PENYISIPAN TEXT PADA GAMBAR MENGGUNAKAN STEGANOGRAFI

Jumiran[1], Aminul Fitri[2]
1,2 Dosen Sekolah STMIK Insan Pembangunan
Jl. Raya Serang Km. 10,5 Bitung, Tangerang
Telp. (021)59492836 Fax. (021) 59492837
E-mail : jumiran_jumjum@yahoo.com, aminul.gip1974@gmail.com,

ABSTRAK

Kebutuhan manusia pada umumnya adalah ingin memiliki rasa aman dan nyaman. Begitu pula halnya di dunia informasi yang pada saat ini bisa dibilang semuanya serba digital, salah satu solusi yang dapat dilakukan adalah dengan Steganografi yaitu tehnik dan seni menyembunyikan informasi dan data digital dibalik informasi digital lain. Dalam steganografi modern ada berbagai macam tehnik untuk menyembunyikan infomasi antara lain adalah Modifikasi Least Significant Bit (LSB), Metode Discrete Cosine Transform (DCT), Metode Red Green Blue Level (RGB). Untuk itu penulisan ini akan membahas tentang suatu aplikasi Steganografi untuk penyisipan informasi dengan menggunakan metode RGB, LSB dan DCT tersebut. Pengembangan aplikasi ini meliputi beberapa tahap, perancangan aplikasi, pembuatan program serta tahap implementasi program. Dalam pembuatan program, penulis menggunakan program Matlab. Aplikasi Steganografi ini dapat menyembunyikan suatu informasi atau pesan rahasia berupa teks ke dalam media gambar digital dengan menggunakan program Matlab, Aplikasi steganografi ini dapat digunakan untuk menghemat media penyimpanan, dan untuk menjaga keamanan informasi sehingga rasa aman dan nyawan dapat dirasakan oleh pengguna IT.
Kata kunci : Steganografi, Matlab, Metode RGB, LSB,DST,IT

1. Pendahuluan

Keamanan dalam dunia teknologi informasi sudah menjadi suatu keharusan. Dewasa ini persaingan diantara perusahaan yang bergerak didunia informasi sangat ketat serta kemajuan teknologi dibidang informasi sangat cepat . Perkembangan teknologi menjadi faktor yang sangat penting terhadap keberhasilan dan perkembangan perusahaan khususnya dibidang teknologi informasi, namun yang terpenting adalah mampu menciptakan rasa aman dan nyaman bagi para pengguna *IT*.

Kemajuan teknologi informasi sejalan dengan kemajuan sistem arsitektur dan pengorganisasian perangkat sistem informasi dalam hal ini sering kita gunakan media komputer untuk mendapatkan informasi secepat mungkin perlu adanya perangkat komputer yang mampu membantu kerja user dalam menyelesaikan masalah-masalah terkait data dan informasi. Dalam hal ini bagaimana data dan informasi tersebut tetap mampu dijaga keamanan dan kerahasiaannya.

Dalam perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi/data secara jarak jauh. Teknologi yang sering dipakai dalam jaringan komunikasi antara lain melaui internet. Bahkan berkembang seperti *facebook, twitter, massaging*, dan lain-lain. Dengan fasilitas tersebut mereka mampu berinteraksi dan saling bertukar informasi antar cabang, antar kota, antar wilayah, antar negara, bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan data dan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna seperti pelaku bisnis, perusahaan-perusahaan, departemen pertahanan, bahkan individu-individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya atau negara lain. Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah *Steganografy.*

Dalam *Steganografi* terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang

hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Sedangkan didalam aplikasinya dapat menggunakan beberapa teknik dan media, antara lain, text mampu disisipkam ke dalam suatu image/gambar, audio, dan lain-lain. Untuk itu penulis mencoba membahas terkait dengan *Steganografy* ini yaitu penyisipan text ke dalam image/gambar.

Ada beberapa alasan yang mendasari penulis mengangkat judul tersebut antara lain :

a) Adanya kebutuhan terhadap pesan rahasia yang disampaikan melalui median gambar sehingga tidak diketahui oleh orang
b) Untuk menyembunyikan suatu pesan dalam gambar secara acak sehingga tidak mudah untuk diketahui orang
c) Untuk bisa membandingkan dengan kondisi gambar yang tidak dapat menyisipkan gambar sehingga dapat dikategorikan sebuah pesan rahasia.
d) Adanya kebutuhan untuk memilih membuat suatu gambar yang dapat disisipin sebuah pesan yang dapat diterima dalam bentuk teks tersembunyi.

