Meningkatkan Kapasistas Pesan yang disisipkan dengan Metode Redundant Pattern Encoding

Erdiansyah Fajar Nugraha/13508055[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung40132, Indonesia
[1]if18055@students.if.itb.ac.id

Steganografi adalah ilmu dan seni dalam menulis pesan yang tersembunyi atau menyembunyikan pesan dengan suatu cara tertentu sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui bahwa ada suatu pesan rahasia. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan suatu pesan tersembunyi atau informasi.

Ada beberapa metode penyembunyian pesan dalam steganografi yaitu Least Significant Bit Insertion (LSB), Algorithms and Transformation, Redundant Pattern Encoding, dan Spread Spectrum method.

Dalam makalah ini akan dibahas lebih mendalam tentang metode steganografi yaitu redundant pattern encoding, dan bagaimana meningkatkan kapasitas pesan yang dapat disisipkan dengan metode tersebut.

Kata Kunci : Steganografi, metode Redundant Pattern Encoding.

I. PENDAHULUAN

Steganografi adalah ilmu dan seni dalam menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara tertentu sehingga selain si pengirim dan si penerima tidak ada seorangpun yang menyadari adanya pesan tersembunyi.

Ada beberapa metode steganografi antara lain Least Significant Bit Insertion (LSB), Algorithms and Transformation, Redundant Pattern Encoding dan Spread Spectrum Method. Masing-masing metode memiliki kelebihan dan kekurangan.

Kekurangan Least Significant Bit Insertion (LSB) dari contoh 8 bit pixel yang menggunakan teknik LSB maka dapat secara drastis mengubah unsur pokok dari warna dari pixel. Hal itu dapat menunjukkan perbedaan yang nyata dari cover image menjadi stego image, sehingga perbedaan tersebut dapat dinyataan sebagai keberadaan steganografi. Kelemahan lain dari metode LSB yaitu mudah diserang dalam pemrosesan image, seperti cropping dan compression. Namun metode LSB ini memiliki keuntugan yaitu cepat dan mudah, serta sudah ada aplikasi yang mendukung.

Untuk metode Spread Spectrum, kelemahan dari metode ini hamper sama dengan metode LSB yaitu lemah terhadap serangan yaitu terhadap cropping dan kompresi.

Untuk metode Redundant Pattern Encoding, metode ini memiliki kelebihan yaitu bertahan terhadap cropping namun kerugiannya yaitu tidak dapat menggambar pesan yang lebih besar.

Ada beberapa teknik steganografi antara lain Physical steganografi, Digital steganografi, Network steganografi, Printed steganografi, Text steganografi, dan Steganografi menggunakan sudoku puzzle.

Physical steganografi beberapa contoh dari teknik ini antara lain pada perang dunia ke 2, Prancis mengirimkan pesan melalui kurir dengan menuliskannya pada punggung kurir tersebut dengan tinta tidak terlihat, contoh lainnya pesan ditulis pada amplop yang di bagian yang tertutupi perangko.

Digital steganografi, adalah teknik steganografi modern, teknik muncul saat komputer muncul, perkembangan teknik ini lambat pada awalnya seiring perkembangan teknologi pada komputer. Contoh dari teknik steganografi ini yaitu metode-metode yang sudah kita kenal sekarang yaitu Lesat Significant Bit Insertion, Algorithms and Transformation, Redundant Pattern Encoding dan Spread Spectrum Method.

Network Steganografi, teknik ini menggunakan media digital seperti gambar, video, dan suara sebagai cover message untuk data yang akan disembunyikan, menggunakan control protocol elemen dasar dan dasar funsionalitas dari protocol tersebut. Contoh steganografi dengan teknik ini ada dua antara lain Steganophone dan WLan steganografi. Steganophone adalah teknik steganografi yaitu menyembunyikan pesan pada header file yang tidak digunakan. WLan steganografi adalah teknik steganografi yang digunakan pada jaringan WLan untuk menyembunyikan data atau informasi yang dikirim pada jaringan WLan.

Printed Steganografi, pada teknik ini pesan di enkripsi dengan metode tradisional yang akan menghasilkan ciphertext kemudian cipher text tersebut barulah disisipkan covertext yang dimodifikasi sedemikian rupa agar tersisip dengan baik cipher text hasil enkripsi.

Text Steganografi, teknik ini dapat digunakan diberbagai media seperti text video, audio, gambar dan lain-lain. Teknik ini sangat sulit digunakan karena penuh denga redundancy pada file.

Steganografi dengan Puzzle sudoku, maksud dari teknik ini yaitu menggunakan key dari sudoku puzzle

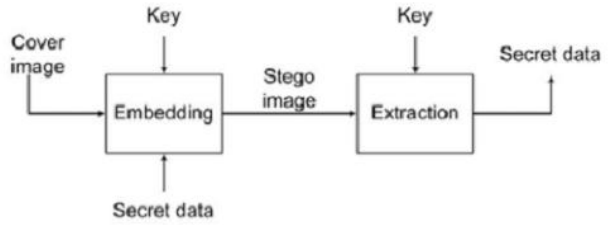
untuk menyisipkan informasi pada media gambar. Kunci yang digenerate dengan sudoku puzzle ini merupakan salah satu solusi dari sudoku puzzle, sudoku puzzle memiliki kemungkinan solusi sebanyak 6.71×10^{21}.

