TIN: Terapan Informatika Nusantara
Vol 1, No 3, Agustus 2020, Hal 118-122
ISSN 2722-7987 (Media Online)

Penerapan Steganografi Pada Image GIF Menggunakan Metode Ezstego dan Elgamal

Mhd Ariya Fattah

Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: ariyabroken73@gmail.com

Abstrak−Masalah Keamanan dan kerahasiaan data merupakan salah satu aspek penting dalam hal pertukaran informasi. Salah satu solusi untuk menjaga keamanan dan kerahasiaan pada proses steganografi adalah dengan teknik penyisipan pesan untuk enkripsi file dengan kriptografi elgamal yang digunakan untuk steganografi image Gif. Penelitian ini memaparkan mengenai pengembangan steganografi yang menerapkan algoritma Ezstego yang digunakan untuk steganografi image Gif. Algoritma ezstego dipilih karena menyisipkan bit-bit pesan dari nilai piksel. Penelitian ini menghasilkan sebuah program aplikasi bertujuan untuk pencegahan keamanan pada image Gif. Citra Gif adalah jenis citra terindeks, format jif biasanya digunakan untuk menyimpan citra grafika komputer, citra ikonik, kartun, logo, animasi maupun citra natural. Dalam pembuatan aplikasi ini, metode yang digunakan adalah Algoritma Eztego, karena sangat cocok untuk steganografi image Gif yang menghasilkan penyelesian proses kriptografi elgamal pada penyisipan pesan. Aplikasi ini dibuat dengan perangkat lunak visual basic 2008 dan pembuatan aplikasi steganografi image Gif dengan proses penyisipan pesan enkripsi dan deskripsi diharapkan untuk mengatasi permasalahan tersebut.

Kata Kunci: Kriptografi elgamal, Steganografi, Ezstego

Abstract−Security and data confidentiality is one of the important aspects in terms of information exchange. One of the solutions to maintain the security and confidentiality of the steganography process is the message insertion technique for file encryption with electronic cryptography used for Gif image steganography. This study describes the development of steganography that applies the Ezstego algorithm which is used for Gif image steganography. The ezstego algorithm was chosen because it inserts message bits from pixel values. This research produces an application program that aims to prevent safety on Gif images. Gif image is a type of indexed image, the jif format is usually used to store computer graphic images, iconic images, cartoons, logos, animation and natural images. In making this application, the method used is the Eztego Algorithm, because it is very suitable for Gif image steganography which results in the completion of the electronic cryptography process on message insertion. This application is made with Visual Basic 2008 software and the creation of a Gif image steganography application with the process of inserting an encryption message and description is expected to solve this problem.

Keywords: Legal Cryptography, Steganography, Ezstego

1. PENDAHULUAN

Kriptografi merupakan seni dan ilmu untuk menulis rahasia "*The Art of Secreet Writing*". Tujuan dari kriptografi adalah mengolah informasi dengan algoritma tertentu supaya pesan tidak dapat dibaca. Proses yang dilakukan untuk mengamankan sebuah pesan (*plaintext*) menjadi pesan yang tersembunyi (*ciphertext*) disebut dengan enkripsi (*encryption*). Chiphertext adalah pesan yang sudah tidak dapat dibaca dengan mudah atau sulit dimengerti maknanya. Proses untuk mengembalikan atau mengubah *ciphertext* menjadi *plaintext* disebut dekripsi (*decryption*).Namun penggunaan kriptografi sering menimbulkan kecurigaan pihak ketiga, sebab pesan yang sulit dimengerti pasti sudah diolah dan menunjukkan bahwa pesan itu merupakan informasi penting. Apalagi saat ini semakin berkembang kemampuan untuk memecahkan kriptografi yang disebut krpitanalisis.

Perkembangan komunikasi data membuat aspek keamanan dan kerahasiaan data menjadi sangat penting. Dalam membangun aplikasi ini, penulis menggunakan teknik steganografi, dimana pesan rahasia disisipkan kedalam media gambar sehingga orang lain tidak mengetahui bahwa didalam file tersebut terdapat pesan rahasia. Steganografi membutuhkan dua properti, yaitu media penampung (media untuk menyembunyikan pesan) dan data rahasia yang akan disembunyikan.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kata *Cryptography* berasal dari bahasa Yunani yang terdiri dari dua kata yaitu *kryptos* yang berarti rahasia dan *graphein* yang berarti tulisan (Mollin, 2007). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain[2].

