Techno.COM, Vol. 13, No. 3, Agustus 2014: 150-157

GABUNGAN ALGORITMA VERNAM CHIPER DAN END OF FILE UNTUK KEAMANAN DATA

Christy Atika Sari[1], Eko Hari Rachmawanto[2]
[1,2]Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jalan Nakula 1 No.5-11, Semarang, 50131, Telp. 024-3517261
E-mail : atikasari@research.dinus.ac.id[1], rachmawanto@research.dinus.ac.id[2]

Abstrak

Adanya kesamaan fungsi pada metode Kriptografi dan Steganografi untuk mengamankan data, maka makalah ini menggunakan algoritma Vernam Cipher sebagai salah satu algoritma yang popular pada Kriptografi dan End Of File (EOF) pada metode Steganografi. Vernam Cipher mempunyai kemampuan untuk menyembunyikan data karena proses enkripsi dan dekripsi menggunakan sebuah kunci yang sama. Kunci ini berasal dari perhitungan XOR anatar bit plainteks dengan bit kunci. Sedangkan EOF dikenal sebagai pengembangan dari metode Least Significant Bit (LSB). EOF dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Pada penelitian ini digunakan file asli berformat .mp3 dan file spoofing berformat .pdf. file hasil stegano berhasil di ekstraksi menjadi file asli dan file spoofing. Ukuran file yang telah melalui proses penyisipan sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam file tersebut.

Kata Kunci: *Vernam Chiper, End Of File, Kriptografi, Steganografi.*

Abstract

The similarity function on Cryptography and Steganography method for secure data, then this paper uses Vernam cipher algorithm as one of the popular algorithms in cryptography and the End Of File (EOF) in Steganography methods. Vernam Cipher has the ability to hide data for encryption and decryption using a common key. This key is derived from the XOR calculations anatar bit plaintext with the key bits. While EOF is known as the development of a method of Least Significant Bit (LSB), EOF can be used to insert data size according to needs. In this study, the original file format, MP3 and spoofing file format, PDF, Stegano file extraction be successful in the original file and the file spoofing. The size of files that have been through the same insertion process with a file size of data inserted before plus the size of the data that is inserted into the file.

Keywords: *Vernam Chiper, End Of File, Cryptography, Steganography.*

1. PENDAHULUAN

Perkembangan yang pesat dalam proses pengiriman data membawa dampak yang besar, yaitu masalah keamanan data yang di kirim. Untuk itu, tidak mungkin mengirim data melalui media-media tersebut secara polos (*plain*), melainkan harus dilakukan proses pengamanan untuk data yang akan di kirim, salah satunya dilakukan dengan cara melakukan enkripsi pada sebuah file.

Kriptografi dapat menjadi jawaban dari masalah tersebut. Sebagai ilmu yang telah diaplikasikan untuk pengamanan data, kriptografi 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 [1].

Dalam perkembangan ilmu kriptografi masa sekarang ini, telah banyak tercipta algoritma-algoritma yang dapat digunakan untuk mengubah data asli (*plain text*) menjadi simbol tertentu (*chiper text*) [2]. Salah satu contohnya adalah algoritma *Vernam Chiper*. Algoritma ini termasuk dalam algoritma *kriptografi* modern dan merupakan algoritma *stream chipper* [3].

Namun pada era sekarang ini masih di rasa kurang dalam pengamanan data menggunakan kriptografi. Setelah file tersebut dienkripsi, kita perlu melakukan penyembunyian file ke dalam file lain supaya pihak yang bukan berkepentingan tidak begitu curiga dalam melihat file tersebut. Langkah seperti ini sering disebut dengan Steganografi.

Steganografi merupakan salah satu cara yang sangat efektif untuk mengurangi rasa curiga dari pihak-pihak lain (selain pengirim dan penerima yang sah). Dalam perkembangannya, steganografi mempunyai berbagai macam metode yang dapat digunakan untuk menyembunyikan file tersebut. Salah satu contohnya adalah metode *End of File* (EOF) [4].

