

STUDI PERBANDINGAN ENKRIPSI STEGANOGRAFI DENGAN MENGGUNAKAN METODE *LEAST SIGNIFICANT BIT* DAN *END OF FILE*

Harianto Antonio

Program Studi Teknik Informatika
Jurusan Teknik Elektro Fakultas Teknik Universitas Tanjungpura
antonio09041@gmail.com

Abstract- Communications and information technology is rapidly grows and provides a major influence on people's lives. The rapid development of information technology is currently supported by the importance of the need for information. It can be seen from the development of today's internet network is rapidly increasing. Informations that transmitted is not meant for everyone. Along with the development of these technologies, security threats becomes more and more powerful, particularly for the undisclosed information. Various threats in cyberspace such as hacker, cracker, carder makes people worry about the security of the information they sends. This concern that make the development of information hiding techniques. One of the well known information hiding technique is steganography. In general, steganography means a technique and art of hiding a fact to communicate. By using steganography, secret message can be inserted into an unsuspecting information and send it without being aware of the existence of the secret message. There are several criteria that must be considered in steganography is fidelity, robustness, and recovery. Fidelity means that stegomedium quality has not changed much due to the insertion. The changes can not be perceived by the senses.

Keywords: *computer answer sheet, smart scanning techniques, image preprocessing, scanline, computer answer sheet correction*

1. Pendahuluan

Teknologi komunikasi dan informasi berkembang dengan sangat pesat dan memberikan pengaruh besar terhadap kehidupan manusia. Cepatnya perkembangan teknologi informasi saat ini didukung dengan pentingnya kebutuhan akan mendapatkan informasi. Hal ini dapat dilihat dari berkembangnya jaringan internet saat ini yang

semakin pesat. Informasi yang dikirimkan tidak hanya informasi untuk semua orang. Seiring dengan perkembangan teknologi tersebut, ancaman terhadap keamanan informasi yang dibutuhkan semakin besar, terutama untuk informasi yang dirahasiakan tersebut. Berbagai ancaman di dunia maya seperti *hacker, cracker, carder* membuat orang khawatir akan keamanan informasi yang dikirimnya. Kekhawatiran inilah yang membuat berkembangnya teknik penyembunyian informasi yang akan dikirimkan. Teknik penyembunyian informasi yang cukup terkenal adalah steganografi.

Steganografi berasal dari bahasa Yunani yaitu kata *stegos* yang berarti sembunyi dan *graphia* yang berarti tulisan. Steganografi secara umum memiliki arti ilmu dan seni menyembunyikan suatu fakta untuk berkomunikasi. Dengan menggunakan steganografi, pesan rahasia dapat disisipkan ke dalam sebuah informasi yang tidak mencurigakan dan mengirimkannya tanpa ada yang mengetahui keberadaan dari pesan rahasia tersebut. Beberapa kriteria yang harus diperhatikan dalam steganografi adalah *fidelity, robustness, dan recovery*. *Fidelity* berarti mutu *stegomedium* tidak berubah banyak akibat penyisipan. Perubahan tersebut tidak dapat dipersepsi oleh inderawi. Misalnya, jika *covertext* berupa citra, maka penyisipan pesan membuat citra *stegotext* sukar dibedakan oleh mata dengan citra *covertext*-nya. Untuk kriteria *robustness* berarti data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung (seperti pengubahan kontras, penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan (*cropping*), dan sebagainya). Bila pada citra dilakukan operasi pengolahan citra, maka data yang disembunyikan tidak rusak. Kriteria *recovery* sendiri berarti bahwa pesan yang disembunyikan harus dapat diungkapkan kembali. Karena tujuan steganografi adalah *data hiding*, maka sewaktu-waktu pesan rahasia di dalam *stegotext* harus dapat diambil kembali untuk digunakan lebih lanjut. Teknik

steganografi memiliki beberapa metode yang dapat digunakan, seperti metode *Least Significant Bit* (LSB) dan metode *End Of File* (EOF). Kedua metode ini memiliki ciri tersendiri dalam proses enkripsi dan dekripsi data, selain itu metode ini sendiri masih digunakan dalam pengembangan ilmu steganografi ini sendiri untuk menciptakan metode-metode baru dalam dunia steganografi. Berdasarkan hal di atas, maka penulis akan mengkaji beberapa algoritma steganografi, yaitu algoritma LSB dan EOF kemudian membandingkan kedua metode tersebut dengan tujuan memudahkan pengguna dalam memilih algoritma yang tepat sesuai dengan kebutuhan.

