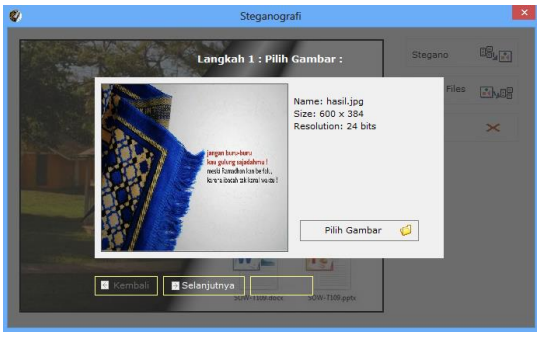
Pada Gambar 6 adalah halaman input password dimana user menginput password untuk mengunci file yang di input dalam file spoof tersebut. Password bisa juga dikosongkan jika user tidak menginginkan untuk penguncian file yang disisipkan.

5. Form Output Hasil Steganografi

Gambar 7 Form Output Hasil Steganografi

Pada gambar 7 adalah halaman output hasil steganografi dimana proses penyisipan telah selesai. User dapat melihat hasilnya langsung dengan menekan tombol "Lihat Hasilnya" atau menutup dengan menekan tombol "Selesai".

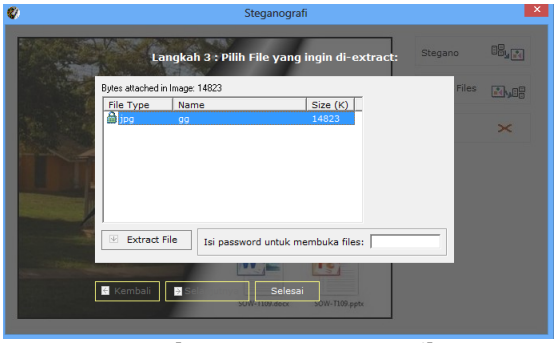
6. Form Dekripsi File



Gambar 8 *Form* Dekripsi File

Pada gambar 8 merupakan halaman ekstrak file dimana user dapat melakukan input file spoof yang telah di sisipkan file, dengan menekan tombol "Tambah File" pada halaman tersebut. Setelah user menginput file spoof, maka proses ekstrak file dapat di lanjutkan, jika tidak ada file yang disisipkan, maka program tidak bisa dilanjutkan.

7. Form Output file

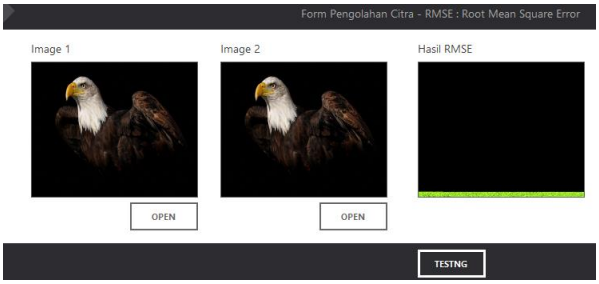


Gambar 9 Form Output File

Pada gambar 9 adalah halaman ekstrak output file, dimana user dapat memilih file yang ingin di ekstrak dengan membuka kunci sesuai dengan sandi yang dipakai untuk mengunci file tersebut. Setelah menginput password dan password benar, maka user dapat mengekstrak file dan menghasilkan output file.

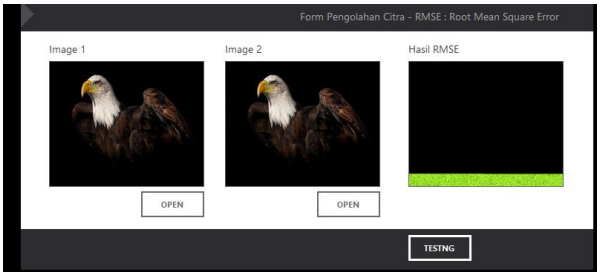
8. Pengujian Pixel Gambar

Pengujian pixel gambar adalah pengujian perbedaan pixel gambar yang sebelum diproses dan setelah diproses steganografi berdasarkan pixel file spoof menggunakan aplikasi bantuan Visual Studio Root Mean Square Error.exe. Aplikasi ini digunakan untuk menemukan perbedaan pixel binary dari dua file yang diinputkan, sebelum dan sesudah diimplementasi steganografi.



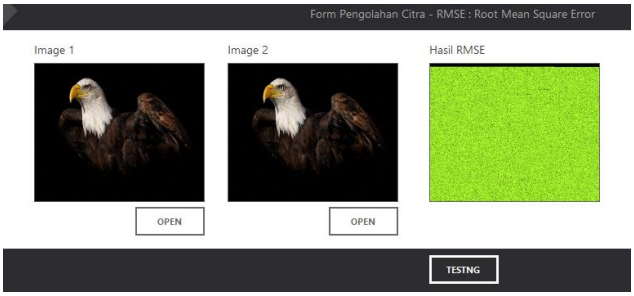
Gambar 10 Pengujian File Spoof dengan Plain File .txt

Gambar 10 merupakan pengujian file *eagle.bmp* dengan *pixel* 800x640 disisipkan file *.txt* dengan ukuran 6.74kb. Terlihat dari hasil *Root Mean Square Error*, menemukan bahwa *pixel binary* dibagian bawah berbeda dari yang sebelum diimplementasi steganografi.



Gambar 11 Pengujian File Spoof dengan Plain File .jpeg

Pada Gambar 11, merupakan pengujian file eagle.bmp dengan pixel 800x640 disisipkan file .jpeg dengan ukuran 17,3kb. Terlihat dari hasil Root Mean Square Error, menemukan bahwa pixel binary dibagian bawah berbeda dari yang sebelum diimplementasi steganografi.