Terdapat perbedaan antara steganografi dengan kriptografi. Pada steganografi, penyembunyian pesan dibuat dengan tujuan pihak lain tidak mengetahui bahwa ada pesan lain di dalam pesan yang dikirim. Pesan inti tersebut tetap dipertahankan, dalam penyampaiannya dikaburkan atau disembunyikan dengan berbagai cara. Hanya pihak penerima yang sah saja yang dapat mengetahui pesan lain tersebut. Sedangkan pada kriptografi, karakter pesan diubah atau diacak menjadi bentuk lain yang tidak bermakna. Pesan yang disampaikan dalam kriptografi menjadi lebih mencurigakan karena makna yang ada pada media yang digunakan. Sedangkan pesan dalam steganografi, terlihat seperti pesan biasa sehingga kecil kemungkinan untuk dicurigai. Namun demikian, bukan berarti tidak ada kekurangan pada steganografi ini. Kelemahan pada steganografi ini terjadi apabila kita mengubah format pesan yang dikirimkan, maka pesan rahasianyapun menjadi hilang.

Berdasarkan keunggulan dari kedua algoritma tersebut, makalah ini menganalisa kemampuan gabungan dari Vernam Chiper dan *End Of File* untuk mengamankan email.

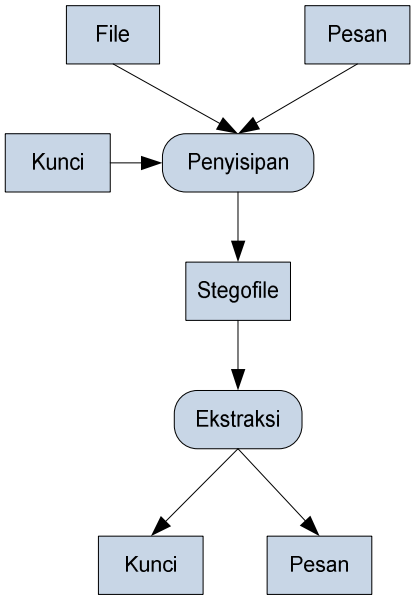
Beberapa penelitian mengenai steganografi dan kriptografi telah dilakukan melalui berbagai teknik dan aplikasi tertentu.

Steganografi diterapkan melalui teknik *End Of File* (EOF) dan LSB [5,9], pada penelitian yang dilakukan oleh Aditya [5] menggunakan file induk berupa gambar dan file pesan berupa teks, dan dihasilkan kualitas gambar setelah proses penyisipan pesan lebih baik dibanding metode LSB, tetapi ukuran gambar berubah. Pada penelitian yang dilakukan oleh Krisnawati [9], menggunakan citra *grayscale* dimana proses stegano berhasil dan dalam penelitian ini jumlah karakter pesan yang disispkan masih terbatas sehingga besarnya citra harus menyesuaikan bersarnya pesan yang digunakan.

Steganografi dengan teknik EOF juga telah dilakukan pada media video MP4 dan pesan berupa teks [7]. EOF juga telah di-*hybrid* dengan teknik rijndael

[8,10], sedangkan Mukharrom menggabungkan EOF dengan teknik kriptografi yaitu Caesar chipper [6]. Kriptografi juga telah diterapkan dengna menggunakan teknik kripto ESB [11], vernam chiper dan permutasi chipper [12], stream chiper [13], LSB dan trile DES [14].

