SIGMA
JURNAL TEKNOLOGI PELITA BANGSA
Vol. 7 No. 2 September 2016 ISSN: 2407-3903
Diterima, 10 Agustus 2016 | Direvisi, 18 Agustus 2016 | Dipublikasikan, 28 September 2016

STEGANOGRAFI GAMBAR DENGAN METODE *LEAST SIGNIFICANT BIT DENGAN KRIPTOGRAFI DCPCHIPER*

Sufajar Butsianto

Program Studi Teknik Informatika Sekolah Tinggi Teknologi Pelita Bangsa
sufajar@pelitabangsa.ac.id

Abstrak

Jaringan Internet berkembang dengan pesat dan memberikan pengaruh besar bagi kehidupan manusia.Perkembangan jaringan Internet telah memungkinkan banyak orang untuk saling bertukar data secara bebas. Oleh karena itu, keamanan dan kerahasiaan sangat dibutuhkan dalam komunikasi data. Hal yang sering dilupakan oleh para user internet adalah keamanan data. Dimana informasi di internet sifatnya adalah terbuka, dengan kemungkinan akses oleh user dari seluruh dunia. Dalam kasus yang sensitif, beberapa informasi ditujukan hanya untuk user atau pihak tertentu, dalam hal inilah diperlukan suatu proteksi untuk melindungi informasi dari pihak-pihak yang tidak berhak mengaksesnya. Steganografi adalah pendekatan proteksi data yang prosesnya adalah penyembunyian pesan dalam media gambar. Dengan steganografi ini proses transaksi data diharapkan akan menjadi lebih aman dari pihak-pihak yang tidak berhak mengaksesnya. Ada banyak metode yang digunakan untuk steganografi pada dokumen citra seperti metode Least Significant Bit (LSB), Spread Spectrum Steganography, dan Bit-Plane Complexity Segmentation (BPCS){2}.Dengan menggunakan metode Least Significant Bit (LSB), yaitu suatu metode penyembunyian pesan rahasia melalui media digital file image untuk mengeksploitasi keterbatasan sistem penglihatan manusia, Sehingga dengan keterbatasan tersebut manusia sulit menemukan gradasi penurunan kualitas warna file gambar yang telah disisipi pesan rahasia.

Kata Kunci : Kriptografi, Steganografi, Gambar, Metode Least Significant Bit,Delphi.

Abstract

Internet network is growing rapidly and give a great influence to the life of the network manusia.Perkembangan Internet has allowed many people to exchange data freely. Therefore, the security and confidentiality is needed in data communications. It is often forgotten by the internet user is the security of data. Where the nature of information on the Internet is open, with the possibility of access by users from around the world. In the case of sensitive, some information intended only for the user or a particular party, in this case a protection is necessary to protect the information from those who are not entitled to access it. Steganography is the process approach to data protection is hiding messages in media images. With this steganography process data transactions are expected to be safer than those who are not entitled to access it. There are many methods used for steganography in image documents such as the method of Least Significant Bit (LSB), Spread Spectrum Steganography, and Bit-Plane Complexity Segmentation (BPCS) {2} By using the method of Least Significant Bit (LSB), which is a method of concealment secret messages through digital media image file to exploit the limitations of the human visual system, so with the limitations of humans is difficult to find gradations of color quality degradation of image files that have been inserted secret message.

***Keywords** : Cryptography, Steganography, Image, Method of Least Significant Bit, Delphi*.

1. Pendahuluan

1.1. Latar Belakang

Steganografi merupakan teknik penyembunyian informasi dengan cara penyisipan pada suatu media. Kata steganography (steganografi) berasal

dari bahasa Yunani yaitu steganos yang berarti menyembunyikan dan graptos artinya tulisan sehingga arti secara keseluruhan ialah tulisan yang disembunyikan (Stellars, 1996).

Masalah yang dapat dirumuskan dari latar belakang di atas adalah bagaimana membangun suatu aplikasi steganografi pada citra digital file gambar bitmap yang efisien, bagaimana mengeksploitasi keterbatasan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada file gambar yang belum disisipi pesan rahasia, sehingga dengan keterbatasan tersebut manusia sulit menemukan gradasi penurunan kualitas warna file gambar yang telah disisipi pesan rahasia.