Gambar 12 Pengujian *File Spoof* dengan *Plain File* *.txt* dan *.jpeg*

Gambar 12 merupakan pengujian file eagle.bmp dengan pixel 800x640 dsisipkan file .txt dan .jpeg dengan ukuran 172kb.Terlihat dari hasil Root Mean Square Error, menemukan bahwa pixel binary dibagian bawah berbeda dari yang sebelum diimplementasi steganografi. Error yang ditemukan hampir pada seluruh gambar, karena file yang disisipkan hampir mencapai maksimum yaitu 175kb, maka dapat diambil kesimpulan bahwa, warna hijau pada hasil Root Mean Square Error adalah pixel binnary yang berbeda dari kedua gambar yang diinput, dan pixel gambar dari gambar kedua telah mengalami perubahan pixel karena adanya plain file yang diinput kedalam file spoof. Dari tiga hasil pengujian pixel gambar, terlihat bahwa semakin besar file yang disisipkan, maka semakin banyak pixel yang berubah.

6. KESIMPULAN

Dari hasil penelitian ini pembahasan yang telah diuraikan pada bab sebelumnya, maka dapat ditarik kesimpulan sebagai berikut :

1. Teknik Pengamanan Data Dengan Menggunakan Steganografi Metode End of File dan Kriptografi Vernam Cipher ini dapat bekerja menyisipkan sebuah atau beberapa plain file didalam sebuah file spoof dengan format bitmap (.bmp) dengan mengimplementasikan steganografi metode end of file, sehingga plain file tersebut tersembunyi didalam file spoof.
2. Enkripsi plain file menjadi cipher file dengan menggunakan kriptografi algoritma vernam cipher, sehingga file tersebut tidak dapat dibaca ataupun digunakan sebelum didekripsikan kembali.
3. Steganografi dan vernam cipher, mengenkripsikan plain file menjadi cipher file dan disisipkan kedalam file spoof. Semakin besar ukuran file spoof dan plain file, semakin lama waktu yang digunakan untuk menyelesaikan proses steganografi dan vernam cipher tersebut.
4. Program ini merupakan sistem yang dibuat untuk membantu pengguna(user) dalam mengamankan plain file agar tidak diketahui oleh masyarakat umum, seperti file dokumen dan gambar.

7. SARAN

Berdasarkan hasil dari pembahasan dan kesimpulan, maka didapat saran sebagai berikut :

1. Program Teknik pengamanan data dengan stganografi metode end of file dan kriptografi vernam cipher bisa dikembangkan menjadi berbasis online dan bisa diakses dimana saja.

2. Program ini masih banyak kekurangan yang dapat dikembangkan dan diperbaiki menjadi lebih baik dan menarik sesuai dengan perkembangan ilmu pengetahuan dan tekhnologi yang berkembang.
3. Program yang masih dapat dikembangkan untuk jadi lebih menarik lagi seperti aplikasi berbasis android.
4. Program yang dibuat masih hanya untuk bitmap (.bmp) file, diharapkan dapat dikembangkan untuk tipe-tipe file yang lainnya seperti .mp3, jpeg, dan lain-lain.
5. Metode alternatif lain yang bisa digunakan selain dengan kriptografi vernam cipher, bisa menggunakan metode kriptografi asimetris, dimana menggunakan 2 buah kunci, yaitu kunci publik dan kunci private.

8. DAFTAR PUSTAKA

Buku:

Ariyus, Dony. 2008, *Pengantar Ilmu Kriptografi*. Yogyakarta: CV. ANDI OFFSET.

Febrian, Jack. 2006. *Pengetahuan Komputer & Teknologi Informasi*. Bandung : Informatika.

Imron, Mahud. 2013, *Aljabar Linear Dasar Edisi Kedua*. Jakarta: Erlangga.

Jogiyanto. 2009, *Analisis & Desain Sistem Informasi : Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis*, Yogyakarta : Penerbit Andi.

Koswara, Eko. 2011, *Visual Basic 6 Beginner Guide*, Yogyakarta: Penerbit Mediakom.

Kurniawan, Agus. 2008, *Konsep dan Implementasi Cryptography Dengan .NET* .Jakarta: PC Media.

Ladjamudin, Al Bahra. 2006, *Analisis dan Desain Sistem Informasi*, Tangerang : Penerbit Graha Ilmu.

Munir, Renaldi. 2006, *Pengantar Kriptografi*, Bandung: Informatika.

Sommerville, Ian. 2011, *Software Engineering (Rekayasa Perangkat Lunak)*. Jakarta: Airlangga.

Sutojo, T. 2010, *Teori dan Aplikas Aljabar Linear dan Matriks*, Semarang: CV. ANDI OFFSET.

Jurnal Ilmiah:

Edisuryana, M., Isnanto, R.R., dan Somantri, M. 2013, *Aplikasi Steganografi Pada Citra Berformat Bitmap Dengan Menggunakan Metode End of File*, Universitas Diponegoro Semarang

Arifin, R., dan Oktaviana, L.T. 2013, *Implementasi Kriptografi dan Steganografi Menggunakan Algoritma RSA dan Metode LSB*, Universitas Malang.

Wicaksono, S.R. 2011, *Proteksi Dokumen Word Dengan Kombinasi Enkripsi Vernam Cipher dan Shift Transposition*, Universitas STIKOM Surabaya.

Artikel dari situs internet:

ASCII table and Extended ASCII Table, www.asciitable.com, diakses pada tanggal 16 Maret 2015