IMPLEMENTASI VERNAM CIPHER DAN STEGANOGRAFI END OF FILE (EOF) UNTUK ENKRIPSI PESAN PDF

Marsela Sutikno Dibiyo[1], Aisyatul Karima[2]
[1,2]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Nakula 1 No 5-11 Semarang 50131 (024) 3569196
Email: 111201105905@mhs.dinus.ac.id[1], aisyatul.karima@dsn.dinus.ac.id[2]

Abstrak

Keamanan pesan dalam proses pengiriman informasi menjadi hal yang sangat penting, dikarenakan meningkatnya tingkat kebutuhan masyarakat akan jaminan keamanan. Dengan metode konvensional, masyarakat mengamankan pesan format Word dengan melakukan konversi ke format PDF dengan harapan pesan tidak dapat dirusak oleh pihak yang tidak berwenang. Namun format PDF juga rentan terhadap kerusakan serta keamanan informasi yang terdapat di dalamnya juga tidak terjamin ,karena orang lain bisa mengetahui secara jelas serta bisa dengan mudah melakukan modifikasi isi dari pesan format PDF. Oleh karena itu, diperlukan sebuah alat bantu yang mampu menjaga keaslian dan kerahasiaan pesan tersebut.Metode yang diimplementasikan adalah dengan mengubah pesan asli menjadi pesan acak yang sudah dienkripsi oleh suatu kunci. Selain itu pesan yang sudah diubah menjadi pesan acak harus disembunyikan ke sebuah media. Algoritma yang digunakan untuk mengacak pesan rahasia tersebut adalah kriptografi Vernam Cipher yang dikombinasikan dengan Steganografi End of File untuk menyembunyikan pesan yang sudah dienkripsi ke dalam media gambar .Hasil yang diperoleh bahwa pesan yang sudah terenkripsi dengan Vernam Cipher dan disisipkan ke dalam media gambar dengan metode end of file tidak mengalami perubahan gambar secara kasat mata, karena metode steganografi end of file tidak akan mengubah kualitas gambar / citra.

***Kata Kunci** : Kriptografi, Vernam Cipher, Steganografi, End of File, media gambar.*

Abstract

The security message in sending information becomes a major thing because the demand of security guarantee increases significantly. Through conventional method, people tend to protect their file by converting Word format to PDF so that their file cannot be corrupted by others. However PDF format has some weaknesses such as corrupted file and unsecure information, people can easily modify the PDF format message. Therefore people need software to protect the original message and security message. The method has implemented by converting the original message (plaintext) into the ciphertext with the key. After encryption process the ciphertext must be hidden on the media. The Cryptography algorithm that is used Vernam Cipher combines with the End of File (EoF) Steganography to hide the ciphertext into image media. The result shows that the ciphertext image has encrypted using Vernam Cipher and the End of File unchanged by visualizes observation, because the End of File (EoF) steganography did not change the quality of image.

***Keywords :** Cryptography, Vernam Cipher, Steganography, End of File, image.*

1. PENDAHULUAN

Data berupa suatu keadaan, gambar, suara, huruf, angka, matematika, bahasa ataupun simbol-simbol lainnya yang digunakan sebagai bahan untuk melihat lingkungan, objek, kejadian ataupun suatu konsep [1]. Data yang berupa pesan teks merupakan pesan yang tiap hari digunakan masyarakat untuk mengirim informasi penting dari pengirim kepada penerima.

Perkembangan pesan teks semakin pesat, karena tingkat kebutuhan masyarakat yang sangat tinggi dalam pengiriman informasi. Berawal dari pesan teks yang menggunakan microsoft word ke PDF, dahulu orang-orang menggunakan microsoft word untuk menyimpan pesan yang akan disampaikan ke penerima, karena kawatir pesan itu dimodifikasi atau dirusak oleh pihak-pihak lain maka pesan berformat word itu kemudian dirubah menjadi pesan yang berformat PDF.

Namun seiring perkembangan teknologi, keamanan pesan rahasia dalam format PDF sudah tidak aman lagi, karena semakin banyak aplikasi yang bisa merubah atau merusak pesan dalam format PDF. Misalnya mengganti nama penulis makalah milik orang lain dalam format PDF, dengan berbagai aplikasi tersebut sangatlah mudah untuk merubah nama yang diinginkan [2]. Oleh sebab itu, si pengirim pesan membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan informasi atau data yang akan dikirim ke penerima.

Salah satu sistem keamanan yang digunakan pada saat ini adalah kriptografi yang memiliki kemampuan penyandian pesan sehingga pesan terlihat sepeti diacak. 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) [3] [4].

