PERBANDINGAN DIGITAL STEGANOGRAFI PADA MEDIA IMAGE, AUDIO, VIDEO DAN TEKS SERTA KEKUATANNYA TERHADAP STEGANALISIS

James Filipus – NIM : 13507087
IF3058 – Kriptografi, Semester II 2009-2010
Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
e-mail: if17087@students.if.itb.ac.id

ABSTRAK

Digital steganografi merupakan sebuah sarana penyembunyian pesan atau data yang sangat diminati karena mampu menyembunyikan pesan atau data dalam sebuah media digital khususnya *image*, *audio*, *video* dan *teks*. Untuk menjaga keamanan dari pesan yang disembunyikan maka perlu diketahui media mana yang paling baik untuk menyembunyikan pesan, karena setiap media tentu memiliki karakteristik yang berbeda dan kualitas hasil steganografi yang berbeda pula. Metode yang digunakan untuk steganografi juga akan mempengaruhi kekuatan dari hasil steganografi terhadap steganalisis.
Masalah terbesar dalam steganografi adalah membuat orang yang melihat media yang sudah disisipi pesan tidak menyadari bahwa pada media tersebut terdapat sebuah pesan yang disembunyikan karena apabila kita menyisipkan pesan ke dalam byte atau anatar bit dari media mungkin saja merubah tampilan luarnya sehingga dapat disadari oleh orang yang melihatnya. Maka perlu dilakukan perbandingan antar ketiga media tersebut serta teknik steganografi yang digunakan untuk menemukan media serta teknik steganografi yang terbaik dihubungkan dengan kekuatannya terhadap steganalisis. Karena pada umumnya orang bahkan tidak akan bersusah payah mencoba untuk mengungkap, mengekstraksi, menyadap atau mengganti pesan dalam sebuah media apabila orang tersebut tidak menyadari bahwa dalam media yang dilihatnya ada pesan yang disembunyikan. Selain itu dalam steganografi perlu diperhatikan *fidelity* dari media, *robustness* dan *recovery* dari pesan atau data yang disembunyikan.
Tujuan dari penelitian ini yaitu untuk mendeteksi pesan dalam media yang digunakan untuk tujuan yang buruk atau digunakan oleh pihak jahat seperti teroris untuk meyebarkan pesan terorisme ke anggotanya yang lain, sehingga terorisme dapat dicegah.

Kata kunci: Digital steganografi, media steganografi, image, *teks*, video, audio, *fidelity*, *robustness*, *recovery*, steganalisis, terorisme.

1. PENDAHULUAN

Di jaman modern sekarang ini keamanan (*security)* dari informasi menjadi isu penting yang terus dicari solusinya. Setiap orang tidak ingin informasinya diketahui oleh orang yang tidak berkepentingan terlebih lagi bila informasi tersebut merupakan informasi rahasia. Terlebih lagi dengan adanya internet, semakin banyak celah di internet yang dapat digunakan untuk menyadap dan mendapatkan informasi rahasia tersebut apabila pengirim tidak berhati-hati. Steganografi merupakan salah satu cara penyembunyian pesan yang dimaksudkan agar pesan tidak dapat diketahui oleh pihak lain. Inti dari steganografi adalah untuk menyembunyikan pesan dalam sebuah media sedemikian rupa sehingga pesan tersebut tidak terdeteksi keberadaannya oleh indera manusia.

2. DIGITAL STEGANOGRAFI

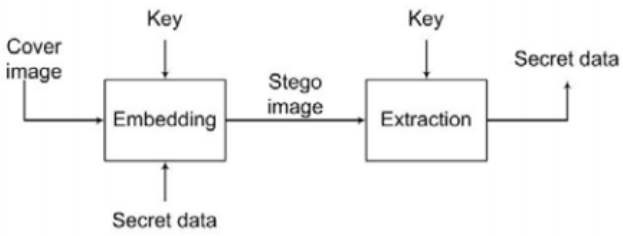
Ada dua property utama yang dibutuhkan oleh steganografi yaitu wadah penampung (media) dan pesan atau data rahasia yang akan disembunyikan.

Pada makalah ini akan dibahas khusus tentang *digital* steganografi, oleh karena itu media yang digunakan yaitu media digital seperti image, audio, video dan teks. Selain itu steganografi dapat digunakan sebagai kelanjutan dari kriptografi, sehingga dapat meningkatkan keamanan dari pesan. Dengan terlebih dahulu mengenkripsi pesan lalu kemudian chiperteks hasil enkripsi tersebut baru kemudian disembunyikan dalam media steganografi. Dengan demikian diperlukan dua buah kunci untuk mendapatkan pesan yang sebenarnya dan lebih sulit untuk dipecahkan, bahkan belum tentu keberadaan cipherteks itu dapat disadari oleh orang yang melihatnya.