Dari beberapa alasan tersebut penulis mencoba untuk melakukan analisa kelebihan dan kekurangan dari metode *Steganografy* yang merupakan suatu komponen yang dapat membuat gambar dengan menyisipkan teks secara tersembunyi, yang kesemua itu mempunyai tujuan yang sama yaitu untuk menciptakan rasa aman dan nyaman bari para pengguna *IT*. Tujuan penulisan karya ilmiah ini antara lain :

a) Mengetahui sejarah perkembangan progam Matlab secara keseluruhan
b) Mengetahui keunggulan dan kelemahan dalam membuat pencitraan gambar digital
c) Mengetahui informasi dan perkembangan pemrograman Matlab terkini dan terbaru.
d) Membandingkan antara metode *Steganografy* dan *Kriptografy.*
e) Sebagai bahan materi atau referensi dalam perkembangan ilmu komputer mendatang
f) Sebagai tugas penyusunan artikel ilmiah mata kuliah “Tehnik Komputasi Terapan”

2. Landasan Teori

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied Cryptography", kriptografi adalah ilmu pengetahuan dan seni menjaga *message-message* agar tetap aman (secure). Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni :

a. Confidelity (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.

b. Data integrity (keutuhan data) yaitu layanan yang mampu mengenali / mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).

c. Authentication (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.

d. Non-repudiation (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

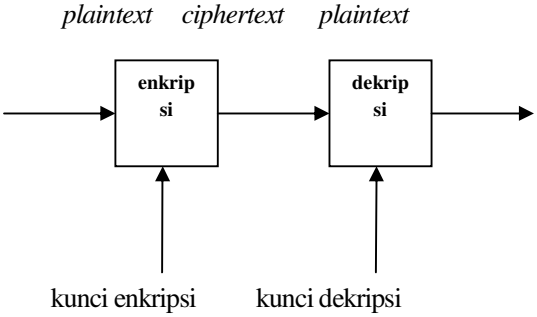
Berbeda dengan kriptografi klasik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan (yang artinya apabila algoritma yang digunakan telah diketahui maka

pesan sudah jelas "bocor" dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut), kriptografi modern lebih menitikberatkan pada kerahasiaan kunci yang digunakan pada algoritma tersebut (oleh pemakainya) sehingga algoritma tersebut dapat saja disebarkan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan bagi para pemakainya. Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi :

- *Plaintext* (M) adalah pesan yang hendak dikirimkan (berisi data asli).
- *Ciphertext* (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
- *Enkripsi* (fungsi E) adalah proses pengubahan *plaintext* menjadi *ciphertext*.
- *Dekripsi* (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.
- *Kunci* adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Seperti yang telah dijelaskan di atas, proses enkripsi mengubah *plaintext* menjadi *ciphertext* (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti. Ini adalah teknik dari ilmu kriptografi, jadi seseorang bisa mengirimkan pesan/text, tetapi orang lain susah mengartikan text tersebut karena harus ada proses penterjemahan dari text yang dikirim tersebut, sehingga keamanan dan kenyamanan dalam tukar menukar data/informasi dapat dirahasiakan.

Berikut secara bagan terjadinya proses enkripsi dan dekripsi :



GAMBAR 2.1

Diagram proses enkripsi dan dekripsi

Peranan kunci sangatlah penting dalam proses enkripsi dan dekripsi (disamping pula algoritma yang digunakan) sehingga kerahasiaannya sangatlah penting, apabila kerahasiaannya terbongkar, maka isi dari pesan dapat diketahui.