Tujuan yang di harapkan antara lain membangun perangkat lunak steganografi pada citra digital file gambar bitmap dengan menggunakan bahasa pemrograman delphi, dan menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi dan menghasilkan file gambar yang mempunyai kualitas tidak jauh berbeda dengan citra digital file gambar aslinya, sehingga pesan terlihat hanya seperti pesan biasa saja.

1.2. Tujuan Penelitian

Berdasarkan rumusan masalah di atas, dapat disimpulkan bahwa penelitian ini bertujuan untuk : "Membuat sebuah aplikasi steganografi untuk menginput dan mengekstrak informasi pada media gambar dengan mengaplikasikan metode Least Significant Bit".

1.3. Batasan Masalah

Permasalahan yang ditemukan selama penelitian ini dibatasi oleh hal-hal yang tercantum berkut ini:

1. Aplikasi yang dibuat mencakup aplikasi steganografi sederhana yang berfungsi untuk menyisipkan dan mengekstak informasi dari media gambar.
2. Informasi yang dimaksud disini dibatasi hanya pada informasi berupa text.
3. Text yang disisipkan pada media gambar menggunakan metode Least Significant Bit.
4. Media gambar adalah file image dengan ekstensi bitmap (BMP), dan JPG.
5. Prototype Pembuatan aplikasi steganografi ini dengan menggunakan DELPHI.

2. Landasan Teori

1.1. Steganografi

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. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Kata "steganografi" berasal dari bahasa Yunani steganos, yang artinya "tersembunyi atau terselubung", dan graphein, "menulis".

Kini, istilah steganografi termasuk penyembunyian data digital dalam berkas-berkas (file) komputer. Contohnya, si pengirim mulai dengan berkas 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).

Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia (teks atau gambar) di dalam berkas-berkas lain yang mengandung teks, image, bahkan audio tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari berkas 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 pesan disembunyikan 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.

Adapun data yang disimpan juga dapat berupa citra, suara, video, teks, atau pesan lain. Pada penelitian ini, steganografi yang diterapkan adalah steganografi pada dokumen citra. Ada banyak metode yang digunakan untuk steganografi pada dokumen citra seperti metode Least Significant Bit (LSB), Spread Spectrum Steganography, dan Bit-Plane Complexity Segmentation (BPCS){2}.

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

- Format image : bitmap (bmp), gif, pcx, jpeg, dll.
- Format audio : wav, voc, mp3, dll.
- Format lain : teks file, html, pdf, dll.

Kelebihan steganografi jika dibandingkan dengan 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{1}.

1.2. Metode Least Significant Bit

Least significant bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. Sedangkan most significant bit adalah sebaliknya, yaitu angka yang paling berarti/paling besar dan letaknya disebelah paling kiri.

Contohnya adalah bilangan biner dari 255 adalah 11111111 (kadang-kadang diberi huruf b pada akhir bilangan menjadi 1111 1111b).

Bilangan tersebut dapat berarti :

$1 * 2^7 + 1 * 2^6 + 1 * 2^5 + 1 * 2^4 + 1 * 2^3 + 1 * 2^2 + 1 * 2^1 + 1 * 2^0 = 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255$

Dari barisan angka 1 di atas, angka 1 paling kanan bernilai 1, dan itu adalah yang paling kecil. Bagian tersebut disebut dengan least significant bit (bit yang paling tidak berarti), sedangkan bagian paling kiri bernilai 128 dan disebut dengan most significant bit (bit yang paling berarti).

Least significant bit sering kali digunakan untuk kepentingan penyisipan data ke dalam suatu media digital lain, salah satu yang memanfaatkan Least significant bit sebagai metode penyembunyian dalah steganografi audio dan gambar.

Metode yang digunakan untuk penyembunyian pesan rahasia pada aplikasi ini adalah dengan cara menyisipkan pesan ke dalam bit rendah (least significant bit) pada data pixel yang menyusun file gambar BMP 24 bit tersebut.