Dalam steganografi, penyisipan pesan dalam suatu media pasti akan mengubah media tersebut karena ada pesan yang disisipkan ke dalam media tersebut baik disispkan dalam byte atau antar bit media. Akan tetapi perubahan tersebut belum tentu disadari oleh orang yang

melihatnya. Oleh karena itu ada tiga faktor yang perlu diperhatikan dalam penyembunyian data :

- Fidelity
  Penyembunyian pesan harus dapat menjaga kualitas dari media yang digunakan agar media tidak jauh berubah dan tidak dapat disadari perubahannya oleh indera manusia.
- Robustness
  Pesan atau data yang disembunyikan harus tahan terhadap manipulasi seperti apapun yang dilakukan terhadap mediannya. Jadi data tidak poleh rusak meskipun medianya dimenipulasi.
- Recovery
  Data yang disembunyikan harus dapat diekstraksi kembali dan tidak rusak sehingga pesan dapat tersampaikan.[1]



Gambar 1. Framework umum dari steganografi

Steganografi digunakan untuk data dengan jumlah yang besar dalam dunia digital khususnya internet. Format data yang paling popular yaitu .bmp, .doc, .gif, .jpeg, .mp3, .txt. dan wav. karena banyak digunakan di internet dan format data ini lebih mudah digunakan untuk steganografi dan data noise atau redundan dapat digantikan dengan pesan rahasia. Teknologi steganografi adalah bagian yang sangat penting dari masa depan keamanan Internet dan privasi pada sistem terbuka seperti Internet.

Penelitian mengenai steganografi ini terutama didorong oleh kurangnya kekuatan daRI sistem kriptografi sendiri dan keinginan untuk memiliki kerahasiaan sepenuhnya dalam lingkungan sistem terbuka.

Pada prakteknya ada tiga metode dasar yang digunakan dalam steganografi :

- Pure Steganography
  Pure Steganography didefinisikan sebagai system steganografi yang tidak membutuhkan pertukaran stego-key atau kunci untuk menyisispkan pesan dalam media. Metode ini adalah metode yang paling tidak aman yang hanya dimaksudkan untuk berkomunikasi secara rahasia karena pengirim dan penerima dapat mengandalkan asumsi bahwa tidak ada pihak lain yang sadar akan pesan rahasia tersebut. Dengan menggunakan sistem terbuka seperti internet kita mengetahui bahwa kenyataan tidak seindah itu karena banyak pihak lain yang mungkin saja menyadap atau meyadari bahwa pesan yang dikirim adalah pesan rahasia.

- Secret Key Steganography
  Secret Key Steganography didefinisikan sebagai sistem steganografi yang membutuhkan pertukaran kunci rahasia (stego-key) sebelum komunikasi. Secret Key Steganography mengambil media dan menyembunyikan pesan rahasia di dalamnya dengan menggunakan
  kunci rahasia (stego-key). Hanya pihak-pihak yang mengetahui kunci rahasia dapat membalikkan proses dan
  membaca pesan rahasia. Tidak seperti Pure steganography dimana terdapat saluran komunikasi tak kasat mata yang dirasakan hadir, Secret Key steganography melakukan pertukaran suatu stego-key, yang membuatnya lebih rentan terhadap intersepsi. Akan tetapi bahkan jika terintersepsi, hanya pihak yang mengetahui kunci rahasia saja yang dapat mengambil pesan rahasia.

- Public Key Steganography
  Public Key steganografi mengambil konsep dari Kriptografi Kunci Publik dimana pada steganografi ini menggunakan kunci publik dan sebuah kunci pribadi untuk mengamankan komunikasi antara pihak-pihak yang akan berkomunikasi secara rahasia. Pengirim akan menggunakan kunci publik selama proses encoding dan hanya kunci pribadi, yang memiliki hubungan matematis langsung dengan kunci public yang dapat digunakan untuk memecahkan pesan rahasia. Public Key steganografi menyediakan cara yang lebih kuat untuk mengimplementasikan sistem steganografi karena dapat memanfaatkan teknologi yang jauh lebih kuat dari yang digunakan pada Kriptografi Kunci Publik. Public Key steganografi juga memiliki beberapa tingkat keamanan di pihak-pihak yang tidak diinginkan pertama harus berurusan dengan perkiraan penggunaan steganografi dan kemudian mereka akan harus menemukan cara untuk memecahkan algoritma yang digunakan oleh sistem kunci publik sebelum mereka bisa mengintersepsi pesan rahasia.[2]

Berikut akan dijelaskan mengenai steganografi pada masing-masing media.

2.1 Steganografi pada media teks

Rahasia penyandian pesan dalam teks dapat tugas yang sangat menantang. Ini karena file teks memiliki sangat sedikit data yang redundan untuk diganti dengan pesan rahasia. Kekurangan lainnya adalah kemudahan untuk

mengubah steganografi berbasis teks sehingga dapat diubah oleh pihak yang tidak diinginkan dengan hanya mengubah teks itu sendiri atau reformatting teks ke bentuk lain (dari. TXT ke. PDF,dll). Ada banyak metode yang digunakan untuk steganografi berbasis teks. Beberapa metode tersebut adalah seperti yang akan dijelaskan di bawah ini.

Line-shift encoding melibatkan pergeseran sebenarnya dari setiap baris teks secara vertikal ke atas atau ke bawah oleh sesedikitnya 3 cm. Tergantung pada apakah jalur ini naik atau turun dari garis stasioner maka akan sama dengan nilai yang akan atau dapat dikodekan menjadi pesan rahasia.

Word-shift encoding bekerja dalam banyak cara yang sama seperti cara line-shift encoding bekerja, hanya yang digunakan pada metode ini adalah ruang(spasi) horisontal di antara kata-kata untuk menyamakan nilai untuk pesan tersembunyi. Metode pengkodean ini lebih tidak terlihat daripada line-shift encoding tetapi mensyaratkan bahwa format teks mendukung variabel *spacing*. Fitur khusus pengkodean melibatkan pengkodean pesan rahasia ke dalam teks berformat dengan mengubah atribut teks tertentu seperti vertikal / horisontal panjang huruf seperti b, d, T, dll. Ini adalah metode pengkodean teks paling sulit untuk mengitersepsi setiap jenis teks berformat memiliki sejumlah besar fitur yang dapat digunakan untuk pengkodean pesan rahasia.