Steganografi di dunia modern biasanya mengacu pada informasi atau suatu arsip yang telah disembunyikan ke dalam suatu arsip citra digital, audio, atau video [7]. Berikut ini merupakan proses sederhana pada teknik steganografi:



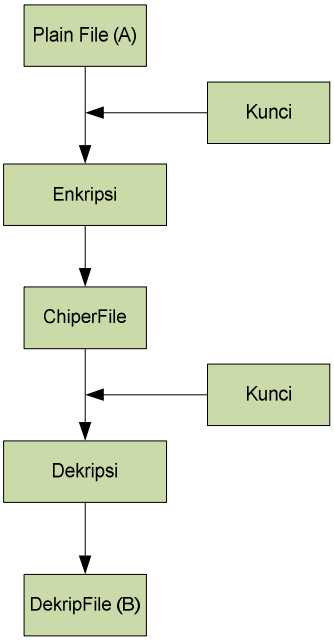
Gambar 1. Penyisipan Pesan pada Steganografi

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.

Tujuan steganografi adalah merahasiakan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi [7,9].

Kriptografi tidak sekedar berupa kerahasiaan data (*privacy*) saja, tapi juga bertujuan untuk menjaga integritas data (*data integrity*), keaslian data (*authentication*) dan anti penyangkalan (*non-repudiation*) [1].

Di dalam kriptografi terdapat 5 hal utama yaitu enkripsi, dekripsi, dan kunci (*key*), pengirim, dan penerima. Enkripsi merupakan proses penyandian *plainteks* (pesan awal) menjadi *cipherteks* (pesan yang tersandikan), sedangkan dekripsi merupakan kebalikan dari proses enkripsi. Baik proses enkripsi dan dekripsi, keduanya menggunakan kunci untuk menjaga kerahasiaan data.



Gambar 2. Skenario Dasar Kriptografi

Di dalam skenario dasar kriptografi, seperti yang diperlihatkan pada Gambar 1, terdapat dua belah pihak, sebut saja A dan B, yang ingin berkomunikasi satu sama lain. Kemudian pihak ketiga, C, adalah seorang *eavesdropper* (orang yang mengakses informasi rahasia tanpa izin). Ketika A ingin mengirimkan informasi, yang disebut *plaintext*, kepada B, dia mengenkripsi *plaintext* tersebut dengan menggunakan metode yang telah dirancang oleh B. Biasanya, metode enkripsi diketahui oleh si *eavesdropper*, dalam hal ini adalah C. Yang membuat pesan tersebut tetap bersifat rahasia adalah *key*-nya. Ketika B menerima pesan yang telah dienkripsi, yang disebut dengan *ciphertext*, dia mengubahnya kembali menjadi *plaintext* dengan menggunakan *key* dekripsi.

$$C = E(M) \quad (1)$$

dimana :
M = pesan asli
E = proses enkripsi
C = pesan dalam bahasa sandi (untuk ringkasnya disebut sandi)

Sedangkan dekripsi adalah proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali.

$$M = D(C) \quad (2)$$

D = proses dekripsi

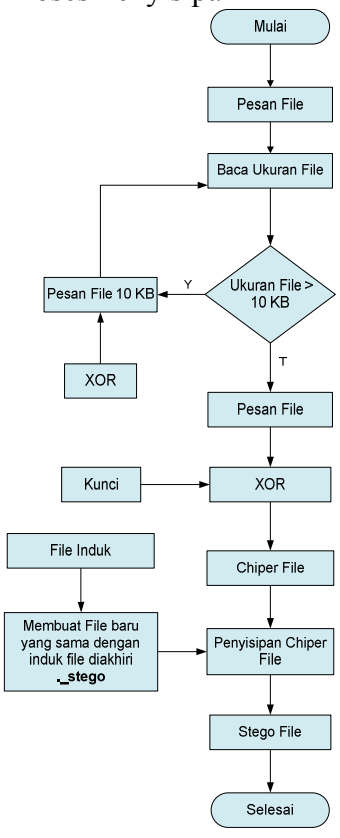
Umumnya, selain menggunakan fungsi tertentu dalam melakukan enkripsi dan dekripsi, seringkali fungsi itu diberi parameter tambahan yang disebut dengan istilah kunci [5].