2. Teori Dasar

2.1 Gambar Digital

Gambar digital merupakan dokumen berbentuk *file* yang dihasilkan melalui perangkat elektronik atau media digital (Ahmad, 2005). Sebuah gambar digital terdiri atas piksel-piksel. Piksel adalah akronim dari *Picture Element*. Setiap piksel mengandung informasi mengenai warna piksel tersebut. Warnanya bisa dalam susunan Merah, Hijau, Biru (*Red, Green, Blue* atau RGB), atau bisa juga dalam sistem warna yang lain, misal *Hue Saturation Value* (HSV) dan *Cyan Magenta Yellow Key* (CMYK).

Biasanya, setiap warna direpresentasikan oleh bilangan biner sebanyak 8 *bit*. Dengan demikian, setiap piksel mengandung minimal 3 x 8 *bit* = 24 *bit* data, yaitu 8 *bit* untuk merah, 8 *bit* untuk hijau, dan 8 *bit* untuk biru.

Ukuran sebuah gambar biasanya dinamakan resolusi. Resolusi berarti dimensi gambar dalam piksel. Misalnya, sebuah gambar berukuran 800 x 600 piksel berarti memiliki panjang 800 piksel dan lebar 600 piksel. Total piksel dalam gambar tersebut adalah 480.000 piksel. Jika setiap piksel mengandung informasi warna sebanyak 24 *bit*, ukuran digital gambar tersebut adalah 480.000 x 24 *bit* = 11.520.000 *bit* = 11.250 *Kbit* = 10,99 *Mbit* = 1,37 *MByte* (1 *Byte* = 8 *bit*) Ini adalah ukuran minimal, karena biasanya gambar digital juga mengandung *meta-data* mengenai gambar tersebut. *Meta-data* gambar menambah ukuran *file* digital meskipun biasanya ukurannya tidak terlalu besar. *Meta-data* diantaranya mengandung waktu pembuatan gambar, resolusi, jenis pemampatan (*compression*) dan pembuat gambar.

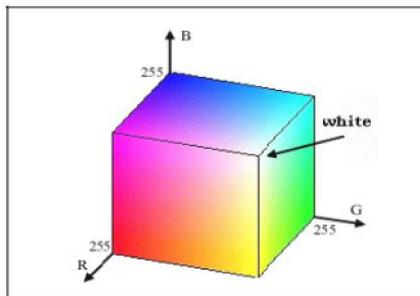
Ada beberapa tipe gambar digital yang sering digunakan yaitu:

1. *Bitmap* (BMP)
Tipe *file* BMP umum digunakan pada sistem operasi Windows dan OS/2. Kelebihan tipe *file* BMP adalah dapat dibuka oleh hampir semua aplikasi pengolah gambar. Baik *file* BMP yang terkompresi maupun tidak terkompresi, *file* BMP memiliki ukuran yang lebih besar daripada tipe-tipe yang lain.
2. *Joint Photographic Experts Group* (JPG/ JPEG)
Tipe *file* JPG sangat sering digunakan untuk *web* atau *blog*. *File* JPG menggunakan teknik kompresi yang menyebabkan kualitas gambar turun (*lossy compression*). Setiap kali menyimpan ke tipe JPG dari tipe lain, ukuran gambar biasanya mengecil, tetapi kualitasnya turun dan tidak dapat dikembalikan lagi. Ukuran *file* BMP dapat turun menjadi sepersepuluhnya setelah dikonversi menjadi JPG. Meskipun dengan penurunan kualitas gambar, pada gambar-gambar tertentu (misalnya pemandangan), penurunan kualitas gambar hampir tidak terlihat mata.
3. *Graphics Interchange Format* (GIF)
Tipe *file* GIF memungkinkan penambahan warna transparan dan dapat digunakan untuk membuat animasi sederhana, tetapi saat ini standar GIF hanya maksimal 256 warna saja. *File* ini menggunakan kompresi yang tidak menghilangkan data (*lossless compression*) tetapi penurunan jumlah warna menjadi 256 sering membuat gambar yang kaya warna seperti pemandangan menjadi tidak realistis. Pada program Microsoft Paint, tidak ada fasilitas penyesuaian warna yang digunakan (*color table*) sehingga menyimpan *file* GIF di Microsoft Paint seringkali menghasilkan gambar yang terlihat rusak atau berubah warna. Pada program pengolah gambar yang lebih baik, seperti Adobe Photoshop, *color table* bisa diatur otomatis atau manual sehingga gambar tidak berubah warna atau rusak.
4. *Portable Network Graphics* (PNG)
Tipe *file* PNG merupakan solusi kompresi yang kuat dengan warna yang lebih banyak (24 *bit* RGB + alpha). Berbeda dengan JPG yang menggunakan teknik kompresi yang menghilangkan data, *file* PNG menggunakan kompresi yang tidak menghilangkan data (*lossless compression*). Kelebihan *file* PNG adalah adanya warna transparan dan alpha. Warna alpha memungkinkan sebuah gambar transparan, tetapi gambar tersebut masih dapat dilihat mata seperti samar-samar atau bening. *File* PNG dapat diatur jumlah warnanya 64 *bit* (*true color* + alpha) sampai *indexed color* 1

bit. Dengan jumlah warna yang sama, kompresi *file* PNG lebih baik daripada GIF, tetapi memiliki ukuran *file* yang lebih besar daripada JPG. Kekurangan tipe PNG adalah belum populer sehingga sebagian *browser* tidak mendukungnya.

2.2 RGB

Warna pada dasarnya adalah hasil persepsi cahaya dalam spektrum wilayah yang terlihat oleh retina mata, dan memiliki panjang gelombang antara 400 nm sampai dengan 700 nm. Ruang warna RGB dapat divisualisasikan sebagai sebuah kubus seperti pada Gambar 2.1, dengan tiga sumbu yang mewakili komponen warna merah (*red*) R, hijau (*green*) G, biru (*blue*) B. Salah satu pojok alasnya yang berlawanan menyatakan warna hitam ketika $R = G = B = 0$, sedangkan pojok atasnya yang berlawanan menyatakan warna putih ketika $R = G = B = 255$ (sistem warna 8 bit bagi setiap komponennya).



Gambar 2.1 Komponen Warna RGB
Sumber: Ahmad, 2005

RGB sering digunakan di dalam sebagian besar aplikasi komputer karena dengan ruang warna ini tidak diperlukan transformasi untuk menampilkan informasi di layar monitor. Alasan ini juga yang menyebabkan RGB banyak dimanfaatkan sebagai ruang warna dasar bagi sebagian besar aplikasi.

2.3 Steganografi

2.3.1 Definisi Steganografi

Menurut Krenn, J.R (2004), Steganografi berasal dari bahasa Yunani yaitu *stegos* yang berarti atap atau tertutup dan *graphia* yang berarti tulisan, jadi steganografi adalah ilmu dan seni menyembunyikan keberadaan komunikasi. Dengan menggunakan steganografi pesan rahasia dapat disisipkan ke dalam sebuah media yang tidak mencurigakan dan mengirimnya tanpa ada seorangpun yang mengetahui keberadaan pesan tersebut. Steganografi berbeda dengan kriptografi yaitu terletak pada hasil keluarannya. Hasil dari kriptografi memiliki bentuk yang berbeda dengan data asli, sehingga informasi yang ada pada data