Ketiga metode pengkodean berbasis teks memerlukan baik file asli atau pengetahuan tentang format file asli untuk dapat mengekstraksi pesan rahasia.

2.2 Steganografi pada media image

Menyembunyikan pesan rahasia dalam gambar digital adalah media yang paling banyak digunakan dari semua metode dalam dunia digital saat ini. Hal ini karena dengan media image maka dapat mengambil keuntungan dari daya terbatas dari sistem visual manusia (HVS). Hampir semua teks biasa, sandi teks, gambar, dan lainnya dapat dikodekan menjadi aliran bit dapat disembunyikan dalam gambar digital. Dengan pertumbuhan yang berkelanjutan dari kekuatan grafik dalam dunia komputer dan penelitian image steganografi, bidang ini akan terus tumbuh pada kecepatan yang sangat cepat.

Bagi computer image adalah *array of numbers* yang menyatakan intensitas cahaya pada berbagai titik atau pixel. Ketika berhadapan dengan gambar digital untuk digunakan dengan steganography, 8-bit dan 24-bit per pixel file gambar biasanya khas. Keduanya memiliki kelebihan dan kekurangan, gambar 8-bit adalah format yang baik untuk menggunakan karena ukurannya yang relatif kecil. Kekurangannya adalah bahwa hanya 256 warna yang mungkin dapat digunakan yang dapat menjadi masalah potensial dalam pengkodean. Biasanya palet warna grayscale yang digunakan ketika berhadapan dengan gambar 8-bit seperti (. GIF) karena perubahan warna secara bertahap akan lebih sulit untuk dideteksi setelah gambar disisipkan dengan pesan rahasia. Gambar 24-bit memberikan lebih banyak fleksibilitas ketika digunakan untuk steganography. Jumlah warna yang besar (lebih dari 16 juta) yang dapat digunakan melampaui sistem visual manusia (HVS), yang membuatnya sangat sulit sekali untuk mendeteksi pesan rahasia yang telah disisipkan. Manfaat lain yaitu bahwa jumlah pesan rahasia yang dapat disembunyikan jauh lebih besar dari pada pesan yang dapat disimpan dalam gambar 8-bit. Satu kekurangan utama untuk gambar digital 24-bit adalah ukurannya yang besar(biasanya dalam MB) membuat mereka lebih dicurigai daripada gambar 8-bit yang jauh lebih kecil ukurannya(biasanya dalam KB) ketika dikirim melalui sistem terbuka seperti Internet.

Solusi terbaik untuk mengatasi ukuran gambar 24-bit yang besar yaitu dengan mengkompresinya dengan teknik lossless karena teknik ini menjaga agar pesan rahasia tetap utuh saat gambar sudah dikompresi, akan tetapi kekurangannya yaitu ukuran gambar tidak banyak berkurang. Sedangkan teknik kompresi lossy sebaliknya yaitu, mengurangi ukuran gambar dalam jumlah cukup besar tetapi tidak menjamin keutuhan dari pesan rahasia. Oleh krena itu teknik kompresi lossless lah yang umum dipilih mengingat tujuan utama dari steganografi adalah menyampaikan pesan rahasia dalam media.

Berikut akan dibahas teknik-teknik steganografi pada image yang popular yaitu Least Significant Bit(LSB) dan teknik Masking and Filtering. LSB adalah teknik yang paling populer digunakan untuk gambar digital. Dengan menggunakan LSB dari setiap byte (8 bit) dalam sebuah gambar untuk pesan rahasia, kita dapat menyimpan 3 bit data dalam setiap pixel untuk 24-bit gambar dan 1 bit pada setiap pixel untuk 8-bit gambar. Seperti yang Anda lihat, lebih banyak informasi yang dapat disimpan dalam gambar 24-bit. Tergantung pada palet warna yang digunakan untuk gambar sampul (yaitu, semua abu-abu), mungkin untuk mengambil 2 LSB's dari satu byte tanpa dapat dibedakan oleh sistem visual manusia (HVS). Satu-satunya masalah dengan teknik ini adalah bahwa teknik ini sangat rentan terhadap serangan seperti perubahan dan format terhadap gambar(contohnya, merubah dari. GIF ke. JPEG).

Teknik Masking dan Filtering steganografi pada gambar digital mirip seperti Digital Watermarking yang lebih populer dengan teknik kompresi lossy seperti (. JPEG). Teknik ini sebenarnya memperbesar sebuah data gambar dengan menyembunyikan data rahasia atas data asli yang bertentangan dengan menyembunyikan informasi bagian dalam data. Beberapa ahli berpendapat bahwa ini jelas merupakan suatu bentuk penyembunyian informasi, tetapi tidak secara teknis merupakan steganografi. Kelebihan teknik Masking and Filtering bahwa mereka kebal terhadap manipulasi gambar yang membuatnya sangat

kuat(*robust).* Ada banyak teknik lainnya yang tidak dibahas dalam makalah ini yang dapat berkrmbang menjadi teknik yang lebih bagus dari kedua teknik ini.

