STEGANOGRAFI PADA PESAN TERKOMPRESI HUFFMAN MENGGUNAKAN ALGORITMA GIFSHUFFLE (STEGANOGRAPHY OF HUFFMAN COMPRESSED MESSAGE USING GIFSHUFFLE ALGORITHM)

Firman Adriansyah Ginting[1], Adiwijawa[2], Agung Toto Wibowo[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Pada tugas akhir ini akan dirancang dan diimplementasikan blind steganografi pada citra digital mengunakan algoritman Gifshuffle. Graphics Interchange Format (GIF) adalah sebuah format yang sering digunakan karena ukurannya yang relative kecil dan juga banyaknya software editor gambar yang telah mendukung citra ini. GIF berukuran kecil karena membatasi jumlah warnanya sebanyak 256 warna sehingga dapat menghemat ukuran berkas.

Algoritma Gifshuffle yang dikembangkan oleh Matthew Kwan adalah salah satu algoritma steganografi yang mengunakan berkas citra dengan format GIF. Dalam algoritma Gifshuffle terdapat proses encoding dan juga decoding. Algoritma ini melakukan penyisipan pesannya dengan cara mengganti ururan palet warna yang terdapat pada citra GIF. Aplikasi yang dibuat dalam penelitian ini tidak hanya mengimplementasikan algoritma Gifshuffle, tetapi juga mengimplementasikan algoritma Huffman sebagai kompresi dari pesan yang diinputkan, sehingga pesan yang disisipkan dapat lebih banyak.

Setelah dilakukan perancangan dan implementasi, dilakukan pengujian terhadap citra stego untuk melihat ketahanannya terhadap serangan. Adapun jenis attack yang diuji adalah rotate (skala rotasi 30° : 45° : 60° : 90°), rescale (skala rescale 0.25: 0.5: 0.75: 0.99), dan salt and pepper noise (skala noise 0.05 : 0.1 : 0.25 : 0.5).

Dari hasil pengukuran secara subjektif dan objektif, algoritma Gifshuffle menunjukan kualitas citra stego MSE rata-rata system adalah 0 dan PSNR infinity. Setelah dilakukan gangguan berupa Rotate, Rescale, dan pemberian Salt and Pepper Noise. Pada Rotate dan Rescale, pesan hasil ekstrasi semua kembali dengan normal, ini disebabkan susunan palet warna tidak berubah.

Kata Kunci : Steganografi, Graphics Interchange Format (GIF), Gifshuffle, Citra Digital

Abstract

Within this final project a blind steganography will be designed and implemented in digital images using Gifshuffle algorithm. Graphics Interchange Format (GIF) is a format that frequently used because of its small size and there are plenty numbers of image editor softwares that have been supporting this small-sized image. GIF has small size because it keeps the amount of the colors up to 256 colors, so that it can save the file size.

Gifshuffle algorithm is developed by Matthew Kwan, it is one of steganography algorithms that uses a file image with the GIF format. Gifshuffle algorithm contains encoding and decoding process. This algorithm performs the insertion of a message by replacing the sequence of palette colors which found in the GIF image. The application that made in this research is not only just implementing the Gifshuffle algorithm, but also implementing the Huffman algorithm as a compression of input messages, so that the messages can be inserted more.

After performing the design and implementation, the stego images are tested in order to see the resistance of attack. The type of attacks that tested are rotate (scale rotation of 30 °: 45 °: 60 °: 90 °), rescale (rescale value of 0.25: 0.5: 0.75: 0.99), and salt and pepper noise (noise scale value of 0:05: 0.1: 0.25: 0.5).

From the subjective and objective measurement results, Gifshuffle algorithm shows that the average stego image quality MSE system is 0 and the PSNR is infinity. After performing some attacks, such as Rotate, Rescale, and giving Salt and Pepper Noise, it appears that in the Rotate, Rescale, Salt and Pepper noise, the extracted messages are back to normal, it's because the order of the color palette has not changed.