2.2 Steganografi

Steganografi Steganography (steganografi) merupakan seni untuk menyembunyikan pesan rahasia kedalam pesan lainnya sedemikian rupa sehingga membuat orang lain tidak menyadari adanya sesuatu di dalam pesan tersebut. Kata Steganography berasal dari bahasa Yunani, yaitu gabungan dari kata steganos (tersembunyi atau terselubung) dan graphein (tulisan atau menulis), sehingga makna Steganography kurang lebih bisa diartikan sebagai menulis tulisan yang tersembunyi [5].

Vol 1, No 3, Agustus 2020, Hal 118-122
ISSN 2722-7987 (Media Online)

2.3 Citra Digital

Citra atau gambar dapat didefinisikan sebagai sebuah fungsi yang terdiri dari dua variabel f(x,y), dengan x dan y adalah koordinat bidang datar, dan harga fungsi f disetiap pasangan koordinat (x,y) disebut intensitas atau level keabuan (grey level) dari gambar di titik itu. Jika x,y dan f semuanya berhingga (finite), dan nilainya diskrit, maka gambarnya disebut citra digital (gambar digital). Sebuah citra digital terdiri dari sejumlah elemen berhingga, dimana masing-masing mempunyai lokasi dan nilai tertentu. Elemen-elemen ini disebut sebagai picture element, image element, pels atau pixels[8].

2.4 Metode Esztego

EzStego menyisipkan bit-bit pesan pada bit LSB dari indeks palet. Akibat penyisipan tersebut, indeks palet dapat bertambah satu, tetap, atau berkurang satu. Oleh karena indeks palet merupakan *pointer* ke palet warna, maka indeks yang baru (setelah penyisipan LSB) menunjuk ke warna berikutnya atau ke warna sebelumnya di palet yang tentu saja secara visual berbeda signifikan. Hal ini tentu menimbulkan degradasi warna yang membuat citra stego berbeda jauh dengan citra *cover*. Untuk meminimalkan degradasi warna, maka langkah pertama di dalam algoritma *EzStego* adalah mengurutkan warna-warna di dalam palet sedemikian sehingga perbedaan dua warna yang bertetangga adalah minimal. Perbedaan dua warna dapat dihitung dengan rumus jarak Euclidean. Misalkan warna 1 dinyatakan sebagai vektor (*R*1, *G*1, *B*1) dan warna 2 dinyatakan sebagai (*R*2, *G*2, dan *B*2). [1] Jarak Euclidean kedua warna tersebut dihitung dengan rumus :

$$d = \sqrt{(R_1 - R_2)^2 + (G_1 - G_2)^2 + B_1 - B_2)^2} \quad \text{.....(1)}$$

Jadi, proses pengurutan palet dilakukan dengan menghitung jarak antar warna di dalam palet, lalu mengurutkan palet berdasarkan jarak terkecil sedemikian sehingga akhirnya dua warna bertetangga memiliki jarak Euclidean yang kecil. Bit-bit pesan disisipkan pada bit LSB indeks dari palet yang terurut secara sekuensial. Algoritma *EzStego* diusulkan di dalam [6] sehingga peyisipan dan ekstraksi pesan membutuhkan kunci (*stego-key*). Kunci berguna untuk membangkitkan posisi acak di dalam citra sebagai lokasi penyisipan bit-bit pesan[1].

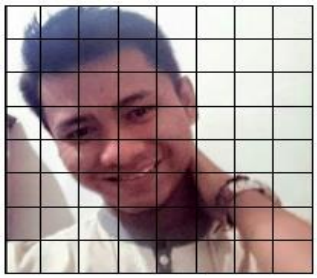
3. HASIL DAN PEMBAHASAN

3.1 Analisa

Analisa file merupakan tahapan dimana dilakukannya análisa terhadap file-file apa saja yang diolah dalam sistem atau prosedur sebuah rancangan, dalam hal ini file image yang akan dienkripsi dan dekripsi pada aplikasi adalah berupa *file image* berformat (*.GIF). Alasan menggunakan teknik steganografi, dimana pesan rahasia disisipkan kedalam media gambar sehingga orang lain tidak mengetahui bahwa didalam file tersebut terdapat pesan rahasia. Steganografi membutuhkan dua properti, yaitu media penampung (media untuk menyembunyikan pesan) dan data rahasia yang akan disembunyikan. Steganografi pada gambar GIF untuk menyisipkan pesan rahasia pada media gambar animasi bergerak seperti gambar GIF guna meningkatkan keamanan data dengan menerapkan metode *Eztego* dan menggunakan kriptografi *elgamal*.