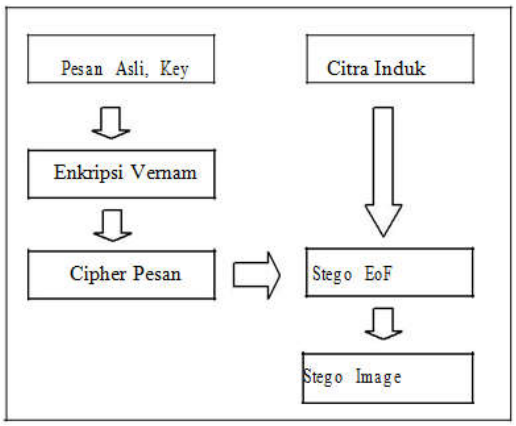
Algoritma kriptografi yang akan digunakan adalah algoritma kriptografi vernam cipher dan bersifat simetris bersifat sehingga data hasil enkripsi (cipherteks) mempunyai ukuran yang sama dengan data asli (plainteks). Teknik kriptografi simetris dipilih karena diharapkan dengan algoritma ini proses enkripsi – dekripsi data dapat dilakukan dengan waktu yang lebih cepat dibandingkan dengan algoritma kriptografi kunci publik (asimetris). Selain itu, algoritma ini beroperasi pada plainteks/cipherteks dalam bentuk bit tunggal sehingga enkripsi dan dekripsi pesan dalam bentuk bit per bit [5].

Namun, kelemahan dari algoritma Vernam Cipher ini adalah hasil enkripsi yang masih tampak oleh mata manusia, sehingga mudah dikenali sebagai data yang telah mengalami proses enkripsi. Oleh sebab itu, perlu menyembunyikan data yang sudah dienkripsi ke dalam gambar supaya pihak yang tidak berkepentingan tidak merasa curiga dalam melihat gambar tersebut. Teknik penyembunyian data ke dalam gambar ini disebut dengan teknik steganografi. Berdasarkan [6] implementasi kriptografi yang dikembangan menggunakan dua metode enkripsi dan dekripsi dengan kunci tertentu untuk mengamankan dan menjamin kerahasiaan data. Oleh karena itu, penulis menggabungkan dua metode yaitu kriptografi Vernam Cipher dengan steganografi End of File.

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Algoritma steganografi End of File memiliki tingkat keamanan yang cukup baik [7][8][9]. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi.

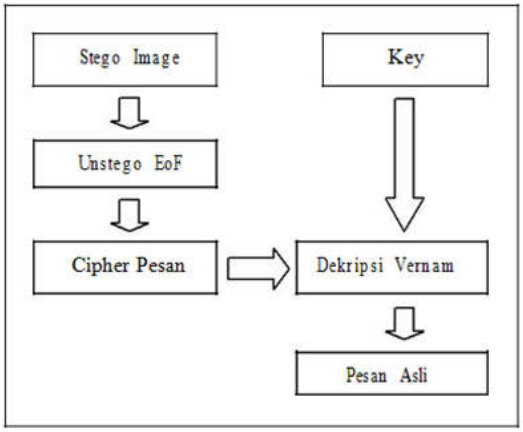
2. METODE

Adapun metode yang diusulkan adalah pesan asli atau plainteks dengan kunci dienkripsikan menggunakan algoritma kriptografi vernam cipher dan menghasilkan data berupa cipherteks. Selanjutnya cipherteks disisipkan ke dalam sebuah citra mengunakan steganografi end of file yang akan menghasilkan Stego Image yang terdapat pada gambar 1.



Gambar 1. Metode Enkripsi Data

Dekripsi data dengan cara unstego *stego image* hasil enkripsi diatas akan menghasilkan *cipherteks*, lalu dengan kunci yang sama untuk mengenkripsi pesan awal tadi digunakan untuk mendekripsi *cipherteks* dan menghasilkan pesan asli atau *plainteks*. Terdapat dalam gambar 2 dibawah ini.



Gambar 2. Metode Dekripsi Data

3. HASIL DAN PEMBAHASAN

Berdasarkan metode yang digunakan, proses enkripsi diawali dengan pesan asli (plaintext) yang dienkripsi menggunakan algoritma Vernam disertai dengan kunci yang sudah ditentukan. Pesan asli berupa file berekstensi PDF yang selanjutnya akan kita sisipkan ke dalam gamba / citra induk yang merupakan media untuk menyembunyikan, sesuai pada gambar 3 berikut ini.

Gambar 3. Proses Stego

Gambar 3 diatas merupakan proses stego. File pdf yang akan disembunyikan adalah "keplek.pdf" . Gambar yang digunakan sebagai media merupakan file induk dimana file ini sebagai tempat persembunyian dari file asli. Tahap kedua adalah memilih file induk dimana file asli akan disembunyikan. Dalam hal ini, dipilih gambar "images.jpg" sebagai tempat penyembunyian file asli. Setelah itu masukan kata kunci dan tekan tombol stego untuk memproses stego file tersebut.