Keywords : Steganography, Graphics Interchange Format (GIF), Gifshuffle, Digital Image

I. Pendahuluan

1.1. Latar Belakang Masalah

Kemajuan cara berpikir manusia membuat masyarakat menyadari bahwa teknologi informasi merupakan salah satu aspek penting dalam peradaban manusia untuk mengatasi (sebagian) masalah derasnya arus informasi. Dimana kemajuan teknologi informasi telah berkembang dengan pesat sehingga menjadikannya sebagai suatu lahan baru bagi pelaku tindak kriminal untuk menjalankan aksinya. Berbicara mengenai kejahatan di dunia maya (cyber crime) sepertinya tidak akan ada habisnya mengingat teknik dan modus operandi-nya akan selalu berkembang seiring dengan kemajuan teknologi informasi itu sendiri. Salah satu pekerjaan manusia yang akan sangat terbantu dengan hadirnya teknologi informasi, dengan keuntungan yang ditawarkan, yaitu pekerjaan manusia dalam menyembunyikan pesan baik pada teknik steganografi maupun kriptografi.

Salah satu perbedaan dari kriptografi dan steganografi bisa juga dilihat jika arti dari keduanya ditelaah. Sebuah pesan rahasia, yang berhubungan dengan kriptografi, biasanya akan menimbulkan kecurigaan bagi yang tidak mengetahuinya pesan sebenarnya. Sementara itu sebuah pesan yang terselubung (berhubungan dengan steganografi) tidak akan menimbulkan kecurigaan secara langsung saat seseorang melihat pesan tersebut karena pesan yang terlihat bukanlah pesan yang sebenarnya. Pesan yang telah dienkripsi dengan metode kriptografi manapun, umumnya terlihat kacau, aneh, dan tidak terbaca, sementara pesan yang disembunyikan dengan steganografi masih bisa terbaca oleh orang awam,sehingga tidak menimbulkan kecurigaan.

Perbedaan yang kedua adalah algoritma sandi yang digunakan dalam mengamankan pesan. Kebanyakan teknik kriptografi menggunakan aturan tertentu dalam mengubah *plaintext* menjadi *ciphertext*, dan sebaliknya. Sementara itu cara mengamankan pesan dalam steganografi umumnya didasari oleh kreativitas sang penyembunyi pesan. Hanya beberapa teknik dalam steganografi yang menggunakan algoritma tertentu

dalam menyembunyikan pesan. Oleh karena itu, meskipun kriptografi dan steganografi sama-sama disebut sebagai ilmu dan seni, namun perbedaan ini membuat kriptografi lebih terlihat sebagai sebuah ilmu dan steganografi lebih terlihat sebagai sebuah seni.

Dengan mengetahui perbedaan, karakteristik, serta kelebihan dan kekurangan dari kriptografi dan steganografi, manusia dapat memilih metode apa yang akan digunakan dalam mengamankan data atau pesannya. Jika tempat penyimpanan data atau pesan yang diamankan juga disembunyikan, pemiliknya dapat menggunakan kriptografi saja untuk melindungi data atau pesannya, mungkin dengan alasan kemudahan mendekripsi jika sewaktu-waktu ingin dilakukan modifikasi terhadap data atau pesan tersebut. Namun jika pengirim pesan ingin menyampaikan pesan rahasia kepada orang tertentu saja yang tidak diketahui lokasinya, pengirim pesan dapat menyebarkan pesannya di public (misalnya melalui iklan pada media massa) dan menggunakan steganografi untuk mengubah pesan, sehingga pesan yang asli hanya dimengerti oleh orang yang memang dituju dan orang yang tidak berkepentingan tidak akan curiga terhadap pesan tersebut. Pengamanan bisa diperketat lagi jika data atau pesan diamankan dengan teknik dalam kriptografi kemudian ciphertext hasilnya diubah lagi dengan steganografi atau sebaliknya, dilakukan pengamanan dengan metode steganografi terlebih dahulu kemudian dienkripsi lagi sehingga menjadi pesan yang rahasia [23].