II. DIGITAL STEGANOGRAFI

Dalam steganografi ada dua property utama yang dibutuhkan yaitu media penampung pesan yang disisipkan dan pesan atau data rahasia yang akan disisipkan.

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 dimanipulasi.
- Recovery
  Data yang disembunyikan harus dapat diekstraksi kembali dan tidak rusak sehingga pesan dapat tersampaikan.



Gambar 1Framework 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.

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 komputer, 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.Salah 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 karena 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).

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 menyembunyikan 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.

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

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

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

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

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 dapa 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 sangat rendah sehingga diinginkan dapat diperbaiki dan interferensi cukup menggangu.
4	Perceptible but not annoying	Video memiliki kualitas yang bagus namun masih ada sedikit noise yang mengganggu
5	Imperceptible	Video memiliki kualitas yang bagus, enak dilihat, dan interferensi noise belum dirasa mengganggu.

III. REDUNDANT PATTERN ENCODING

Redundant Pattern Encoding merupakan salah satu metode penyisipan pesan pada teknik Digital Steganografi. Metode Redundant pattern encoding ini biasanya menggonakan media gambar sebagai cover dari pesan yang akan disembunyikan.

Kelebihan metode redundant pattern encoding ini yaitu tahan terhadap cropping dan compresi pada pemrosesan file gambar. Namun metode ini memiliki kekurangan yaitu ukuran file yang disisipkan terbatas

Penyisipan pesan pada metode Redundant pattern encoding adalah pesan akan disisipkan pada noise atau bagian yang kurang diperhatikan atau bagian yang tidak terlihat secara visual atau kasat mata pada file, seperti header file, dan noise pada gambar.

Karena penyisipan pesan dengan metode redundant patter encoding ini hanya dilakukan pada tempat yang terbatas tersebut maka kapasitas pesan yang disisipkan menjadi terbatas.

Untuk mengatasi hal tersebut dapat dilakukan beberapa cara sebagai berikut:

- Menggunakan banyak file yang memiliki hubungan tertentu misal sebuah album foto, atau kumpulan foto yang memiliki kategori yang sama, untuk ukuran pesan yang cukup besar. Dengan menggunakan banyak file maka dapat dipastikan header file yang digunakan sebagai tempat penyisipan pesan kapasitas nya lebih banyak. Namun dengan cara seperti ini si penerima pesan agak sulit untuk mendapatkan pesan yang dirahasiakan karena harus memikirkan atau mengurutkan tiap pesan yang terkandung dalam gambar hasil ekstraksi. Karena pada proses ekstraksi tidak dapat dipastikan bahwa urutan ekstraksi pesan pada gambar, belum tentu berurutan sesuai dengan pada saat proses penyisipan pesan yang dilakukan oleh si pengirim.
- Menggunakan file yang banyak memiliki noise, sehingga kapasitas pesan yang dapat disisipkan akan lebih besar dibanding pesan yang disisipkan pada file yang memiliki sedikit noise. Namun cara ini belum tentu baik mungkin dapat timbul kecurigaan pada proses distribusi image karena gambar yang dikirim tidak baik. Karena kekurangan tersebut maka image yang memiliki noise tinggi yang telah disisipi pesan tersembunyi, dapat disisipkan pada image lain yang memiliki noise kecil sehingga dapat mengurangi kemungkinan image tersebut dicurigai sebagai image yang memiliki pesan yang tersembunyi.
- Cara yang ketiga yaitu mengkombinasikan dua cara yang telah disebutkan sebelumnya yaitu dengan menggunakan banyak file yang termasuk dalam kategori yang sama atau kumpulan file tersebut merupakan sebuah album foto, file-file gambar yang memiliki noise yang tinggi yang telah disispkan pesan tersembunyi tersebut kemudian disisipkan pada file image yang memiliki noise kecil yang memiliki kategori yang sama atau maupun file gambar dalam satu album.

Berdasarkan tiga cara yang telah dijelaskan sebelumnya kapasitas pesan yang disisipkan dengan metode redundant pattern encoding dapat ditinggkatkan

IV. SIMPULAN

Dalam dunia yang 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.

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.

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 menyadari adanya perubahan atau keanehan pada media itu maka, dia pun tidak akan bersusah payah untuk mendeteksi lebih lanjut atau bahkan mencoba memecahkannya.

Metode redundant pattern encoding memiliki kelebihan yang diinginkan setiap orang yang akan menyisipkan pesan rahasia, namun memiliki keterbatasan yaitu kapasitas pesan yang disisipkan, cara cara yang telah dijelaskan sebelumnya memang belum sempurna atau munkin jauh dari sempurna, namun setidaknya dapat digunakan untuk meningkatkan kapasitas pesan yang dapat disisipkan dengan metode redundant pattern encoding.

REFERESI

Slide kuliah kriptrografi if3058

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

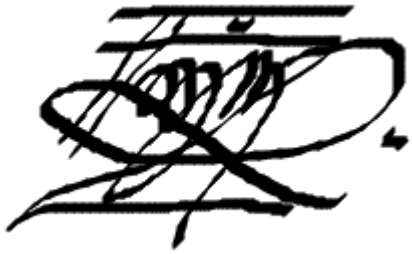
http://en.wikipedia.org/wiki/Steganography

http://id.wikipedia.org/wiki/Steganography

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23 Maret 2011



Erdiansyah Fajar Nugraha / 13508055