Pada file gambar BMP 24 bit setiap pixel pada gambar terdiri dari susunan tiga warna yaitu merah, hijau, biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (1 byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Sebagai contoh file gambar BMP 24 bit dengan warna merah murni dalam format biner akan terlihat sebagai berikut :

00000000 00000000 11111111
00000000 00000000 11111111

Sedangkan untuk warna hijau murni dalam format biner akan terlihat sebagai berikut :

00000000 11111111 00000000
00000000 11111111 00000000

informasi dari warna biru berada pada bit pertama sampai bit delapan, dan informasi warna hijau berada pada bit sembilan sampai dengan bit 16, sedangkan informasi warna merah berada pada bit 17 sampai dengan bit 24.

Metode penyisipan LSB (least significant bit) ini adalah menyisipi pesan dengan cara mengganti bit ke 8, 16 dan 24 pada representasi biner file gambar dengan representasi biner pesan rahasia yang akan disembunyikan. Dengan demikian pada setiap pixel file gambar BMP 24 bit dapat disisipkan3 bit pesan, misalnya terdapat data raster original file gambar adalah sebagai berikut :

00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101001

Sedangkan representasi biner huruf A adalah 01000001, dengan menyisipkannya ke dalam pixel di atas maka akan dihasilkan

00100111 11101001 11001000
00100110 11001000 11101000
11001000 00100111 11101001

Terlihat pada bit kedelapan, enambelas dan 24 diganti dengan representasi biner huruf A, dan hanya tiga bit rendah yang berubah (cetak tebal), untuk penglihatan mata manusia sangatlah mustahil untuk dapat membedakan warna pada file gambar yang sudah diisi pesan rahasia jika dibandingkan dengan file gambar asli sebelum disisipi dengan pesan rahasia {3}.

1.3. Prototype

Howard (1997) mengemukakan bahwa prototyping adalah salah satu pendekatan dalam rekayasa perangkat lunak yang secara langsung mendemonstrasikan bagaimana sebuah perangkat lunak atau komponen-komponen perangkat lunak akan bekerja dalam lingkungannya sebelum tahapan konstruksi aktual dilakukan.

Prototyping merupakan salah satu metode pengembangan perangkat lunak yang banyak digunakan. Metode ini akan menghasilkan suatu prototype yaitu rancang bangun sistem yang akan dibuat atau biasa disebut dengan blueprint.

Kunci agar model prototype ini berhasil dengan baik adalah dengan mendefinisikan aturan-aturan main pada saat awal, yaitu pelanggan dan pengembang harus setuju bahwa prototype dibangun untuk mendefinisikan kebutuhan. Prototype akan dihilangkan sebagian atau seluruhnya dan perangkat lunak aktual aktual direkayasa dengan kualitas dan implementasi yang sudah ditentukan.

1.4. Blackbox Testing

Black-box testing adalah metode pengujian perangkat lunak yang tes fungsionalitas dari aplikasi yang bertentangan dengan struktur internal atau kerja (lihat pengujian white-box). pengetahuan khusus dari

kode aplikasi / struktur internal dan pengetahuan pemrograman pada umumnya tidak diperlukan.

Uji kasus dibangun di sekitar spesifikasi dan persyaratan, yakni, aplikasi apa yang seharusnya dilakukan. Menggunakan deskripsi eksternal perangkat lunak, termasuk spesifikasi, persyaratan, dan desain untuk menurunkan uji kasus. Tes ini dapat menjadi fungsional atau non-fungsional, meskipun biasanya fungsional. Perancang uji memilih input yang valid dan tidak valid dan menentukan output yang benar. Tidak ada pengetahuan tentang struktur internal benda uji itu.

Metode uji dapat diterapkan pada semua tingkat pengujian perangkat lunak: unit, integrasi, fungsional, sistem dan penerimaan.Ini biasanya terdiri dari kebanyakan jika tidak semua pengujian pada tingkat yang lebih tinggi, tetapi juga bisa mendominasi unit testing juga.