Teknologi komputer memberikan kontribusi baru dalam revolusi menyembunyikan pesan. Steganografi pada era informasi digital merupakan teknik dan seni menyembunyikan informasi dan data digital dibalik informasi digital lain. Secara teori, semua file umum yang ada di dalam komputer dapat digunakan sebagai media, seperti file gambar berformat PNG (*Portable Network Graphics*), JPEG (*Joint Photographic Experts Group*), GIF (*Graphics Interchange Format*), dan lain-lain, semua bisa dijadikan tempat bersembunyi, selama file media tersebut jika dimodifikasi. Kemudian pada data digital, teknik-teknik yang sering digunakan dalam steganografi modern antara lain : Modifikasi *Least*

Significant Bit (LSB), *Mask and Filtering*, Algoritma kompresi dan transformasi, dan Teknik Pixel Mapping yang dikenal dengan Metode Modifikasi *Red Green Blue* (RGB) Level[15].

Untuk mempercepat proses pengiriman pesan rahasia, diperlukan sebuah media penampung pesan yang berukuran kecil namun tetap dapat menjamin kerahasiaan pesan yang dikandungnya. GIF (*Graphics Interchange Format*) adalah format gambar yang diperkenalkan oleh CompuServe pada 1987 dan merupakan salah satu format yang umum digunakan dalam web karena ukurannya yang kecil [15].

Gifshuflle merupakan sebuah algoritma yang menyisipkan pesan ke dalam citra berformat GIF. *Gifshuffle* adalah algoritma steganografi yang diperkenalkan oleh Matthew Kwan pada 21 January 2003. Cara kerjanya adalah dengan mengubah susunan palet warna pada citra tersebut di mana setiap perubahan berkorespondensi dengan sebuah karakter yang dideklarasikan sebelumnya[14].

Ada dua tipe utama kompresi citra, yaitu kompresi tipe *lossless* dan kompresi tipe *lossy*. Salah satu contoh dari kompresi tipe *lossless* adalah metode *Huffman*. Metode *Huffman* paling efisien dari metode lain yang sejenis karena pemetaan lain simbol dari sumber data menjadi string unik menghasilkan file output yang lebih kecil ketika frekuensi symbol sesuai dengan frekuensi yang digunakan untuk menghasilkan kodenya[18].

Didorong oleh hal-hal tersebut, penulis tertarik untuk membahas tentang pembuatan sebuah aplikasi program Steganografi. Program aplikasi ini akan menyediakan kemudahan penyisipan pesan, yaitu berupa teks yang terkompresi ke dalam sebuah file digital, menganalisa kapasitas ukuran file yang disisipkan dan keamanan dari media pembawa pesan tersebut. Sehingga jika media pembawa pesan tersebut tahan dari serangan, secara tidak langsung pesan yang tersimpan dalam media tersebut akan tetap aman.

1.2. Perumusan Masalah

Dalam kajian ini penulis ingin memberikan suatu solusi dengan merancang dan mengaplikasikan suatu aplikasi pengamanan digital dengan teknik steganografi, dapat dirumuskan menjadi beberapa masalah sebagai berikut.

1. Bagaimana melakukan penyembunyian pesan ke dalam sebuah citra GIF dan ekstraksi pesan tersembunyi pada citra GIF yang telah disisipkan pesan menggunakan metoda *GifShuffle*.
2. Bagaimana melakukan pengompresan pada pesan berupa *text* dan dekompresi pesan tersebut menggunakan algoritma *Huffman*.
3. Bagaimana membandingkan kualitas citra GIF yang telah disisipkan pesan rahasia dengan citra GIF yang belum disisipkan pesan rahasia.