tersebut diketahui tetapi tidak dimengerti karena informasi tersebut dikodekan terlebih dahulu. Sedangkan hasil dari keluaran steganografi memiliki bentuk yang sama dengan data aslinya, sehingga keberadaan informasi yang disembunyikan tidak terlihat menurut persepsi indra manusia tetapi tidak oleh komputer atau pengolah data digital lainnya. Secara umum steganografi dan kriptografi mempunyai tujuan yang sama yaitu menyembunyikan informasi supaya tidak dapat dibaca, dimengerti atau diketahui secara langsung. Steganografi memanfaatkan keterbatasan yang ada pada indra manusia seperti mata dan telinga. Dengan keterbatasan inilah maka steganografi dapat diterapkan dalam berbagai media digital. Kualitas dari kriptografi terletak pada informasi kunci rahasia, sedangkan pada steganografi terletak pada ada-tidaknya pesan rahasia. Keamanan kriptografi menjadi patah jika kunci rahasia diketahui, sedangkan keamanan dari steganografi menjadi patah jika keberadaan pesan rahasia diketahui meskipun isi pesan belum diketahui. Menyisipkan data yang ingin disembunyikan ke dalam sebuah media membutuhkan dua buah arsip. Pertama adalah arsip media penampung seperti citra, suara, video dan sebagainya yang terlihat tidak mencurigakan untuk menyimpan pesan rahasia. Arsip kedua adalah arsip pesan yang ingin disembunyikan, dapat berupa *plaintext*, *chipertext*, citra lain, atau apapun yang dapat disembunyikan dalam *bit stream*.

Terdapat beberapa istilah yang berkaitan dengan steganografi, yaitu:

1. *Embedded message* atau *hiddentext*: pesan rahasia yang disembunyikan
2. *Cover-object* atau *covertext*: media yang digunakan untuk menyembunyikan *hiddentext*. Media ini disebut juga media pembawa, citra penutup, *cover-image*, dan *cover medium*.
3. *Stego-object* atau *stegotext*: media yang sudah berisi *hiddentext*. Untuk media yang berupa citra sering disebut *stego-image* atau *stegogram*.
4. *Stego-key*: kunci yang digunakan untuk mengacak posisi pesan pada saat penyisipan pesan dan mengekstraksi pesan dari *stego-object*. Misalnya *password*.
5. Steganografer: orang yang merancang metode steganografi.
6. Steganalisis: seni dan ilmu dalam mendeteksi ada-tidaknya pesan tersembunyi dalam sebuah objek.
7. Steganalis: orang yang berusaha untuk memecahkan metode steganografi dengan menggunakan berbagai metode steganalisis.

2.3.2 Least Significant Bit (LSB)

Metode ini banyak digunakan karena komputasinya tidak terlalu kompleks dan pesan yang disembunyikan cukup aman. Metode ini memodifikasi nilai yang paling kurang signifikan dari jumlah *bit* dalam 1 *byte file carrier*. *Bit* yang memiliki signifikansi paling tinggi adalah numerik yang memiliki nilai tertinggi (misal, $2^8 = 256$), artinya bila terjadi perubahan pada *bit* ini akan menghasilkan perubahan yang sangat signifikan. *Bit* yang memiliki signifikansi paling rendah adalah numerik yang memiliki nilai terendah (misal, $2^0 = 1$), artinya bila terjadi perubahan pada *bit* ini akan menghasilkan perubahan yang tidak terlalu signifikan. Untuk menjelaskan metode ini, digunakan citra digital sebagai *coverimage*. Setiap *pixel* dalam citra digital berukuran 1 sampai 3 *byte*. Pada susunan *bit* dalam *byte* (1 *byte* = 8 *bit*), terdapat *bit* yang paling kanan atau disebut juga *Least Significant Bit*. Misalnya pada 00011001, maka *bit* LSB adalah *bit* yang terletak paling kanan yaitu 1. Untuk melakukan penyisipan pesan, *bit* yang paling cocok untuk diganti dengan *bit* pesan adalah *bit* LSB, sebab pengubahan bit tersebut hanya akan mengubah nilai *byte*-nya menjadi satu *bit* lebih tinggi atau satu *bit* lebih rendah. Besar pesan yang dapat disisipkan menggunakan metode LSB sangat bergantung dari ukuran citra *carrier*, yaitu besar ukuran citra *carrier* dibagi dengan delapan, hal ini disebabkan diperlukan delapan buah *byte* untuk setiap penyisipan satu buah karakter dari pesan yang akan disisipkan.