Vernam Cipher diciptakan oleh Mayor J. Maugborne dan G. Vernam pada tahun 1917. Algoritma Vernam Chiper merupakan algoritma berjenis *symetric key*, yaitu kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara stream cipher yang berasal dari hasil XOR antara bit plaintext dan bit key.

End Of File (EOF) 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. EOF merupakan pengembangan dari metode *Least Significant Bit* (LSB). LSB menambahakan data file pada akhir bit-nya, maka EOF langsung menambahkan data di akhir file.

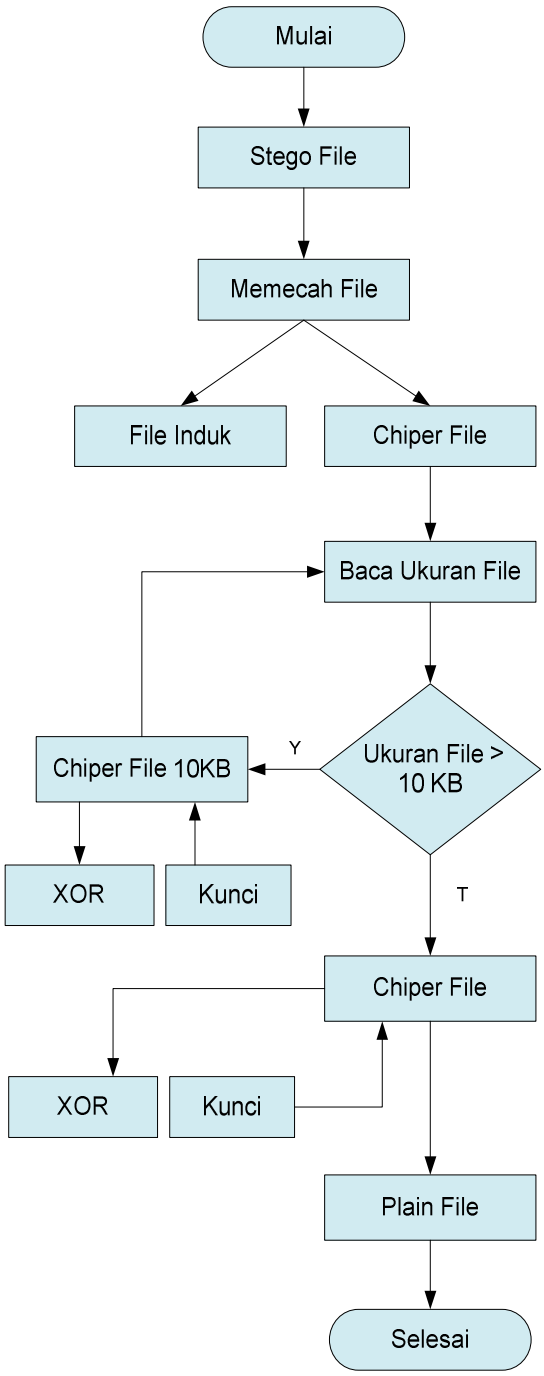
2. METODE

a. Proses Penyisipan



Gambar 3. Flowchart Proses Penyisipan File

b. Proses Ekstraksi

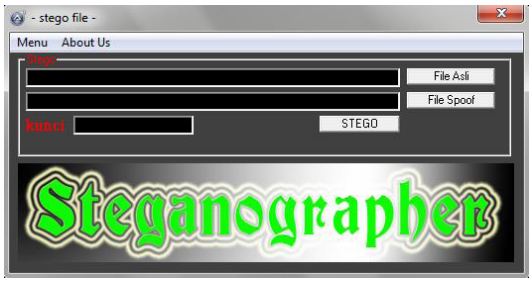


Gambar 4. Flowchart Proses Ekstraksi File

3. HASIL DAN PEMBAHASAN

Pada penelitian ini, percobaan menggunakan file .pdf sebagai filu induk dan file .mp3 sebagai file yang disisipkan. Aplikasi Kriptografi dan Steganografi ini dibuat dengan bahasa pemrograman Visual Basic 6.0.