1.3. Tujuan

Tujuan dari penulisan Tugas Akhir ini adalah:

1. Menganalisis dan mengimplementasikan aplikasi yang menyisipkan dan mengekstrak pesan berupa teks dalam media penampung berupa citra dengan format GIF menggunakan algoritma *Gifshuflle* dengan mengompresi dan mendekompresi pesan teks mengunakan algoritma *Huffman.*
2. Menganalisis performa algoritma *Gifshuffle* dan algoritma *Huffman* pada proses steganografi.
3. Menganalisis keamanan citra *carrier* ketika diberi serangan, sehingga pesan yang dibawa tetap aman.

1.4. Batasan Masalah

Penulis mambatasi permasalahan yang dibahas dalam tugas akhir ini hanya mencakup hal-hal sebagai berikut.

1. Metode yang digunakan adalah algoritma *GifShuffle*.
2. File citra yang akan digunakan sebagai media penampung adalah file yang berformat GIF berwarna dan non-animated dan image berukuran 256 x 256 pixel.

3. File yang disisipkan hanya file berupa text (Alfanumerik dan Tanda baca).
4. Algoritma kompresi yang digunakan dalam aplikasi ini adalah *Huffman*.
5. Parameter yang dianalisa adalah *Imperceptible, Fidelity, Recovery* dan *Robustnes*.
6. Format GIF yang digunakan memiliki 256 palet warna, maka penyimpanan maximum dari format ini adalah 1680 bit.
7. Ukuran pesan yang di sisipkan harus lebih kecil atau sama dengan besar file gambar.

1.5. Metodologi

Format GIF yang kecil dan bersifat *loosless* maka format ini baik untuk disisipkan data. Banyak teknik menyembunyikan pesan dalam citra digital. Salah satu algoritma penyisipan data adalah algoritma *GifShuffle*. Oleh karena itu muncul permasalahan seberapa besar aspek *robustness* dari algoritma ini.

Metode penelitian yang diterapkan pada pengerjaan Tugas Akhir ini adalah :

a. Studi Literatur

Pada tahap ini dilakukan studi literature yang relevan dengan tugas akhir yang dibuat, baik itu berupa buku, artikel, dan sumber lain yang berhubungan yaitu mengenai citra digital (GIF), teori dasar Steganografi, algoritma *GifShuffle* dan algoritma *Huffman*.

b. Perancangan dan Implementasi

Dalam tugas akhir ini dibuat sebuah aplikasi, untuk menyisipkan data di dalam sebuah citra yang berformat GIF. Pertama akan dilakukan proses memasukan data kedalam sebuah file Gif. Setelah berhasil maka melakukan proses pembongkaran isi data yang ada di dalam format Gif tersebut. Langkah selanjutnya adalah menguji file

yang telah disisipkan data berbeda jauh dengan file yang belum disisipkan.

Pada saat pengujian dilakukan uji scenario dengan melihat *Imperceptible*, *Fidelity*, *Recovery* dan *Robustnes* apakah sesuai dengan yang diinginkan dan menganalisa algoritma dan hasil yang di dapatkan.

c. Tahap Pengujian dan Analisis

Melakukan pengolahan data yang diperoleh dari pengujian yang dilakukan dengan melihat hasil-hasil yang telah dicoba, dan dari hasil yang di dapat dilakukan analisa bagaimana dampak file GIF setelah dan sebelum disisipi file dengan memperhatikan *Imperceptible*, *Fidelity*, *Recovery* dan *Robustnes* sebagai pengujian algoritma *GifShuffle*. Menganalisis algoritma yang digunakan setelah mendapatkan hasil.

d. Penyusunan Laporan Tugas Akhir

Berdasarkan hasil analisis yang telah dilakukan pada tahap sebelumnya untuk kemudian disusun laporan terhadap analisis yang telah dilakukan.

1.6. Sistematika Penulisan

Laporan tugas akhir ini terdiri atas 5 Bab, yaitu Bab Pendahuluan, Dasar Teori, Analisis dan perancangan, Pengujian dan Analisis, dan terakhir adalah Bab Kesimpulan dan Saran. Pada paragraph selanjutnya dijelaskan apa yang termuat pada masing masing Bab pada laporan tugas akhir ini.