1.5. Blackbox Testing

Metode ujicoba blackbox memfokuskan pada keperluan fungsional dari software. Karna itu ujicoba. blackbox memungkinkan pengembang software untuk membuat himpunan kondisi input yang akan melatih seluruh syarat-syarat fungsional suatu program. Ujicoba blackbox bukan merupakan alternatif dari ujicoba whitebox, tetapi merupakan pendekatan yang melengkapi untuk menemukan kesalahan lainnya, selain menggunakan metode whitebox.

Ujicoba blackbox berusaha untuk menemukan kesalahan dalam beberapa kategori, diantaranya :

1. Fungsi-fungsi yang salah atau hilang
2. Kesalahan interface
3. Kesalahan dalam struktur data atau akses database eksternal
4. Kesalahan performa
5. Kesalahan inisialisasi dan terminasi

3. Analisis Sistem

Fungsi Utama Aplikasi Fungsi utama Aplikasi Steganografi adalah sebagai berikut :

"Untuk menyisipkan pesan berupa teks dan mengekstraknya kembali sesuai dengan pesan teks yang disisipkan kedalam file gambar".

3.1. Analisis Kebutuhan Dan Perancangan

Sistem steganografi yang dibahas akan di fokuskan kepada bagaimana cara membangun suatu sistem steganografi pada citra digital file gambar yang efisien dan untuk mengeksploitasi keterbatasan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada file gambar yang belum disisipi pesan rahasia. Sehingga dengan keterbatasan tersebut manusia sulit menemukan gradasi penurunan kualitas warna file gambar yang telah disisipi pesan rahasia. Sistem ini terdiri dari dua buah sub sistem yaitu : sistem penyisipan dan sistem pengekstrakkan.

Sistem penyisipan berfungsi untuk melakukan proses penyembunyian pesan ke file citra digital gambar. Komponen dari sistem penyisipan ini yaitu terdapat komponen untuk menuliskan pesan yang dipakai untuk menempatkan penulisan pesan rahasia.

Sistem pengekstrakkan berfungsi untuk melakukan pengekstrakkan file untuk memeperoleh pesan yang telah disisipkan ke dalam file gambar tersebut. Komponen pada sistem pengekstrakkan ini terdapat komponen untuk membaca baca pesan yang digunakan untuk menempatkan pesan rahasia yang akan dibaca, sehingga keluarannya akan memulai proses pemisahan pesan rahasia dari file gambar.

3.2. Implementasi Sistem

3.2.1. Lingkungan Pemograman

Aplikasi Steganografi ini dibuat dengan menggunakan bahasa pemograman Delphi dan dikembangkan menggunakan Aplikasi Delphi 2007.

3.2.2. Perancangan Perangkat Lunak

Dalam pembuatan program steganografi dan tentunya juga menggunakan teknik steganografi yaitu penyisipan LSB. Walaupun terbilang sederhana, tapi keamanaan informasi tetaplah hal utama yang harus diperhatikan.

Untuk itu dalam prakteknya perlu mengkombinasikan steganografi penyisipan LSB dengan algoritma kriptografi RC4. Perlu diketahui untuk keperluan kriptografi kita menggunakan sebuah komponen built in yaitu DCPChiper.

Dalam pembuatan perangkat lunak kami menggunakan DELPHI 7, yang terdiri dari beberapa komponen yaitu :

2 TImage, 2 TButton untuk Reset, 2 TButton masing-masing bersungsi sebagi trigger Encoding dan Decoding, 2 TMemo sebagai interface masukan data pesan pada proses Encoding dan Decoding, sebagai media carrier menggunakan sebuah file bitmap (BMP) 24bit. beberapa fungsi dan properti yang kita gunakan.

Beberapa di antaranya:

Str, procedure delphi yang digunakan untuk konversi atau memformat tipe data integer ke tipe data string. Fungsi ini terdiri dari 2 parameter yaitu nilai integer yang akan dikonversi dan variable string untuk menyimpan nilai balik.

Trunc, adalah fungsi delphi untuk konversi tipe data real (pecahan) ke tipe data integer (bulat). Fungsi ini hanya meminta nilai data real sebagai masukan untuk dikonversi dan tentunya kita membutuhkan variable eksternal untuk menerima nilai baliknya.