Gambar 4. Proses UnStego

Pada gambar 4 diatas merupakan proses unstego file yang akan mengembalikan file stego ke file asli. Proses Unstego ini merupakan proses dekripsi dari file PDF yang sudah disisipkan ke dalam media gambar (ciphertext) menjadi file PDF semula (plaintext).

Proses unstego diawali dengan mengubah stego image menggunakan algoritma EoF menjadi sebuah ciphertext. Selanjutnya adalah proses dekripsi dengan algoritma vernham dengan kunci yang sudah ditentukan sebelumnya. Hasil akhir dari dekripsi inilah yang merupakan file PDF semula atau yang disebut dengan istilah pesan asli (plaintext).

Pengujian aplikasi dilakukan dengan metode random sampling, yakni mengambil masing – masing 15 sampel file pdf dan 15 sampel data gambar guna diujikan pada aplikasi. File kemudian diujikan pada aplikasi untuk melihat hasil akhir dari enkripsi dan stego yang diproses pada aplikasi. Untuk pengujian, penulis memasukkan kunci sama untuk tiap-tiap percobaan, kunci yang dimasukkan adalah “123”.

Masing – masing data akan diujikan ke aplikasi. Pertama, data pdf akan diproses dengan algoritma vernam cipher, proses ini disebut dengan proses enkripsi. Pada proses enkripsi bertujuan mengacak file pdf atau dapat disebut pesan rahasia agar pihak lain yang tidak berwenang tidak dapat menemukan makna atau pesan rahasia di dalamnya.

Kemudian hasil dari proses enkripsi tadi akan diproses guna menyembunyikan file hasil enkripsi tersebut dalam sebuah citra atau gambar. Proses itu sendiri disebut dengan proses stego. Untuk kedua proses ini, baik enkripsi maupun stego atau sebaliknya proses dekripsi maupun unstego, pengguna akan diminta memasukkan sebuah kunci. Dimana kunci ini sama antara kedua proses tersebut, untuk mempercepat waktu dalam proses enkripsi maupun dekripsi.

Tabel 1: Tabel Pengujian

No	File PDF	Gambar	Ukuran File PDF	Ukuran Gambar	Ukuran Gambar Stego	Ukuran File PDF Enstego
1	Keplek.pdf	images.jpg	68 KB	8 KB	75 KB	68 KB
2	Abstrak.pdf	aman.jpg	5 KB	87 KB	91 KB	5 KB
3	Eof.pdf	burung.jpg	240 KB	9 KB	248 KB	240 KB
4	Eof2.pdf	gembok.jpg	311 KB	199 KB	510 KB	311 KB
5	Eof3.pdf	kelinci.jpg	238 KB	6 KB	244 KB	238 KB
6	Judul TA.pdf	krip.jpg	101 KB	42 KB	142 KB	101 KB
7	Pengajuan.pdf	kucing.jpg	101 KB	5 KB	106 KB	101 KB
8	Stream1.pdf	panda.jpg	187 KB	9 KB	196 KB	187 KB
9	Tes.pdf	penguin.jpg	299 KB	7 KB	305 KB	299 KB
10	Test.pdf	security.jpg	279 KB	300 KB	579 KB	279 KB
11	Serpen.pdf	angry.jpg	40 KB	8 KB	48 KB	40 KB
12	Mars.pdf	bibo.jpg	126 KB	7 KB	132 KB	126 KB
13	Pesan.pdf	bird.jpg	282 KB	11 KB	293 KB	282 KB
14	Rijndael.pdf	bob.jpg	279 KB	9 KB	288 KB	279 KB
15	Cipher.pdf	cool.jpg	103 KB	7 KB	109 KB	103 KB

Berdasarkan tabel 1 diatas menunjukkan adanya perbedaan antara ukuran gambar sebelum proses stego dan setelah proses stego, dimana ukuran akan bertambah besar. Hal ini disebabkan karena prinsip metode steganografi End of File ini sederhana, yaitu menambahkan file pdf dibelakang file gambar. Dengan proses seperti itu, tentunya jumlah ukuran file itu akan bertambah. Pertambahan ukuran file ini dapat dirumuskan yaitu besar ukuran file pdf ditambahkan dengan besar ukuran file gambar itu sendiri. Seperti dapat dilihat di tabel 7, ukuran file images.jpg setelah proses stego menjadi 75 KB. Jika dilihat ukuran data sebelumnya, yaitu file pdf yang telah dienkripsi sebesar 68 KB jika ditambah dengan ukuran file gambar sebelum stego sebesar 8 KB maka angka 75 KB adalah hasil dari penambahan ukuran kedua file tersebut. Namun, meskipun terjadi penambahan besar ukuran file gambar, metode steganografi end of file ini memiliki kelebihan dibandingkan dengan metode lainnya yaitu secara kasat mata, tidak ada perbedaan dari kedua gambar sebelum dan sesudah proses stego. Untuk membuktikan kelebihan metode steganografi end of file ini, perlu dilakukan perbandingan antara citra sebelum dan sesudah proses stego. Maka, berikut penulis tampilkan beberapa citra induk sebelum dan sesudah stego :