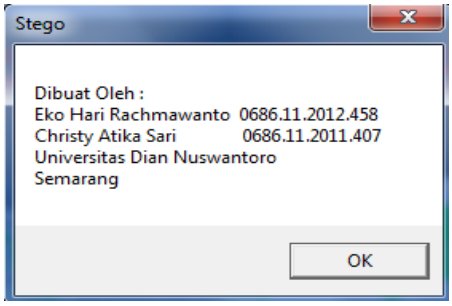
Gambar 5. Tampilan Awal Aplikasi



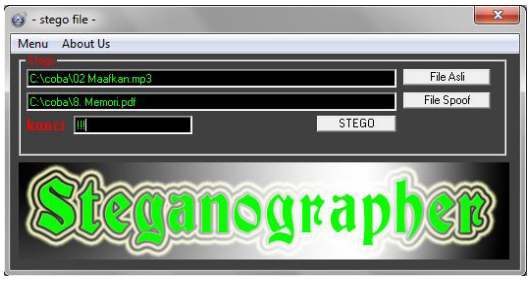
Gambar 6. Menu Utama Aplikasi

Program Kripto dan Stego ini dimulai dengan memproses file stego terlebih dahulu.

Gambar 7. Menu Input Penyisipan File



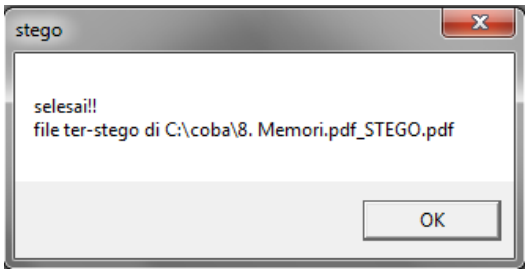
Gambar 8. Menu About Us



Gambar 9. Input File .pdf dan File .mp3 Pada Proses Penyisipan File

Pada Gambar 9 di atas, digunakan file asli yaitu "02 Maafkan.mp3". File Spoof merupakan file induk di mana file ini sebagai tempat persembunyian dari file asli, dalam penelitian ini menggunakan file "8. Memori.pdf" sebagai tempat persembunyian file aslinya.

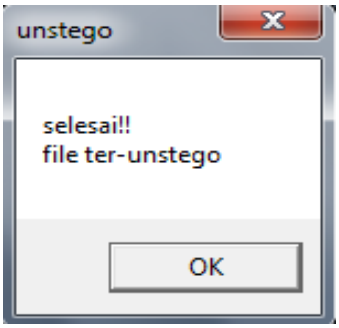
Selanjutnya yang dilakukan adalah memberikan kata kunci sebagai penyempurna keamanan data. Pada gambar terdapat 3 tanda seru (!) yang pada sebenarnya adalah 3 (tiga) huruf sandi. Kemudian tekan tombol Stego untuk memproses pada langkah-langkah selanjutnya.



Gambar 10. Alert Stego Berhasil

Gambar 11. Proses Unstego (Ekstraksi File)

Gambar 11 menunjukkan tampilan menu Unstego. Menu in idigunakan untuk mengembalikan file yang telah di proses sebelumnya dengan cara memasukkan file yang telah ter-Stego yaitu file "8. Memori.pdf_STEGO.pdf". Kemudian memasukkan kata kunci yang telah digunakan sebelumnya, sehingga akan muncul kedua file yang telah dilakukan pada proses penyisipan sebelumnya.



Gambar 12. Alert Proses Unstego Berhasil

Apabila proses telah selesai maka akan muncul tampilan *Message Box* seperti Gambar 12 menunjukkan bahwa file telah ter-unstego dengan baik dan benar. Setelah itu tekan tombol "OK" untuk mengakhiri perintah, sehingga akan muncul file asli.

4. KESIMPULAN DAN SARAN

Kriptografi dan Steganografi merupakan metode penyisipan pesan yang popular. Penelitian ini menggunakan Vernam Chiper pada Kriptografi dan EOF pada Steganografi.