2.3 Steganografi pada media audio

Penyandian pesan rahasia dalam audio adalah teknik yang paling menantang untuk digunakan saat berurusan dengan steganografi. Hal ini karena sistem pendengaran manusia (HAS) memiliki rentang dinamis yang dapat mendengarkan sehingga membuat manusia menjadi sangat peka terhadap perubahan suara sehingga sulit untuk menyisipkan pesan dalam media audio tanpa diketahui pendengarnya. Satu-satunya kelemahan dalam (HAS) yaitu ketika berusaha membedakan suara (suara keras menghanyutkan suara yang lemah) dan ini adalah hal yang harus dieksploitasi untuk mengkodekan pesan rahasia dalam media audio tanpa terdeteksi. Ada dua konsep untuk dipertimbangkan sebelum memilih teknik steganografi audio, yaitu format digital audio dan media transmisi audio. Ada tiga format audio digital biasanya digunakan yaitu Sample Quantization, Temporal Sampling Rate dan Perceptual Sampling.

Sample Quantization yang merupakan 16-bit arsitektur sampling linier yang digunakan oleh format audio populer seperti (. WAV dan. AIFF). Temporal Sampling Rate menggunakan frekuensi yang dapat dipilih(dalam KHz) untuk sampel audio. Umumnya, semakin tinggi sampling rate, semakin banyak ruang data yang dapat digunakan. Format Perceptual Sampling merubah statistik audio secara drastis dengan hanya mengkodekan bagian yang dirasakan pendengar, dengan demikian mempertahankan suara tetapi mengubah sinyal. Format ini digunakan oleh audio digital yang paling popular di Internet saat ini yaitu ISO MPEG (MP3).

Medium transmisi (path audio yang diambil dari pengirim ke penerima) juga harus dipertimbangkan ketika melakukan steganografi audio. W. Bender [8] memperkenalkan empat kemungkinan media transmisi:

- Digital end to end - dari mesin ke mesin tanpa modifikasi.
- Peningkatan / penurunan resampling - tingkat sampel diubah tetapi tetap digital.
- Analog dan resampled - diubah menjadi sinyal analog dan resampled di tingkat yang berbeda.
- Over the air - sinyal ditransmisikan ke dalam frekuensi radio dan resampled dari mikrofon.

Berikut akan dibahas tiga metode steganografi audio yang populer, pertama yaitu Echo data hiding menggunakan gema dari file audio untuk menyembunyikan informasi. Dengan menambahkan suara ekstra kepada gema di dalam file audio, informasi dapat tersembunyi dengan baik karena metode ini dapat meningkatkan suara dari audio di dalam file audio.

Low-bit encoding menyisipkan pesan rahasia ke dalam least significant bit (LSB) dari file audio. Kapasitas saluran 1kb per detik per Kilohertz (44 kbps untuk 44 KHz sampel urutan). Metode ini mudah untuk menggabungkan tetapi sangat rentan terhadap kehilangan data akibat kebisingan saluran dan resampling.

Phase encoding menggantikan fase awal segmen audio dengan fase referensi yang mewakili data yang tersembunyi. Hal ini dapat dianggap sebagai semacam enkripsi untuk sinyal audio dengan menggunakan apa yang dikenal sebagai Diskrit Fourier Transform (DFT), yang tidak lebih dari algoritma transformasi untuk sinyal audio.

Spread spectrum mengkodekan audio selama hampir seluruh spektrum frekuensi. Kemudian akan mengirimkan audio di frekuensi yang berbeda sehingga akan bervariasi, tergantung pada metode spektrum yang digunakan. Direct Sequence Spread Spectrum (DSSS) adalah salah satu metode yang menyebarkan sinyal dengan mengalikan sinyal sumber oleh beberapa urutan acak semu yang dikenal sebagai(CHIP). Laju sampling ini kemudian digunakan sebagai laju chip untuk mengkomunikasikan sinyal audio. Teknik pengkodean Spread spectrum merupakan sarana yang paling aman digunakan untuk mengirim pesan tersembunyi dalam audio, namun dapat memperkenalkan suara acak ke audio dengan demikian menciptakan kesempatan adanya kehilangan data.

2.4 Steganografi pada media video

Steganografi pada video tidak kalah menantang dengan steganografi pada audio karena video merupakan gabungan dari image dan audio sehingga dalam steganografi video kita harus memperhatikan kedua aspek tersebut agar tidak terdeteksi oleh pihak lain dalam menyemunyikan pesan rahasia di dalamnya. Pada umumnya metode yang digunakan untuk metode DCT(Discrete Cosine Transform). Cara kerja DCT yaitu dengan sedikit mengganti setiap gambar dalam video, hanya sebanyak sampai tidak dapat dideteksi oleh mata manusia(HVS). DCT merubah nilai dari bagian tertentu dari image, dan biasanya membulatkannya ke atas. Steganografi pada video mirip dengan steganografi pada image, selain informasi rahasia pda video disembunyikan dalam setiap frame dari video. Bila pesan rahasia yang disembunyikan hanya sedikit jumlahnya, video hasil steganografi pada umumnya tidak akan terdeteksi, tetapi semakin besar pesan yang disisipkan maka semakin dapat terdeteksi.