Exp, fungsi delphi untuk melakukan operasi eksponensial atau pemangkatan. Hanya membutuhkan sebuah parameter masukan nilai angka yang akan dipangkatkan dan hasil operasinya akan disimpan pada eksternal variable.

Ord, fungsi yangdigunakan untuk mendapatkan nilai posisi atau urutan dari sebuah data. Data bisa berupa integer, karakter dan lain-lain.

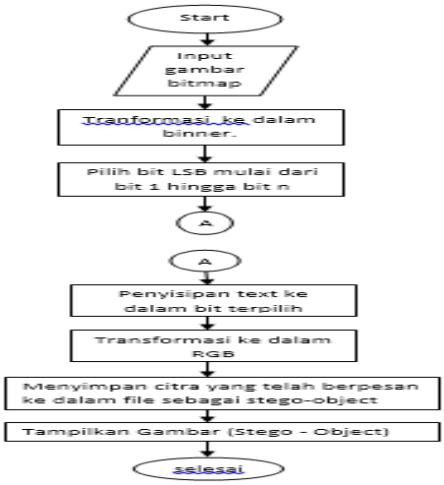
Chr, fungsi untuk mendapatkan karakter dalam bentuk AnsiChar maupun WideChar dari sebuah nilai posisi berupa integer.

GetPixel, adalah fungsi untuk mendapatkan data pixel pada sebuah area canvas, apakah itu canvas TImage, form dan lain-lain. Fungsi ini memutuhkan 3 nilai paramter yakni handle canvas sumber, indeks kolom pixel dan indeks baris pixel.

GetRValue, GetGValue, GetBValue, masing-masing adalah fungsi untuk mengambil nilai warna merah, hijau dan biru pada sebuah nilai pixel (nilai pixel bisa juga didapatkan dari hasil fungsi GetPixel).

Pixels, merupakan sebuah property dari object TCanvas, yang mempunyai 2 buah direktiv yaitu x dan y yang mewakili titik koordinat baris dan kolom.

Berikut gambaran flowchart sistem stenografi yang digunakan :



Gambar 1. Diagram alir proses penyisipan pesan

Gambar 2

Gambar 2. Diagram alir proses ekstraksi pesan

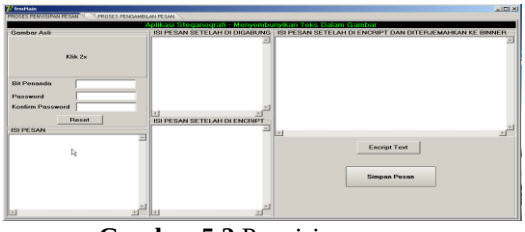
Seperti yang telah disebutkan sebelumnya, pada module enkripsi dan dekripsi kita membutuhkan fungsi built in dari komponen kriptografi DCPChiper dan *RC4* merupakan algoritma yang kita gunakan untuk mengacak data pesan seperti terlihat pada block definisi variable *Cipher: TDCP_rc4*.

Sebenarnya masih banyak algoritma yang disediakan oleh komponen DCPChiper seperti *DES, RIJNDAEL, ICE, BLOWFISH* serta beberapa algoritma dan fungsi hash lainnya, namun karena alasan kemudahan dan sesuai dengan tujuan program kali ini, maka saya memilih untuk menggunakan algoritma RC4.

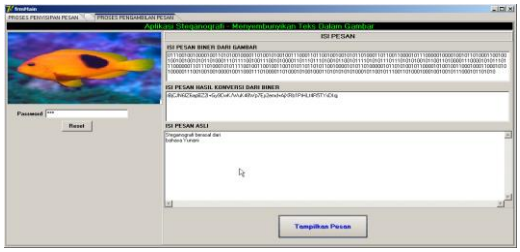
Algoritma RC4 termasuk dalam kelompok algoritma konvensional dan merupakan algoritma simetri yakni algoritma yang menggunakan kunci atau password yang sama pada proses enkripsi dan dekripsi. Karena alasan itu juga saya memilih untuk mengimplementasikan algoritma RC4 pada badan program. Pada urutan proses program nantinya user akan diminta untuk memasukkan password yang sama saat akan menyisipkan maupun menguraikan data pesan.