2.3.3 End Of File (EOF)

Teknik EOF merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini berbeda dengan teknik LSB yang mengubah nilai warna dari setiap pixel dari gambar, teknik ini menyisipkan pesan menggunakan cara dengan menyisipkan pesan langsung pada akhir file. Teknik ini tidak seperti metode LSB yang memiliki batasan ukuran pesan sehingga teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Dalam teknik ini, pesan yang disisipkan pada akhir file akan memiliki tanda khusus sebagai pengenalan start dari pesan tersebut dan pengenalan akhir dari pesan tersebut.

Proses yang terjadi dalam penyisipan pesan dengan metode EOF adalah dengan mengubah pesan menjadi kode desimal, dapatkan nilai atau letak piksel terakhir dari citra, berikan sebuah tanda pengenalan start dari pesan dan tambahkan kode desimal dari pesan. Sedangkan pada proses pengungkapan pesan, maka proses yang diperlukan adalah mengenali letak tanda pengenalan dan mengambil nilai desimal dari pesan rahasia serta terakhir mengubah nilai desimal menjadi sebuah pesan.

Proses penyisipan pesan dengan metode EOF dapat dilihat pada Gambar 2.2.



Gambar 2.2 Diagram alir proses penyisipan pesan metode EOF

Proses pengungkapan pesan dengan metode EOF dapat dilihat pada Gambar 2.3.



Gambar 2.3 Diagram alir proses pengungkapan pesan metode EOF

2.4 Steganalisis secara statistik

Ide yang mendasari metode ini adalah membandingkan distribusi frekuensi pada gambar dengan suatu contoh distribusi lain yang secara teori adalah gambar yang telah disisipi pesan. Metode yang dibahas adalah teknik perhitungan *Peak Signal to Noise Ratio* (PSNR).

PSNR adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan desibel. Pada penelitian ini, PSNR digunakan untuk

mengetahui perbandingan kualitas citra sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus ditentukan nilai rata-rata kuadrat dari error atau *Mean Square Error* (MSE). Cara Perhitungan MSE seperti yang digambarkan dalam Persamaan 2.1.:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} ||I(i,j) - K(i,j)||^2 \quad (2.1)$$

Dimana:

m dan n = dimensi dari gambar
 I(i,j) = piksel dari gambar asli
 K(i,j) = piksel dari gambar yang mengandung pesan
 PSNR sangat berkaitan erat dengan MSE. Hubungan antara MSE dan PSNR berbanding terbalik. Semakin kecil nilai MSE berarti nilai *error* semakin kecil. Semakin tinggi nilai PSNR berarti semakin bagus karena rasio *Signal-to-Noise* akan semakin tinggi. PSNR adalah ukuran kesamaan gambar dengan mengukur perbedaan piksel antara gambar asli dan gambar yang mengandung pesan. Cara Perhitungan PSNR digambarkan dalam Persamaan 2.2.

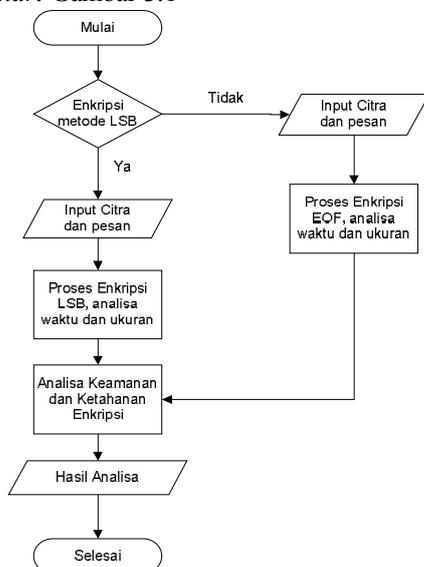
$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) = 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \quad (2.2)$$