Video yang sudah disisipi pesan rahasia pasti tidak sama dengan video aslinya dan mengalami penurunan

kualitas. Kualitas dari video steganografi dapat ditentukan berdasarkan beberapa faktor :

- Mean Square Error (RMSE)
  MSE adalah parameter yang digunakan untuk menentukan tingkat kesalahan pada image-stego.

$$MSE = \frac{1}{N}\sum_{n}\left|y(n) - x(n)\right|^2 \qquad (1)$$

- Peak Signal to Noise Ratio(PSNR)
  PSNR adalah nilai yang menyatakan tingkat noise atas citra yang telah disisipi pesan.

$$PSNR = 20 \cdot \log_{10}\left(\frac{225}{RMSE}\right) \qquad (2)$$

- Mean Opinion Score (MOS)
  Faktor ini merupakan faktor penilaian kualitas secara subjektif berdasarkan criteria sebagai berikut.[5]

Tabel 1 Kriteria penilaian subjektif terhadap Steganografi Video

Nilai	Level Distorsi	Kualitas Video
1	Sangat mengganggu (*Very annoying*)	*video* memiliki kualitas yang sangat rendah, sehingga tidak dapat dilihat lagi
2	Mengganggu (*Annoying*)	*video* memiliki kualitas yang sangat rendah, tetapi masih dapat dilihat. Keberadaan interferensi benar-benar mengganggu
3	Agak mengganggu (*Slightly annoying*)	*video* memiliki kualitas yang rendah sehingga diinginkan dapat diperbaiki dan interferensi terasa cukup mengganggu.
4	*Perceptible but not annoying*	*video* memiliki kualitas yang bagus namun masih ada sedikit noise yang masih mengganggu
5	*Imperceptible*	*video* memiliki kualitas yang bagus, enak dilihat dan interferensi noise belum terasa mengganggu

3. STEGANALISIS

Steganalisis adalah ilmu yang mempelajari karakteristik penyembunyian suatu data pada media (steganografi) dan bagaimana cara untuk mendeteksi bahkan sampai membongkar data tersembunyi tersebut. Steganalisis sangat sulit sekali diterapkan. Secara teoritis memang mudah menerapkan steganalisis, tetapi pada kenyataannya sangat sulit untuk diterapkan.

Steganografi adalah ilmu untuk menyisipkan suatu data pada sebuah media. Apapun metode yang anda gunakan, atau sehebat apapun metode yang digunakan, pasti akan mempunyai jejak statistika penyisipannya. Jika dianalogikan, seperti kita memasukan benda asing (anggap **y**) ke dalam suatu benda asli (anggap **x**), akan membuat suatu perubahan pada benda asli (**x**), baik perubahan itu kasat mata atau tidak kasat mata. Anggap hasil perubahan benda asli sebagai benda **z**, jadi kalu dirumuskan secara matematis, kita dapat menyatakan **z = x + y.**

Hal inilah yang menjadi dasar dari ilmu steganalisis. Steganalysis tidak berurusan dengan mencoba untuk mendekripsi informasi tersembunyi dalam sebuah file, hanya menemukan nya. Bagaimana cara untuk mendeteksi perubahan yang terjadi. Ada banyak metode yang dapat digunakan untuk mendeteksi hal ini. Pada umumnya ita dapat mendeteksi pesan rahasia dengan membendingkan media tersangka dengan media yang asli, apabila terdapat perbedaan maka mungkin saja terdapat pesan rahasia di dalamnbya. Seperti halnya steganografi, metode yang digunakan sangat tergantung dari media yang akan dideteksi. Metode untuk masing-masing media akan dibahas lebih spesifik di bagian berikutnya, akan tetapi metode global yang digunakan untuk steganalisis adalah sebagai berikut:

- Membersihkan noise pada media (de-Noising)
- Mengekstraksi feature-feature yang ada
- Klasifikasi berhasilkan feature-feature tersebut
- Decission

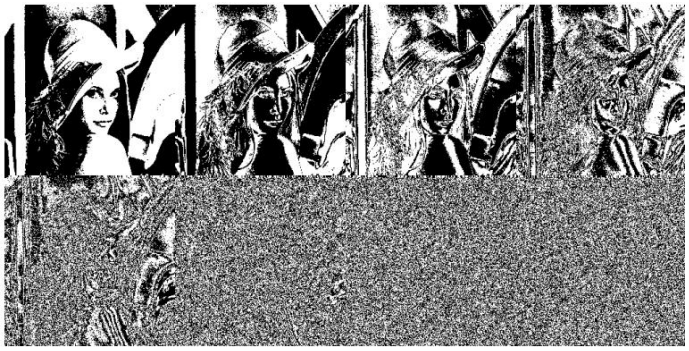
3.1 Steganalisis pada media teks

Informasi dapat disembunyikan di dalam teks-teks sedemikian rupa sehingga kehadiran pesan hanya dapat dideteksi dengan pengetahuan tentangn kunci rahasia, misalnya bila menggunakan metode yang disebutkan sebelumnya menggunakan sebuah buku yang tersedia untuk umum dan kombinasi posisi karakter untuk menyembunyikan pesan, sebagian besar teknik-teknik yang melibatkan perubahan-perubahan pada media tersangka dengan media aslinya. Perubahan ini dapat dideteksi dengan mencari pola dalam teks atau *disturbings* daripadanya, penggunaan bahasa yang aneh dan tidak biasa dalam jumlah spasi. Sehingga apabila ukuran dua buah file teks atau dokumen yang tampak sama persis berbeda maka mungkin saja terdapat pesan rahasia di dalamnya dengan adanya penambahan spasi atau tab.