BAB 1: PENDAHULUAN

Bab Pendahuluan ini berisi uraian mengenai latar belakang pembuatan tugas akhir ini, masalah yang dihadapi, batasan-batasan yang

ditetapkan berkaitan dengan masalah yang ada, tujuan pembahasan dan hipotesis tugas akhir ini.

BAB 2: DASAR TEORI

Bab Dasar Teori menjelaskan teori digital, RGB, Format Gif, dan seluruh teori yang mendukung cara kerja proses steganografi pada citra digital dengan metode *Gifshuffle* dan metode *Huffman*.

BAB 3: ANALISIS DAN PERANCANGAN SISTEM

Bab Analisis dan Perancangan membahas system secara umum, perangkat keras dan perangkat lunak pendukung yang dibutuhkan untuk mengoperasikan system yang dibuat.

BAB 4: PENGUJIAN DAN ANALISIS

Bab Pengujian dan Analisis membahas tentang analisa terhadap kualitas citra hasil steganografi baik secara objektif maupun subjectif.

BAB 5: KESIMPULAN DAN SARAN

Bab Kesimpulan dan Saran menyajikan beberapa kesimpulan yang diperoleh dari penelitian Tugas Akhir ini dan saran sebagai kemungkinan pengembangan topik yang bersangkutan

V. Kesimpulan dan Saran

a. Kesimpulan

Kesimpulan yang diperoleh dari pengukuran secara obyektif maupun subyektif tentang algoritma *Gifshuffle* dalam format GIF pada tugas akhir ini adalah sebagai berikut:

1. Algoritma ini cukup baik karena penyisipan pesan sama sekali tidak menimbulkan adanya perbedaan gambar. Ini disebabkan karena perubahan susunan palet warna tidak mempengaruhi perubahan citra. Sehingga dapat dikatakan memiliki *Imperceptibility* dan *Fidelity* yang baik.
2. Ketika citra stego diberi serangan berupa *rescale, rotate,* dan *salt and paper noise* pesan dapat kembali utuh atau dengan kata lain nilai CER adalah 0. Hal ini disebabkan karena saat penyerangan tersebut jumlah palet dan letak urutan palet tetap. Sehingga dapat dikatakan memiliki *Recovery* dan *Robustnes* yang baik.
3. Kelemahan dari algoritma ini adalah kemampuan penyisipan yang kecil. Karena berdasarkan pengujian algoritma ini hanya dapat disisipkan 1680 bit. Kelemahan itu dapat minimalisir dengan menyisipkan algoritma *Huffman*. Sehingga saat dibandingkan dengan pesan yang dikompres mengunakan algoritma *Huffman*, pesan yang disisipkan hampir 2 kalinya. Persentase keunggulan yang didapatkan menggunakan algoritma *Huffman* tergantung terhadap jenis pesan yang disisipkan.

b. Saran

Saran-saran untuk pengembangan dan perbaikan adalah sebagai berikut:

1. Aplikasi ini hanya dapat menyisipkan pada citra non-animated GIF, untuk pengembangan berikutnya dapat ditambahkan fungsi agar dapat menyisipkan pesan pada animated GIF, sehingga pesan yang disisipkan dapat lebih banyak.
2. Dapat ditambahkan algoritma enkripsi terhadap pesan, sehingga dapat meningkatkan keamanan pesan tersebut.
3. Dapat menggunakan metode lain sebagai pembanding.

Telkom University

DAFTAR PUSTAKA

[1] Acharya, Tinku and Ray, K, Ajoy. *Image Processing Principles and Applications*. A John Wiley & Sons, Inc., Publication.

[2] Adipranata, Handojo, Prayogo, Yenty Yuliana. 2005. *Perancangan dan Pembuatan Aplikasi Segmentasi Gambar dengan menggunakan Metode Morphologocal Watershed*. Surabaya: Universitas Kristen Petra.