Dimana:

MAX_I = nilai piksel maksimum dari gambar asli
 MSE = nilai MSE

3. Hasil Eksperimen

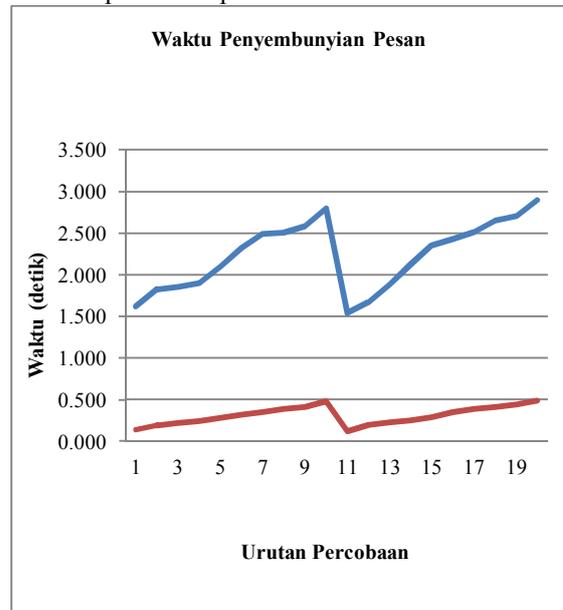
Secara garis besar, alur kerja aplikasi yang dirancang seperti yang digambarkan pada *flowchart* Gambar 3.1



Gambar 3.1 *Flowchart* Diagram alir system

3.1 Analisis Perbandingan Waktu

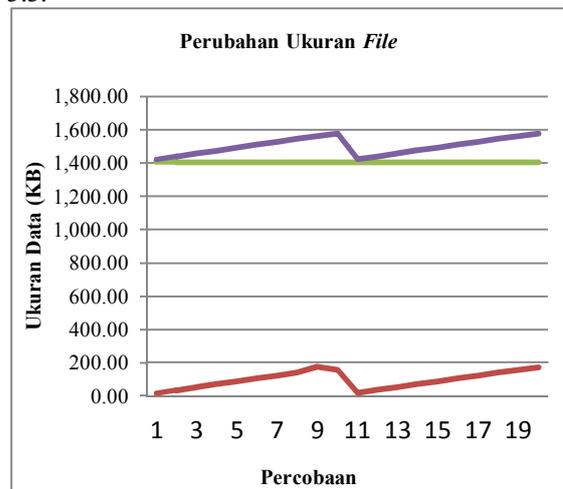
Hasil dari analisis perbandingan waktu yang telah dilakukan dapat diketahui bahwa waktu yang diperlukan dalam penyembunyian dan pengambilan pesan dipengaruhi oleh *file* rahasia yang akan disembunyikan. Hasil pengujian perbandingan waktu dapat dilihat pada Gambar 3.2



Gambar 3.2 Grafik waktu penyembunyian pesan

3.2 Analisis Ukuran Data

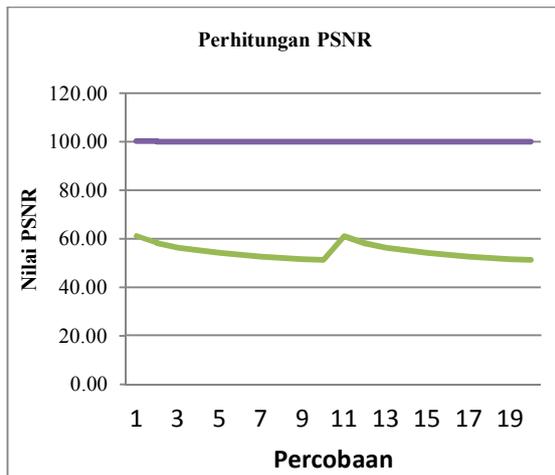
Hasil dari analisis ukuran data yang telah dilakukan dapat diketahui bahwa pengaruh ukuran data terhadap citra yang akan disembunyikan. Hasil pengujian ukuran data dapat dilihat pada Gambar 3.3.