3.2 Steganalisis pada media image

Meskipun gambar dapat dipindai properti yang mencurigakan dalam cara yang sangat dasar, mendeteksi pesan tersembunyi biasanya membutuhkan pendekatan yang lebih teknis. Perubahan dalam ukuran, format file, terakhir diubah timestamp dan di palet warna mungkin menunjukkan adanya pesan tersembunyi, tetapi hal ini tidak akan selalu menjadi kasus. Teknik yang digunakan secara luas untuk pemindaian gambar melibatkan analisis statistik. Kebanyakan algoritma steganografi yang bekerja pada gambar, berasumsi bahwa least sigifikan bit lebih banyak digunakan atau mungkin metode acak. Namun ini adalah asumsi yang salah. Sementara LSB mungkin tidak tampak begitu penting, menerapkan filter yang hanya menunjukkan least signifikan bit(LSB), akan tetap menghasilkan gambar yang dapat dikenali. Dengan demikian, dapat disimpulkan bahwa LSB tidak acak sama sekali, tapi sebenarnya berisi informasi tentang seluruh gambar.

Ketika memasukkan pesan tersembunyi dalam sebuah gambar,properti ini berubah. Terutama data yang terenkripsi, yang memiliki entropi sangat tinggi, maka media gambar LSB akan tidak lagi berisi informasi yang asli, tetapi karena modifikasi mereka sekarang akan acak. Dengan analisis statistik pada LSB, perbedaan antara nilai-nilai acak dan nilai image yang sebenarnya dapat dengan mudah dideteksi. Dengan menggunakan teknik ini, juga memungkinkan untuk mendeteksi pesan tersembunyi di dalam file JPEG dengan metode DCT, karena ini juga melibatkan modifikasi LSB, meskipun ini terjadi dalam frekuensi domain.[3]



Gambar 2. Image yang disisipi pesan dengan metode LSB

3.3 Steganalisis pada media audio

Metode analisis statistik dapat digunakan untuk melawan file audio juga, karena teknik modifikasi LSB dapat digunakan pada suara juga. Akan tetapi, ada beberapa hal yang dapat dideteksi. Frekuensi yang tinggi dan tidak terdengar dapat discan untuk informasi dan distorsi atau pola-pola aneh dalam suara mungkin menunjukkan adanya suatu pesan rahasia. Juga, perbedaan pada pitch, suara gema atau latar belakang dapat menimbulkan kecurigaan.[2]

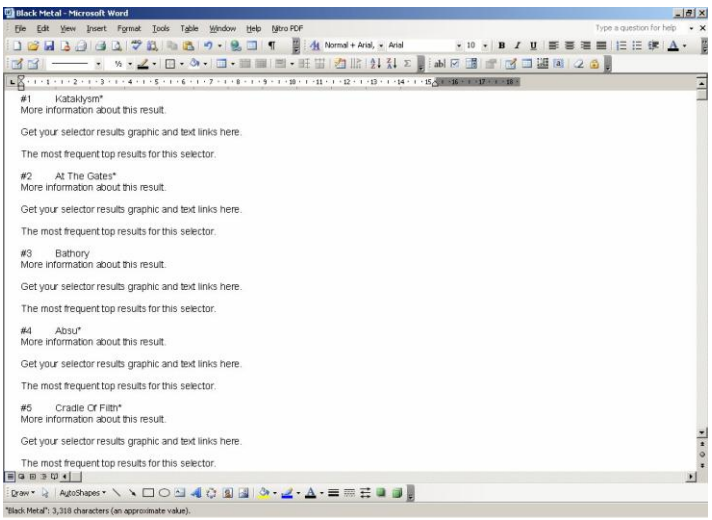
3.4 Steganalisis pada media video

Steganografi pada media video pada dasarnya merupakan gabungan dari steganografi image dan audio sehingga metode pendeteksian informasi tersembunyi juga kombinasi teknik yang digunakan untuk image dan audio. Namun, ada teknik steganographic yang berbeda dapat digunakan terutama akan sangat efektif bila digunakan dalam file video. Penggunaan kode khusus , tanda-tanda atau isyarat sangat sulit untuk mendeteksi dengan sistem komputer. Metode ini digunakan dalam perang Vietnam, jadi tawanan perang bisa mengkomunikasikan pesan rahasia melalui media video yang prajurit musuh dibuat untuk mengirim ke garis depan.[4]

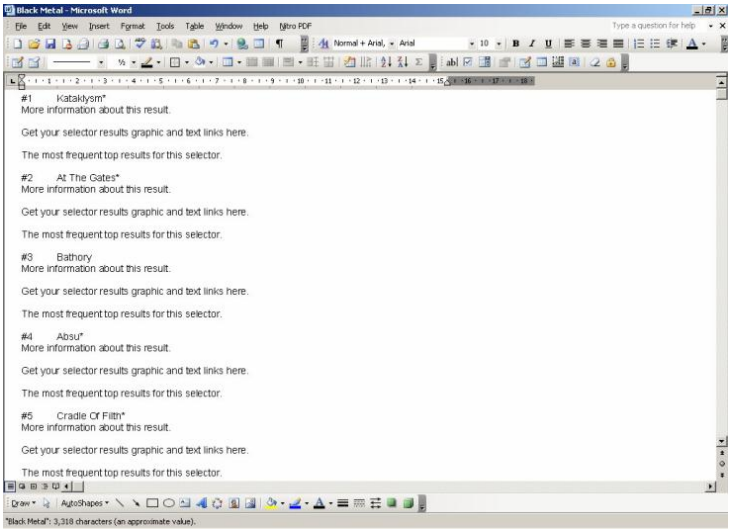
4. ANALISIS

Berdasarkan pembahasan mengenai metode steganografi pada media teks, image, audio dan video yang telah dibahas di atas, maka kini dapat dibandingkan di antara keempat media tersebut untuk menemukan media yang terbaik untuk digunakan menyimpan pesan rahasia menggunakan teknik-teknik steganografi.