[3] Aditya, Yogie. 2010.*Studi Pustaka untuk Steganografi dengan beberapa metode*. Yogyakarta: Seminar Nasional Aplikasi Teknologi Informasi 2010.

[4] Alex, Desi. 2003. *Implementasi Teknik Wtermarking Digital pada Domain DCT untuk Citra Berwarna*. Yogyakarta. Universitas Gadjah Mada.

[5] Bruce, Schneiner, *Applied Cryptography: Protocols, Algorithm, and Source Code in C*, New York: Wiley, 1994.

[6] Fatta, Hanif. 2007.*Konversi Citra RGB ke Format Grayscale Menggunakan Visual Basic*. Yogyakarta, STIMIK AMIKOM.

[7] Ginting, Priskilla. 2010. *kajian Steganografi dengan Metode Bit-Plane Complexity Segmentation (BPCS) pada Dokumen Citra Terkompresi*. Medan: Universitas Sumatera Utara.

[8] Hestiningsih, Idhawati. 2010. *Pengolahan Citra*. Yogyakarta: Universitas Gajah Mada.

[9] Kwan, Matthew, http://www.darkside.com.au/gifshuffle. Website resmi GifShuffle. Tanggal akses: 1 Oktober 2010 pukul 16:00.

[10] Luthfi, Inas. 2009.*Steganografi Digital Citra Bergerak Animated Gif*. Bandung: Institut Teknologi Bandung.

[11] Madenda, Sarifuddin, Hayet, L, and I, Bayu. 2008. *Kompresi Citra Berwarna Mengunakan Metode Pohon Biner Huffman*. Tangerang: Pusat Pengembangan Informaka Nuklir.

[12] Maradilla, Temmi. 2010. Ap*likasi Steganografi Untuk Penyisipan Data Text Ke Dalam Citra Digital*. Universitas Gunadarma.

[13] W. Bender, D. Gruhl, N. Morimoto, A. Lu, *Techniques for data hiding*, IBM System Journal, Vol. 35, 1996.

[14] Munir, Rinaldi. 2004. *Steganography dan Watermarking*. Bandung: Institut Teknologi Bandung.

[15] Munir, Rinaldi. 2005. *Bahan kuliah :Kriptografi*. Bandung: Institut Teknologi Bandung.

[16] Muntina D, Eddy, ST, MT. 2005. *Pengantar Pengolahan Citra Digital*. Slide Mata Kuliah Grafika dan Citra STT Telkom. Bandung. STT Telkom.

[17] Penalosa, Ronald. 2010. *Steganografi pada Citra dengan Format Gif Menggunakan Algoritma Giffshuffle*. Bandung. Institut Teknologi Bandung.

[18] Prasetia, Dikdik. 2001. *Implementasi Steganografi mengunakan metode Least Significant Bit pada Mobile Phone berbasis Symbias OS*. Bandung: Universitas Komputer Indonesia.

[19] Rina, Dewi. And Munawaroh, Nur 2008. *Implementasi Metode Huffman Untuk Kompresi Ukuran File Citra Bitmap 8 Bit Mengunakan Borland Delphi 6.0*. Malang: Sekolah Tinggi Manajemen Informatika dan Komputer ASIA Malang.

[20] Sitompul, Putri. 2010. *Analisis dan Implementasi Steganografi pada Citra Gif Menggunakan Algoritma Giffshuffle*. Universitas Sumatera Utara.

[21] Suhono H. Supangkat, Kuspriyanto, Juanda, *Watermarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital*, Departemen Teknik Elektro, Institut Teknologi Bandung.

[22] Yuda, Aditya. 2001. *Steganografi Video dengan menggunakan Metode DCT*. Bogor: Institut Pertanian Bogor.

[23] Setiawan, Budi. 2009. *Pengunaan Kriptografi dan Steganografi Berdasarkan Kebutuhan dan Karakteristik Keduanya*. Bandung: Institut Teknologi Bandung.