1. Langkah pertama yang dilakukan pada proses encoding adalah mencopy data bitmap dari imgEncode ke sebuah variable global Bmp kemudian mengatur format pixel Bmp menjadi 24bit, artinya akan terdapat 24 bit pada setiap pixel, hal ini perlu diperhatikan karena ketika data disisipkan program menggunakan format 8 bit untuk 1 byte warna.
2. Langkah kedua adalah mengecek apakah file bitmap bisa disisipi pesan, dengan menggunakan fungsi CarrierCheck. Jika nilai balik fungsi true, proses penyisipan akan dilanjutkan.
3. Langkah selanjutnya adalah menghitung total LSB yang bisa digunakan untuk menyisipkan data, dari hasil perhitungan ini nantinya digunakan untuk melakukan validasi apakah sebuah file bitmap mampu menampung data pesan yang diinputkan, di mana total jumlah data pesan adalah panjang password + 1 karakter pemisah (#) + panjang pesan. Jika jumlah LSB tidak mencukupi maka proses penyisipan tidak dilanjutkan.
4. Terakhir yaitu menentukan string penanda @d@ dalam bentuk biner 8 bit.

3.3. Interface Program



Gambar 5.2 Penyisipan pesan

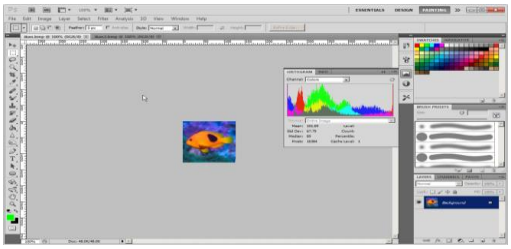


Penguraian Pesan

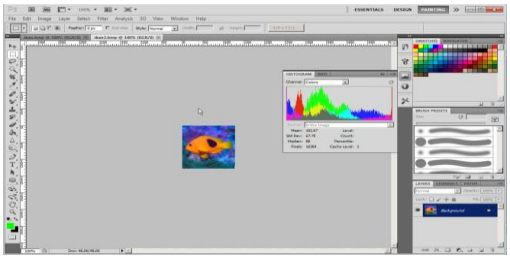
4. Hasil Penelitian

Pengujian

Pengujian ini menggunakan metode pengujian *Black Box*. Pengujian ini berusaha menemukan kesalahan dalam beberapa kategori sebagai berikut : fungsi-fungsi yang tidak benar atau hilang, kesalahan interface, kesalahan kinerja, inisialisasi dan kesalahan terminasi.



Gambar 5.1 Pengujian Histogram File Asli



Gambar 5.2 Pengujian Histogram File yang sudah disisipi pesan.

5. Kesimpulan

Berdasarkan hasil penelitian yang penulis lakukan dengan tema steganografi, dengan mengambil judul aplikasi steganografi ini, diharapkan dapat digunakan untuk membantu user internet dalam bertukar pesan dengan tingkat keamanan yang lebih baik.

Berdasarkan analisis yang telah penulis buat, maka dapat diambil kesimpulan :

1. Dengan aplikasi steganografi ini dapat melindungi transaksi pengiriman pesan antara dua pihak yang saling bertukar pesan.
2. Aplikasi ini dapat menyamarkan pesan, karena secara kasat mata pesan tidak akan terlihat, dan terlihat sebagai gambar biasa.

Daftar Pustaka

[1] Andriawan,M. Anggrie. Solikin. Ismail, Setia Juli Irzal.2012. Implementasi Steganografi Pada Citra Digital File Gambar Bitmap (Bmp) Menggunakan Java. Program Studi Teknik Komputer. Politeknik Telkom Bandung.

[2] Dewi,S inta. Wibowo, Agus Urip Ari. Rachmawati, Heni.2012. Analisis Perbandingan Steganografi Pada Citra Digital Gif Dan Tiff Dengan Metode Bpcs. Teknik Informatika. Politeknik Caltex Riau.

[3] Utomo,Tri Prasetyo. 2012. Steganografi Gambar Dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media Online Jurnal. Jurusan Teknik Informatika. Fakultas Sains Dan Teknologi.