Pada media teks, media yang asli dan media yang sudah disisipi pesan tidak dapat dibedakan dengan hanya melihatnya karena keterbatasan HVS. Berikut adalah contoh teks yang digunakan sebagai media steganografi dengan menggunakan software SNOW.



Gambar 3. Media teks sebelum disisipi pesan rahasia

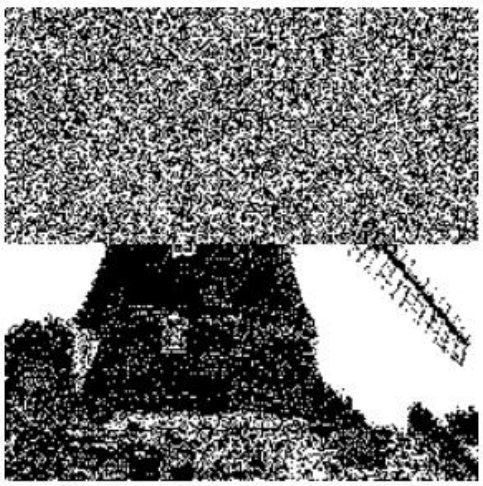


Gambar 4. Media teks setelah disisipi pesan rahasia

Dapat dilihat bahwa kita tidak dapat melihat perbedaan antar kedua gambar tersebut. Sehingga sulit untuk diketahui apakah pada teks tersebut terdapat pesan rahasia atau tidak. Akan tetapi apabila media teks tersebut berbentuk teks yang masih dapat diedit maka kita dapat mengetahui apakah ada spasi atau tab berlrbih yang menunjukkan bahwa file teks tersebut telah disisipi pesan yaitu dengan memblok semua teks tersebut dan kita dapat melihat apakah ada tab atau spasi yang berlebih. Tetapi bila file teks tidak dapat diedit dan hanya dapat dilihat saja maka akan sangat sulit untuk mengetahui apakah ada pesan tersembunyi atau tidak.

Pada media image kita pun tidak dapat membedakan image asli dengan image yang sudah disisipi pesan karena keterbatasan HVS sehingga apabila dilihat tanpa dilakukan usaha yang lain. Image tidak dapat dibedakan. Akan tetapi bila kita menggunakan metode steganalisis seperti yang sudah dijelaskan di atas maka kita dapat mengetahui perbedaan antara image yang asli dengan image yang sudah disisipi pesan. Berikut adalah image yang hanya menampilkan LSB /enhanced LSB.

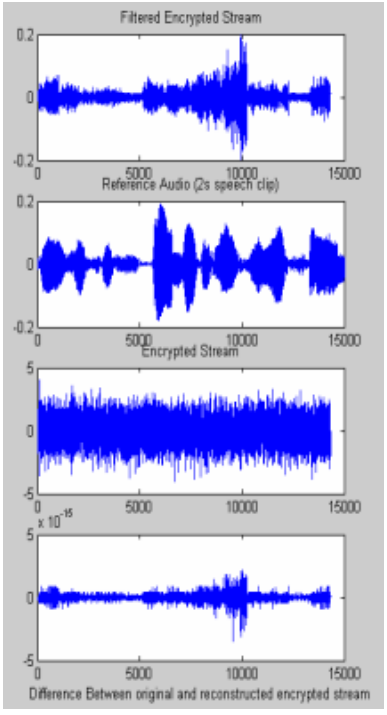
Gambar 5. Gambar tanpa pesan rahasia



Gambar 6. Gambar dengan pesan rahasia

Dari gambar di atas bahwa Gambar 6. Merupakan gambar yang 50% dai gambar tersebut digunakan untuk menyimpan pesan rahasia.

Untuk media audio kita dapat menggunakan indera manusia untuk mengetahui adanya perbedaan antara file audio yang asli dengan file audio yang sudah disisipi pesan karena indera pendengar manusia(HAS) sangatlah peka terhadap suara, meskipun digunakan teknik echo data hiding, kita masih dapat membedakannya dengan file audio yang asli meskipun agak sulit. Untuk itu dapat digunakan data statistic dari file audio yang telah disaring untuk mengetahui keberadaan dari pesan rahasia dalam file audio tersebut. Berikut adalah perbandingan data statistic dari file audioyang sudah disaringberisi suara seseorang yang berpidato singkat.



Gambar 5. Perbandingan statistic dari file audio

Gambar di atas terdiri dari tiga statistic file audio, gambar yang paling atas yaitu audio stream yang mengandung pesan rahasia yang sudah disaring. Berikutnya adalah gambar audio stream dari file audio aslinya, gambar ketiga adalah audio stream yang mengandung pesan rahasia yang belum disaring. Dan gambar terakhir adalah perbedaan antara audio stream file asli dengan file yang sudah disisipi pesan.

Untuk media videomerupakan media yang paling rentan diketahui bahwa ada pesan rahasia tersembunyi di dalam media ini karena video merupakan gabungan dari image dan audio sehingga seperti sudah dibahas di atas bahwa HAS peka terhadap suara dan mata manusia kurang peka terhadap perubahan bit dari gambar akan tetapi video menampilkan gambar (frame-frame) yang berganti-ganti terus, sehingga akan lebih mudah untuk diketahui bahwa ada pesan rahasia yang terkandung di dalamnya. Karena kualitas dari video pasti berkurang tergantung dari metode steganografinya dan besarnya data yang disisipkan.