Secara matematis, proses enkripsi merupakan pengoperasian fungsi E (enkripsi) menggunakan e (kunci enkripsi) pada M *(plaintext)* sehingga dihasilkan C *(ciphertext),* notasinya :

$$\mathbf{E_e(M) - C}$$

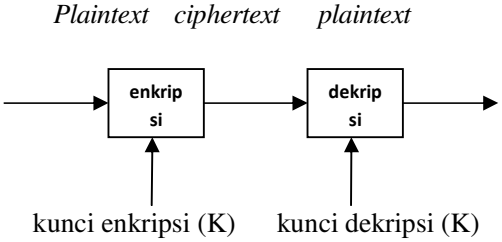
Sedangkan untuk proses dekripsi, merupakan pengoperasian fungsi D (dekripsi) menggunakan d (kunci dekripsi) pada C *(ciphertext)* sehingga dihasilkan M *(plaintext),* notasinya :

$$\mathbf{D_d(C) = M}$$

Sehingga ari dua hubungan diatas berlaku :

$$\mathbf{D_d(E_e(M)) = M}$$

Algoritma simetris *(symmetric algorithm)* adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm.*



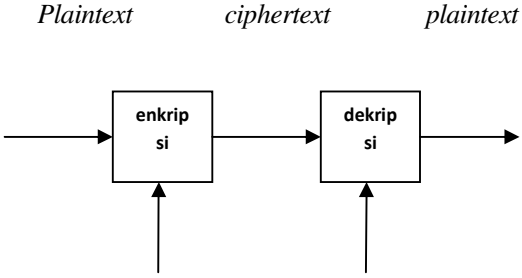
GAMBAR 2.2

Diagram proses enkripsi dan dekripsi algoritma simetris

Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga algoritma kunci rahasia *(secret-key algorithm).* Kelebihan dari

algorithma simetris yaitu kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik dan karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem *real-time* . Sedangkan kelemahanya yaitu untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut dan permasalahan dalam pengiriman kunci itu sendiri yang disebut *"key distribution problem"*

Algoritma asimetris *(asymmetric algorithm)* adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan dua kunci yakni kunci publik *(public key)* dan kunci privat *(private key).* Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan. Berikut penggambaran tentang algoritma asimetris :



GAMBAR 2.3
Diagram proses enkripsi dan dekripsi algoritma asimetris

Pada umumnya kunci publik *(public key)* digunakan sebagai kunci enkripsi sementara kunci privat *(private key)* digunakan sebagai kunci dekripsi. Kelebihannya yaitu masalah keamanan pada distribusi kunci dapat lebih baik, masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit, Sedangkan kelemahan yaitu kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris, untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris, berdasarkan besar data yang diolah dalam satu kali proses, maka algoritma kriptografi dapat dibedakan menjadi dua jenis yaitu :

- Algoritma *block cipher*
  Informasi/data yang hendak dikirim dalam bentuk blok-blok besar (misal 64-bit) dimana blok-blok ini dioperasikan dengan fungsi enkripsi yang sama dan akan menghasilkan informasi rahasia dalam blok-blok yang berukuran sama.

- Algoritma *stream cipher*
  Informasi/data yang hendak dikirim dioperasikan dalam bentuk blok-blok yang lebih kecil (byte atau bit), biasanya satu karakter persatuan persatuan waktu proses, menggunakan tranformasi enkripsi yang berubah setiap waktu.

Pada algoritma penyandian blok *(block cipher),* plainteks yang masuk akan diproses dengan panjang blok yang tetap yaitu *n*, namun terkadang jika ukuran data ini terlalu panjang maka dilakukan pemecahan dalam bentuk blok yang lebih kecil. Jika dalam pemecahan dihasilkan blok data yang kurang dari jumlah data dalam blok maka akan dilakukan proses *pading* (penambahan beberapa bit).

Jenis serangan pada Kriptografi

Selain ada pihak yang ingin menjaga agar pesan tetap aman, ada juga ternyata pihak-pihak yang ingin mengetahui pesan rahasia tersebut secara tidak sah. Bahkan ada pihak-pihak yang ingin agar dapat mengubah isi pesan tersebut. Ilmu untuk mendapatkan pesan yang asli dari pesan yang telah disandikan tanpa memiliki kunci untuk membuka pesan rahasia tersebut disebut kriptoanalisis. Sedangkan usaha untuk membongkar suatu pesan sandi tanpa mendapatkan kunci dengan cara yang sah dikenal dengan istilah serangan (*attack*).Di bawah ini dijelaskan beberapa macam penyerangan terhadap pesan yang sudah dienkripsi :

1. *Ciphertext only attack*, penyerang hanya mendapatkan pesan yang sudah tersandikan saja.
2. *Known plaintext attack*, dimana penyerang selain mendapatkan sandi, juga

mendapatkan pesan asli. Terkadang disebut pula *clear-text attack*.