3.2 Penerapan Metode Elgamal

Proses yang dilakukan adalah pengamanan citra GIF citra asli (Plain Image) sebelum disisipkan pesan menggunakan *EzStego*. Salah satu *cover* yang dapat digunakan untuk menyembunyikan pesan adalah digital warna 24 *bit*. Setiap piksel l pada warna 24 *bit* memiliki warna yang merupakan kombinasi dari tiga warna dasar *Red*, *Green*, *Blue* (RGB). Elgamal memerlukan sepasang kunci yang dibangkitkan dengan memilih bilangan prima *p* dan dua buah bilangan acak (random) *g* dan *x*, dengan syarat bahwa nilai *g* dan *x* lebih kecil dari *p* yang memenuhi persamaan. Sebagai contoh *Image* GIF 24 bit berformat GIF dengan resolusi 8x8 piksel, memperlihatkan matriks pada nilai-nilai piksel setiap baris dan kolom adalah sebagai berikut :



Gambar 1. Citra GIF 8x8 piksel

Vol 1, No 3, Agustus 2020, Hal 118-122
ISSN 2722-7987 (Media Online)

Nilai citra terlebih dahulu di konversi menggunakan matlab 6.1 agar terbentuklah nilai RGB berikut proses pengambilan konversi citra ASCII pada matlab.

3.3 Penerapan Ezstego

Proses yang dilakukan adalah setelah pengamanan citra GIF pada pesan yang di proses menggunakan elgamal dan selanjutnya hasil chiper dari elgamal akan diproses menggunakan citra *EzStego.* Salah satu *cover* yang dapat digunakan untuk menyembunyikan pesan adalah digital warna 24 *bit*. Setiap piksel l pada warna 24 *bit* memiliki warna yang merupakan kombinasi dari tiga warna dasar *Red, Green, Blue* (RGB). Sedangkan satu piksel l warna 24 bit diwakili oleh 3 (tiga) *byte*, dimana masing-masing 1 *byte* merepresentasikan warna *Red, Green, Blue*. Adapun hasil (*Cipher image*) setelah disisipkan pesan dari pengamanan citra GIF menggunakan Elgamal dengan nilai piksel sebagai berikut:

Tabel 1. Penerapan Ezstego

Warna	1	2	3	4	5	6	7	8
R	145	162	216	49	42	72	37	185
	215	110	124	68	235	100	243	62
G	56	232	250	50	166	141	213	111
	160	106	234	103	12	227	30	2
B	247	101	198	68	130	255	206	204
	27	186	20	9	141	195	98	192

Kemudian hasil chiper dari elgamal dikonversikan nilai piksel pada *Red, Green, Blue* kedalam bilangan biner pada warna 24 *bit*, setiap piksel l berukuran 3 *byte* dimana setiap *byte* mewakili warna dari setiap nilai piksel *Red, Green, Blue*.

10010001 10100010 11011000 110001 101010 1001000 100101 10111001
11010111 1101110 1111100 1000100 11101011 1100100 11110011 111110
111000 11101000 11111010 110010 10100110 10001101 11010101 1101111
10100000 1101010 11101010 1100111 1100 11100011 11110 10
11110111 1100101 11000110 1000100 10000010 11111111 11001110 11001100
11011 10111010 10100 1001 10001101 11000011 1100010 11000000

Citra Ezstego menghasilkan chiper pesan kedalam 2 bit dari setiap byte warna. Dan hasil chiper pesan tersebut memberikan nilai piksel 1 baru sebagai berikut :
Penyisipan pesan “H” : 72 : 1001000

10010**10** 101000**01** 110110**00** 1100**00** 101010 1001000 100101 10111001
11010**110** 11011**01** 11111**00** 1000100 11101011 1100100 11110011 111110
11100**10** 11101**01** 11111**000** 110010 10100110 10001101 11010101 1101111
10100**10** 11010**01** 11101**10** 1100111 1100 11100011 11110 10
11110**110** 11001**00** 11000**110** 10001**00** 10000010 11111111 11001110 11001100
11011**10** 10111**01** 10100 10**10** 10001**00** 11000011 1100010 11000000