Untuk kekuatan masing-masing media terhadap serangan, pada umumnya relative sama karena untuk memecahkan file dengan pesan rahasia dibutuhkan kunci atau mungkin juga tanpa kunci tergantung dari metode steganografi yang dipilih, akan tetapi lebih baik bila digunakan metode public key steganography atau secret key steganography agar lebih aman dan sulit untuk dipecahkan.

Jadi menurut analisis untuk masing masing media di atas dapat diambil kesimpulan bahwa media yang paling baik untuk dteganografi adalah media teks dan image. Karena perbedaan antara file yang asli denga file yang sudah disisipi pesan tidak dapat dilihat dengan mata telanjang begitu saja, harus dilakukan usaha lebih untuk mengetahui apakah ada pesan tersembunyi atau tidak, sehingga tidak akan menimbulkan rasa curiga bagi orang yang hanya melihatnya saja tanpa maksud untuk mencari pesan tersembunyi.

5. KESIMPULAN

Dalam dunia yanga telah modern dan jaman globalisasi ini kerahasiaan pesan, keamanan dari informasi menjadi isu yang penting. Steganografi, khususnya dikombinasikan dengan kriptografi, adalah alat yang ampuh yang memungkinkan orang untuk berkomunikasi tanpa penyadap atau pihak lain yang tidak diinginkan bahkan mungkin pihak lain tidak mengetahui adanya suatu bentuk komunikasi dari pertama. Metode yang digunakan dalam ilmu steganografi telah mengalami banyak kemajuan selama berabad-abad, terutama dengan bangkitnya era komputer dan dunia digital Meskipun teknik steganografi masih belum sering digunakan, kemungkinannya dan metode-metodenya tidak terbatas. Banyak teknik yang berbeda dan terus dikembangkan, sementara cara mendeteksi pesan tersembunyi (steganalisis) juga maju dengan cepat. Walaupun pendeteksian tidak pernah memberikan jaminan akan menemukan semua informasi yang tersembunyi, akan tetapi dapat digunakan bersama dengan metode pemecahan steganografi, untuk meminimalkan kemungkinan komunikasi tersembunyi berlangsung. Bahkan kemudian, steganography sempurna, di mana kunci rahasia hanya akan menunjukkan bagian-bagian dari sebuah media yang membentuk pesan rahasia, tidak akan terdeteksi, karena media tidak berisi informasi tentang pesan rahasia sama sekali.

Dalam waktu dekat, penggunaan steganografi yang paling penting terletak pada bidang Watermarking. Steganography mungkin juga menjadi terbatas di bawah undang-undang, karena pemerintah sudah mengklaim bahwa penjahat menggunakan teknik ini untuk berkomunikasi (terorisme).

Dari penelitian dan pembahasan mengenai teknik dan media steganografi setidaknya kita dapat memahami steganografi dan mencegah bahkan mendeteksi penggunaan steganografi untuk tujuan yang buruk.

Bedasarkan hasil penelitian yang telah dijelaskan di atas dapat diketahui bahwa dalam steganalisis kita memerlukan suatu media pembanding yaitu media asli yang belum disisipi pesan untu mengetahui perbedaannya karena tanpa media pembanding media dengan pesan tersembunyi pun akan tampak seperti file media biasa khususnya untuk media teks dan image yang tidak dapat dibedakan atau disadar oleh mata. Untuk setiap media berlaku bahwa semakin banyak data yang disisipkan dalam media tersebut maka kualitas media akan semakin berbeda jauh dari aslinya sehingga tidak lagi sesuai dengan prinsip fidelity dan semakin mudah untuk dideteksi keberadaan pesan rahasia di dalamnya.

Media steganografi yang terbaik digunakan yaitu teks dan image (grayscale dan digital camera) karena kedua media ini tidak diketahui perbedaannya dengan yang asli meskipun sudah disisipi dengan pesan rahasia apabila dilihat dengan mata manusia karena keterbatasan HVS. Dan untuk memperkecil kemungkinan pesan dapat terdeteksi oleh pihak yang tidak diinginkan maka data asli dari media yang digunakan sebaiknya dihapus dan jangan sampai beredar atau sampai ke tangan orang lain sehingga tidak ada media pembanding yang dapat digunakan.

Meskipun pesan rahasia pada teks dan image sebenarnya dapat dideteksi dengan metode yang telah dijelaskan sebelumnya, tetapi tujuan dari steganografi adalah untuk menyembunyikan pesan, maka bila sejak awal orang yang melihat media steganografi bahkan tidak meyadari adanya perubahan atau keanehan pada media itu maka, dia pun tidak akan bersusah payah untuk mendeteksi lebih lanjut atau bahkan mencoba memecahkannya.

REFERENSI

[1] Ir. Rinaldi Munir, M.T., "Diktat Kuliah IF3058 Kriptografi", Departemen Teknik Informatika ITB, 2005, halaman 50-63.

[2] http://www.jjtc.com/pub/ihw98a.htm

[3] http://web.njit.edu/~shi/Steganalysis/steg.htm

[4] N. Provosand, P. Honeyman. "Hide and Seek : An Introduction to Steganography", IEEE Security & Privacy, Pages 32-44, 2003.

[5] Hany Farid, "Detecting Steganographic Messages in Digital Images",Technica lReport TR2001-412, Deparment of Computer Science,Dartmouth College, August2001.

[6] http://www.strangehorizons.com/ 2001/20011008/steganography.shtml