3. *Choosen plaintext attack*, sama dengan *known plaintext attack*, namun penyerang bahkan dapat memilih penggalan mana dari pesan asli yang akan disandikan.

Berdasarkan bagaimana cara dan posisi seseorang mendapatkan pesan-pesan dalam saluran komunikasi, penyerangan dapat dikategorikan menjadi:

1. *Sniffing*: secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum ataupun sudah dienkripsi) dalam suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekam pembicaraan yang terjadi.
2. *Replay attack* [DHMM 96]: Jika seseorang bisa merekam pesan-pesan *handshake* (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.
3. *Spoofing* [DHMM 96]: Penyerang – misalnya Maman – bisa menyamar menjadi Anto. Semua orang dibuat percaya bahwa Maman adalah Anto. Penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. Contohnya jika orang memasukkan PIN ke dalam mesin ATM palsu – yang benar-benar dibuat seperti ATM asli – tentu sang penipu bisa mendapatkan PIN-nya dan copy pita magentik kartu ATM milik sang nasabah. Pihak bank tidak tahu bahwa telah terjadi kejahatan.
4. *Man-in-the-middle* [Schn 96]: Jika *spoofing* terkadang hanya menipu satu pihak, maka dalam skenario ini, saat Anto hendak berkomunikasi dengan Badu, Maman di mata Anto seolah-olah adalah Badu, dan Maman dapat pula menipu Badu sehingga Maman seolah-olah adalah Anto. Maman dapat berkuasa penuh atas jalur komunikas ini, dan bisa membuat berita fitnah.

Kabel koaxial yang sering dipergunakan pada jaringan sangat rentan terhadap serangan *vampire tap,* yakni perangkat keras sederhana yang bisa menembus bagian dalam kabel koaxial sehingga dapat mengambil data yang mengalir tanpa perlu memutuskan komunikasi data yang sedang berjalan. Seseorang dengan *vampire tap* dan komputer jinjing dapat melakukan serangan pada bagian apa saja dari kabel koaxial. Hingga saat ini masih banyak orang yang menggunakan *cryptosystem* yang relatif mudah dibuka, alasannya adalah mereka tidak mengetahui sistem lain yang lebih baik serta kadang kala terdapat motivasi yang kurang untuk menginvestasikan seluruh usaha yang diperlukan untuk membuka suatu sistem.

Kriptografi Protokol

Dalam mempelajari steganografi tak lepas dari kriptografi, sedangkan di dalam kriptografi harus mengetahui hal-hal sebagai berikut :

Suatu protokol adalah serangkaian langkah yang melibatkan dua pihak atau lebih dan dirancang untuk menyelesaikan suatu tugas. Dari definisi ini dapat diambil beberapa arti sebagai berikut :

- Protokol memiliki urutan dari awal hingga akhir;
- Setiap langkah harus dilaksanakan secara bergiliran;
- Suatu langkah tidak dapat dikerjakan bila langkah sebelumnya belum selesai;
- Diperlukan dua pihak atau lebih untuk melaksanakan protokol;
- Protokol harus mencapai suatu hasil;

Selain itu, suatu protokol pun memiliki karakteristik yang lain, yaitu :

- Setiap orang yang terlibat dalam protokol harus mengetahui terlebih dahulu mengenai protokol dan seluruh langkah yang akan dilaksanakan;
- Setiap orang yang terlibat dalam protokol harus menyetujui untuk mengikutinya;
- Protokol tidak boleh menimbulkan kerancuan;
- Protokol harus lengkap;

Kriptograpfi protocol adalah suatu protokol yang menggunakan kriptografi. Protokol ini melibatkan sejumlah algoritma kriptografi, namun secara umum tujuan protokol lebih dari sekedar kerahasiaan. Pihak-

pihak yang berpartisipasi mungkin saja ingin membagi sebagian rahasianya untuk menghitung sebuah nilai, menghasilkan urutan random, atau pun menandatangani kontrak secara bersamaan. Penggunaan kriptografi dalam sebuah protokol terutama ditujukan untuk mencegah atau pun mendeteksi adanya *eavesdropping* dan *cheating*.