Penyisipan Pesan karkter “G” : 71 : 1000111

10010**10** 101000**00** 110110**111** 110001 101010 1001000 100101 10111001
11010**100** 11011**00** 11111**11** 10001**01** 11101011 1100100 11110011 111110
11100**10** 11101**00** 11111**011** 1100**11** 10100110 10001101 11010101 1101111
10100**10** 11010**00** 11101**011** 11001**11** 1100 11100011 11110 10
11110**100** 11001**00** 11000**111** 10001**01** 10000010 11111111 11001110 11001100
11011**10** 10111**00** 10100**11** 100**11** 10001101 11000011 1100010 11000000

Penyisipan Pesan karkter “Y” : 89 : 1011001

11101**10** 11011**11** 11010**000** 10111**01** 10100010 10001101 1111110 1111011
111011**110** 11011**011** 11001**000** 10110**001** 10011010 10001011 10000011 10000001
1111011**110** 11101**011** 11011**000** 11000**001** 10100011 10001100 1111100 1111001
11111010 11100101 11001101 10110001 10011000 10000110 1111011 1111001
11011**10** 11001**11** 11000**00** 10110**01** 10011011 10001000 1111111 1111110
11011100 11001010 10110110 10011111 10001100 10000000 1111001 1110111

Penyisipan Pesan karkter “I” : 73 : 1001001

Vol 1, No 3, Agustus 2020, Hal 118-122
ISSN 2722-7987 (Media Online)

10010**100** 10100**10** 11011**00** 1100**01** 101010 1001000 100101 10111001
11010**110** 1101**101** 1111**1001** 1000100 11101011 1100100 11110011 111110
11100**100** 1110**1010** 1111**1001** 110010 10100110 10001101 11010101 1101111
10100**010** 1101**0101** 1111**0100** 1100111 1100 11100011 11110 10
11110**110** 1100**101** 1100**0110** 1000**101** 10000010 11111111 11001110 11001100
1101**100** 1011**1011** 101**00** 10**01** 10001101 11000011 1100010 11000000

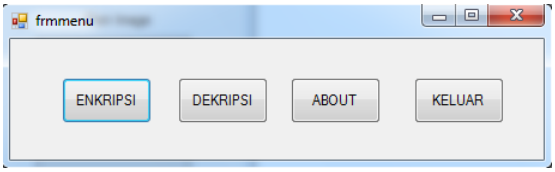
Dan hasil proses setelah dilakukan pengamanan image GIF yang telah disisipkan pesan di enkripsi menggunakan metode Elgamal. Hasil chiper dari pesan pada penjabaran steganografi pada image GIF metode Elgamal pada citra *Esztego* Setiap piksel berformat (*.GIF) merepresentasikan warna *Red*, *Green*, *Blue*.

Gambar 2. Chiper Citra *GIF*

3.3 Implementasi Program

1. Menu Utama

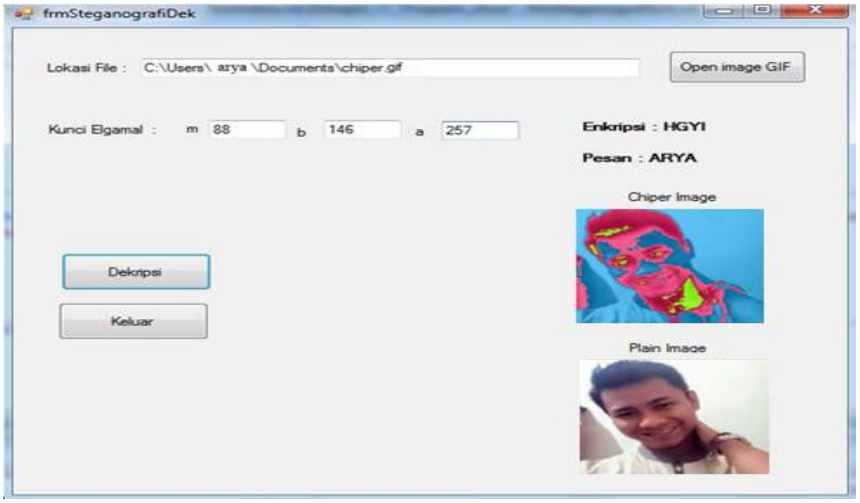
Halaman utama merupakan tampilan halaman yang muncul pertama sekali pada saat sistem dijalankan. Halaman utama memiliki 3 menu bar, yaitu menu menu utama yang terdiri dari enkripsi, dekripsi, about dan keluar. Tampilan Halaman menu utama dapat dilihat pada gambar 3:



Gambar 3. Tampilan Menu Utama

2. Tampilan Enkripsi

Tampilan form ini digunakan untuk mengenkripsi pada penyisipan pesan dan kemudian di enkripsi menghasilkan chiperteks pada pesan penyisipan dan chiper gambar berformat *gif. Adapun *form* enkripsi steganografi tersebut dapat dilihat pada gambar 4 dapat dilihat dibawah ini.



Gambar 4. Tampilan enkripsi steganografi

3. Tampilan Dekripsi

Vol 1, No 3, Agustus 2020, Hal 118-122
ISSN 2722-7987 (Media Online)

Tampilan form ini digunakan untuk mendekripsi pada penyisipan pesan dan kemudian di dekripsi kembali menghasilkan plainteks pada pesan penyisipan dan plain gambar berformat *gif. Adapun *form* dekripsi steganografi tersebut dapat dilihat pada gambar 5 dapat dilihat dibawah ini.

Gambar 5. Tampilan dekripsi steganografi

4. KESIMPULAN

Berdasarkan hasil yang di dapat dalam penelitian dan penyusunan skripsi ini maka diperoleh kesimpulan, sebagai berikut:

1. Proses penyisipan metode Esztego menggantikan hanya pada bit terakhir dari cover atau gambar dan stelah disisipkan pesan hanya mengalami sedikit penurunan kualitas warna dan pada ukuran pada size file tidak mengalami perubahan gambar maupun esztego.
2. Metode Esztego memberikan hasil chiperteks pada penyisipan pesan dengan hasil eksperimen steganalisis pada citra GIF dan sedangkan Elgamal melakukan *generate key* pada karakter pesan untuk menghasilkan hasil chiper pada gambar.
3. Perubahan pada enkripsi steganografi pada gambar format GIF yang dialami perubahan warna, hal ini sangat berguna dalam menjaga kerahasiaan data sehingga tidak banyak orang yang menyadarinya.

REFERENCES

Rinaldi Munir,"Eksperimen Steganalisis Dengan Metode Visual Attack Pada Citra Hasil EzStego Berformat GIF," *SNATI*, pp. C8–C14, 2016

Arius, D. 2008, Awal Sejarah Kriptografi Didunia, STMIK AMIKOM, Yogyakarta.

Munir, R., 2006, Kriptografi, Informatika, Bandung.

Herman Kabetta, "Analisis Kompleksitas Waktu Algoritma Elgamal Dan Data Encryption Standart." *Teknikom*, pp. 13–18, 2017.

Nizirwan Anwar,"Perancangan Steganografi Hidden Message Dengan Metode Least (Significant Bit Insertion (LSB) Berbasis Matlab)," *Algoritma, Logika Dan Komputasi*, vol. 1, no.1, pp. 25-30, 2018

Yudi Prayudi, Puput Setya Kuncoro,"Implementasi Steganografi Menggunakan Teknik Adaptive Minimum Error Least Signifikant Bit Replace (AMELSBR)," *SNATI*, pp. G1–G6, 2005

Provos, N., Honeyman, P. (2003). Hide and Seek: An Introduction to Steganography. IEEE ComputerSociety.

Hermawati, Fajar Astuti. 2013. Pengolahan Citra Digital Konsep & Teori. Yogyakarta: ANDI.

Muntasa, A., & Purnomo, M. H. 2010. Konsep Pengolahan Citra Digital dan Ekstraksi fitur. Yogyakarta: Graha Ilmu.

Adi Nugroho, 2009, Rekayasa Perangkat Lunak Menggunakan UML dan Java. Penerbit ANDI : Yogyakarta

Jogiyanto, H.M., 2005, Analisis dan Desain, Andi Offset, Yogyakarta.

Priyanto, Rahmat, 2009, Langsung Bisa Visual Basic.Net 2008 ,Penerbit ANDI, Yogyakarta.