Gambar 3.3 Grafik perubahan ukuran *file*

3.3 Analisis Keamanan

Hasil dari analisis keamanan yang telah dilakukan dapat diketahui bahwa keamanan dari metode berdasarkan perhitungan PSNR. Hasil pengujian perbandingan keamanan dapat dilihat pada gambar 3.4



. Gambar 3.4 Grafik perhitungan PSNR

3.3 Analisis Ketahanan

Hasil dari analisis ketahanan yang telah dilakukan dapat diketahui dengan melakukan percobaan sebanyak 60 kali dimana setiap percobaan dilakukan manipulasi terhadap citra stegaimage. Dari percobaan yang dilakukan diketahui kedua metode gagal dalam pengujian ketahanan

4. Kesimpulan

1. Metode EOF memerlukan waktu yang lebih sedikit dibandingkan dengan metode LSB dalam penyisipan pesan.
2. Waktu yang dibutuhkan dalam proses penyisipan pesan akan semakin besar seiring bertambahnya ukuran file pesan yang disembunyikan.
3. Stegaimage dari steganografi metode LSB memiliki ukuran data yang sama dengan file cover, sedangkan stegaimage dari steganografi metode EOF memiliki ukuran data yang lebih besar dari file cover.
4. Berdasarkan hasil analisis keamanan, metode EOF lebih baik dibandingkan dengan metode LSB dalam pendeteksian secara statistik perhitungan *Peak to Signal Ratio* (PSNR).
5. Metode LSB dan EOF gagal mengambil pesan yang telah disisipkan ke dalam stegaimage yang telah dilakukan proses manipulasi gambar.
6. Perbedaan tipe file pesan rahasia tidak mempengaruhi waktu, ukuran, serta pengukuran PSNR.

5. Referensi

- Aditya, Yogie., Andhika Pratama, dan Alfian Nurlifa. (2010). *Studi Pustaka Untuk Steganografi dengan Beberapa Metode*. Jurusan Teknik Informatika. Universitas Islam Indonesia.
- Ahmad, Usman. (2005). *Pengolahan Citra Digital dan Teknik Pemrogramannya*. Yogyakarta: Graha Ilmu.

- Bender, W. (1996). *Techniques for Data Hiding*. diakses pada tanggal 10 Januari 2013 dari <http://cs.utsa.edu/~jortiz/Techniques%20or%20Data%20Hiding-p.pdf>.
- Cenadep. (2012). *Steganography Dengan Metode EOF*. diakses pada tanggal 24 Januari 2013 dari <http://www.cenadep.org/2012/05/18/steganography-dengan-metode-eof/>.
- Hariyanto, Paul Gunawan. (2007). *Studi dan Analisis Mengenai Teknik Steganalisis Terhadap Pengubahan LSB Pada Gambar: Enhanced LSB dan Chi-square*. Departemen Teknik Informatika. Institut Teknologi Bandung.
- Munir, Rinaldi. (2004). *Bahan Kuliah IF5054 Kriptografi*. Departemen Teknik Informatika, Institut Teknologi Bandung.
- Sejati, A. (2010). *Studi dan Perbandingan Steganografi Metode EOF(End of File) dengan DCS(Dynamic Cell Spreading)*. ITB. Bandung.
- Sugiono, Eko. (2011). *Perancangan Aplikasi Pengiriman Attachment E-mail Berbasis Desktop Menggunakan Metode Steganografi Least Significant Bit(LSB) Pada Citra Bitmap 24 Bit*. Teknik Informatika. Universitas Tanjungpura. Pontianak.
- Krenn, J.R. (2004). *Steganography and Steganalysis*. diakses pada tanggal 4 Januari 2013 dari <http://www.krenn.nl/univ/cry/steg/article.pdf>.

Biography

Hariato Antonio, lahir di Pontianak, Kalimantan Barat, 20 November 1991. Memperoleh gelar Sarjana Teknik dari Fakultas Teknik Universitas Tanjungpura, Pontianak, Indonesia pada tahun 2013.