Proses pemecahan file dilakukan dengan tujuan mempermudah proses XOR pada file yang telah dipilih. Pembuatan aplikasi menggunakan Visual Basic 6.0. pda penelitian ini menggunakan file. Mp3 dan file .pdf. Implementasi pada ukuran dan jenis file yang berbeda serta hasil akhir file stego yang dapat diekstraksi kembali menjadi file asli menggunakan kunci yang sama telah membuktikan bahwa kemampuan enkripsi dan dekripsi pada Vernam Cipher tetap dapat berjalan dengan baik, sedangkan penambahan ukuran file disebabkan oleh penggunaan EOF pada proses penggabungan file. Ukuran file stego akhir merupakan gabungan ukuran dari file asli dan file spoofing.

DAFTAR PUSTAKA

[1] Frank J. Mabry, dkk, Unicode Steganographic Exploits Maintaining Enterprise Border Security, IEEE Security and Privacy, 2007.

[2] Debbie W. Leung, Quantum Vernam Cipher, Quantum Information and Computation, Vol. 1, 2001, Rinton Press.

[3] O Tornea, dkk, DNA Vernam Cipher, Proceedings of the 3rd International Conference on E-Health and Bioengineering (EHB) November 2011.

[4] Sembiring, Sandro, Perancangan Aplikasi Steganografi Untukk Menyisipkan Pesan Teks Pada Gambar Dengan Metode EOF, Pelita Informatika Budi Darma, Vol. IV, No. 2, Agustus 2013.

[5] Aditya, Yogie, dkk, Studi Pustaka Untuk Steganografi Dengan Beberapa Metode, Seminar Nasional Aplikasi Teknologi Informasi (SNATI), 2010.

[6] Edisuryana, Mukharrom, dkk, Aplikasi Steganografi Pada Citra Berformat Bitmap Dengan Menggunakan Metode EOF, TRANSIENT, Vol.2, No. 3, Sepetember2013.

[7] Azhari, AI, dkk, Aplikasi Steganografi Pada Berkas Video MP4 Dengan Menggunakan Bahasa Pemrograman Java.

[8] Sukrisno, Utami E., Implementasi Steganografi Teknik EOF Dengan Gabungan Enkripsi Rijndael, Shift Cipher dan Fungsi Hash MD5. Seminar Nasional Teknologi (SNT), 2007.

[9] Krisnawati, Metode LSB dan EOF Untuk Menyisipkan Pesan Teks Ke Dalam Citra Grayscale, Seminar Nasional Informatika (semnasIF), 2008.

[10] Wasino, dkk, Impementasi Teknik EOF Dengan Enkripsi Rijndael, Seminar Nasional Teknologi Informasi dan Komunikasi (SENTIKA), 2012.

[11] Putra .C, dkk, Implementasi Kriptografi Untuk Pengamanan Data Sensitif Pada Aplikasi Rekam Medis.

[12] M. Sholeh, J.V. Hamokwarong, Aplikasi Kriptografi Dengan Metode Vernam Cipher dan Metode Permutasi Biner, Momentum, Vol. 7, No. 2, Oktober 2011 : 8- 13.

[13] Y.Yohakim Marwanta, Aplikasi Pengamanan Basis Data dengan Teknik Kriptografi Stream Cipher.

[14] Agus Prihanto, Wahyuningsih, Penyembunyian dan Pengacakan Data Text Menggunakan Steganograf dan Kriptografi Triple DES pada Image, Seminar Nasional Pengamanan Jaringan (SNiPer), STIKOM PGRI Banyuwangi, 2009.

[15] Warsito AB, Proteksi Keamanan Dokumen Setifikat File JPEG Pada Perguruan Tinggi Dengan Menggunakan Steganografi and Kriptografi, Jurnal Telematika Vol.4 No.1, Maret 2012.