Fungsi Protokol

Dalam kehidupan kita sehari-hari terdapat banyak sekali protokol tidak resmi, misalnya saja dalam permainan kartu, pemungutan suara dalam pemilihan umum. Akan tetapi tidak ada seorang pun yang memikirkan mengenai protokol-protokol ini, protokol-protokol ini terus berkembang, semua orang mengetahui bagaimana menggunakannya. Saat ini, semakin banyak interaksi antar manusia dilakukan melalui jaringan komputer. Komputer ini tentu saja memerlukan suatu protokol formal agar dapat melakukan hal yang biasa dilakukan manusia tanpa berpikir. Bila kita berpindah dari satu daerah ke daerah lain dan mengetahui bahwa kartu pemilihan suaranya berbeda dengan yang biasa kita gunakan, kita dapat beradaptasi dengan mudah. Akan tetapi kemampuan ini belum dimiliki oleh komputer, sehingga diperlukan suatu protokol. Protokol digunakan untuk mengabtraksikan proses penyelesaian suatu tugas dari mekanisme yang digunakan. Protokol komunikasi adalah sama meskipun diimplementasikan pada PC atau VAX. Bila kita yakin bahwa kita memiliki protokol yang baik, kita dapat mengimplementasikannya dalam segala benda mulai dari telepon hingga pemanggang roti cerdas.

Penyerangan terhadap protokol

Penyerangan kriptografi dapat ditujukan pada beberapa hal berikut :

- Algoritma kriptografi yang digunakan dalam protokol;
- Teknik kryptografi yang digunakan untuk mengimplementasikan algoritma dan protokol;
- Protokol itu sendiri;

Seseorang dapat mencoba berbagai cara untuk menyerang suatu protokol. Mereka yang tidak terlibat dalam protokol dapat menyadap sebagian atau seluruh protokol. Tindakan ini disebut penyerangan pasif, karena si penyerang tidak mempengaruhi atau mengubah protokol, ia hanya mengamati protokol dan berusaha untuk memperoleh informasi. Selain itu, seorang penyerang dapat berusaha untuk mengubah protokol demi keuntungannya sendiri. Ia dapat mengirimkan pesan dalam protokol, menghapus pesan, atau bahkan mengubah informasi yang ada di dalam suatu komputer. Tindakan-tindakan ini disebut sebagai penyerangan aktif, karena ia membutuhkan suatu campur tangan aktif. Seorang penyerang tidaklah hanya berasal dari lingkungan luar protokol, namun ia mungkin juga berasal dari dalam protokol itu sendiri, ia dapat merupakan salah satu pihak yang terlibat dalam protokol. Tipe penyerang semacam ini disebut sebagai *cheater*. *Passive cheater* mengikuti protokol, tetapi berusaha memperoleh informasi lebih banyak daripada yang diperbolehkan protokol bagi dirinya. *Active cheater* mengubah protokol dalam usahanya untuk berbuat curang. Usaha untuk menjaga keamanan protokol akan semakin sulit apabila pihak-pihak yang terlibat umumnya merupakan active cheater, oleh karena itu suatu protokol yang baik harus mampu atau pun harus aman terhadap kemungkinan *passive cheating*.

Berbagai macam basic cryptanalytic attacks

Tujuan *cryptanalytic attack* adalah untuk mengetahui beberapa *plaintext* yang sesuai dengan *ciphertext* yang ada dan berusaha menentukan kunci yang memetakan satu dengan yang lainnya. *Plaintext* ini dapat diketahui karena ia merupakan standar atau karena pendugaan. Jika suatu teks diduga berada di dalam suatu pesan, posisinya mungkin tidak diketahui, tetapi suatu pesan lazimnya cukup pendek sehingga memungkinkan *cryptanalyst* menduga *plaintext* yang diketahui dalam setiap posisi yang mungkin dan melakukan penyerangan pada setiap kasus secara paralel. Suatu algoritma enkripsi yang kuat tidak hanya mampu bertahan terhadap serangan *plaintext* yang dikenal tetapi juga mampu bertahan terhadap *adaptive chosen plaintext*. Dalam

penyerangan ini, *cryptanalyst* berkesempatan memilih *plaintext* yang digunakan dan dapat melakukannya secara berulang kali, memilih *plaintext* untuk tahap N+1 setelah menganalisis hasil tahap N. Yang dimaksud *cryptanalytic attacks* adalah usaha-usaha yang dilakukan seseorang untuk memperoleh informasi ataupun data yang telah dienkripsi. Secara ringkas terdapat tujuh macam *basic cryptanalytic attacks* berdasarkan tingkat kesulitannya bagi penyerang, dimulai dari yang paling sulit adalah