Gambar 5. Kelinci.jpg sebelum stego

Gambar 6. Kelinci.jpg setelah stego

Dari pengujian yang telah dilakukan, menunjukkan bahwa untuk proses stego dengan metode steganografi end of file tidak akan merubah kualitas gambar sehingga pada gambar yang sudah distego tidak akan menimbulkan kecurigaan untuk pihak yang tidak berwenang maupun yang akan merusak file tersebut, namun akan memperbesar ukuran file karena merupakan penambahan antara ukuran file pesan rahasia dan file induk berupa file gambar.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Dari penelitian yang telah dilakukan, maka dapat disimpulkan :

a. Aplikasi KriptoStego dapat mengamankan data rahasia dengan baik menggunakan kriptografi *vernam cipher* dan steganografi *end of file*, karena pihak ketiga tidak menyadari adanya pesan rahasia dalam sebuah gambar yang sudah disembunyikan.
b. Hasil gambar dengan metode *end of file* setelah disisipkan pesan hasil enkripsi *vernam cipher* dari proses KriptoStego tidak mengalami perubahan gambar secara kasat mata karena metode steganografi *end of file* yag digunakan tidak akan mengubah kualitas gambar / citra.

c. Aplikasi kriptografi *vernam cipher* dan steganografi *end of file* ini dapat mengenkripsi *file* dan mendekripsi *file* dengan baik. Karena terbukti bahwa dengan aplikasi ini dapat menyimpan pesan rahasia dari pengirim untuk sampai ke penerima tanpa adanya kerusakan pesan setelah proses unstego dan pengirim dapat menjamin tidak adanya perubahan file setelah sampai ke penerima. Namun mengalami perubahan ukuran file yang bertambah besar karena terjadi pertambahan ukuran dari kedua *file* tersebut.

4.2 Saran

Dari kesimpulan yang telah diuraikan penulis diatas, saran untuk pengembangan aplikasi KriptoStego adalah sebagai berikut :

a. Aplikasi dapat dikembangkan lagi menggunakan metode lain yang tidak berpengaruh pada ukuran pesan ciphertext.
b. Aplikasi dapat dikembangkan dengan bahasa pemrograman lain yang lebih powerfull dan lebih cepat.

DAFTAR PUSTAKA

[1] Anonimous, ASCII Table and Extended ASCII Table, www. Asciitable . com,10 Agustus 2009
[2] Ramnul. (2012). Cara Mengedit File PDF. Retrieved from http://ramnul.us/2012/07/cara-edit-file-pdf-tanpa-adobe-acrobat.html.
[3] Nathasia, N. D., & Wicaksono, A. E. (2011). Penggunaan Teknik Kriptografi Stream Cipher untuk Pengamanan Basis Data. *Jurnal Basis Data, ICT Research Center UNAS*, 6(1), 1-22.
[4] Sukrisno, & Utami, E. (2007). Implementasi Steganografi Teknik EoF dengan Gabungan Enkripsi Rijndael, Shift Cipher dan Fungsi Hash MD5. *Seminar Nasional Teknologi 2007 (SNT 2007)*, (November), 1-16.
[5] Arifpriyanto, B. (2013). Penyembunyian Pesan Text Terenkripsi Menggunakan Metode Kriptografi Stream Cipher dan Steganografi End Of File (EOF) dengan File Induk PDF. *Dokumen Karya Ilmiah Tugas Akhir Program Studi Teknik Informatika – S1 Fakultas Ilmu Komputer Universitas Dian Nuswantoro Semaranng 2013*, 2013, 1-6.
[6] Sholeh, M., & Hamokwarong, J.V. (2011). Aplikasi Kriptografi Dengan Metode Vernam Cipher dan Metode Permutasi Biner. *Momentum,* 7(2), 8-13.
[7] Iswahyudi, C., Setyaningsih, E., & Widyastuti, N. (2012). Pengamanan Kunci Enkripsi Citra pada Algoritma Super Enkripsi Menggunakan Metode End Of File. Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) Periode III, (November), 278-285.
[8] Aditya, Y., Pratama, A., & Nurlifa, A. (2010). Studi Pustaka untuk Steganografi dengan Beberapa Metode. Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI 2010), 2010, 32-35.
[9] Wandani, H., Budiman, M., & Sharif, A. (2012). Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi End Of File (EOF) dan Rabin Public Key Cryptosystem. Alkhawarizmi. Retrieved from http://jurnal.usu.ac.id/index.php/alkhawarizmi/article/view/500