- *Ciphertext-only attack*. Dalam penyerangan ini, seorang cryptanalyst memiliki *ciphertext* dari sejumlah pesan yang seluruhnya telah dienkripsi menggunakan algoritma yang sama.
- *Known-plaintext attack*. Dalam tipe penyerangan ini, *cryptanalyst* memiliki akses tidak hanya ke *ciphertext* sejumlah pesan, namun ia juga memiliki *plaintext* pesan-pesan tersebut.
- *Chosen-plaintext attack*. Pada penyerangan ini, *cryptanalyst* tidak hanya memiliki akses atas *ciphertext* dan *plaintext* untuk beberapa pesan, tetapi ia juga dapat memilih *plaintext* yang dienkripsi.
- *Adaptive-chosen-plaintext attack.* Penyerangan tipe ini merupakan suatu kasus khusus *chosen-plaintext attack. Cryptanalyst* tidak hanya dapat memilih *plaintext* yang dienkripsi, ia pun memiliki kemampuan untuk memodifikasi pilihan berdasarkan hasil enkripsi sebelumnya. Dalam *chosen-plaintext attack, cryptanalyst* mungkin hanya dapat memiliki *plaintext* dalam suatu blok besar untuk dienkripsi; dalam *adaptive-chosen-plaintext attack* ini ia dapat memilih blok plaintext yang lebih kecil dan kemudian memilih yang lain berdasarkan hasil yang pertama, proses ini dapat dilakukannya terus menerus hingga ia dapat memperoleh seluruh informasi.
- *Chosen-ciphertext attack*. Pada tipe ini, *cryptanalyst* dapat memilih *ciphertext* yang berbeda untuk didekripsi dan memiliki akses atas *plaintext* yang didekripsi.
- *Chosen-key attack. Cryptanalyst* pada tipe penyerangan ini memiliki pengetahuan tentang hubungan antara kunci-kunci yang berbeda.
- *Rubber-hose cryptanalysis*. Pada tipe penyerangan ini, *cryptanalyst* mengancam, memeras, atau bahkan memaksa seseorang hingga mereka memberikan kuncinya.

Steganografi

Steganografi berasal dari bahasa Yunani yaitu *Steganós* yang berarti menyembunyikan dan *Graptos* yang artinya tulisan sehingga secara keseluruhan artinya adalah tulisan yang disebunyikan. Secara umum steganografi merupakan seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia dengan segala cara sehingga selain orang yang dituju, orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut. Steganografi sudah digunakan sejak dahulu kala untuk kepentingan politik, militer, diplomatik, serta untuk kepentingan pribadi sebagai alat. Beberapa contoh penggunaan steganografi pada masa lampau:

- Pada tahun 480 sebelum masehi, seseorang berkebangsaan Yunani yaitu Demaratus mengirimkan pesan kepada polis Sparta yang berisi peringatan mengenai penyerangan Xerxes yang ditunda. Teknik yang digunakan adalah dengan menggunakan meja yang telah diukir kemudian diberi lapisan lilin untuk menutupi pesan tersebut, dengan begitu pesan dalam meja dapat disampaikan tanpa menimbulakn kecurigaan oleh para penjaga.
- Pada abad ke 5 sebelum masehi, Histaiacus mengirimkan pesan kepada Aristagoras Miletus untuk memberontak terhadap raja Persia. Pesan disampaikan dengan cara mencukur kepala pembawa pesan dan mentato kepalanya dengan pesan tersebut. Kemudian saat rambutnya tumbuh kembali, pembawa pesan dikirimkan dan pada tempat tujuan rambutnya kembali digunduli dan pesan akan terbaca.
- Penggunaan tinta yang tak tampak (*invisible ink*). Tinta dibuat dari campuran sari buah, susu dan cuka. Tulisan di atas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

- Pada perang dunia II, Jerman menggunakan *microdots* untuk berkomunikasi. Penggunaan teknik ini biasa digunakan pada *microfilm* chip yang harus diperbesar sekitar 200 kali.
- Pada perang dunia II, Amerika Serikat menggunakan suku Indian Navajo sebagai media untuk berkomunikasi.

Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia (teks atau gambar) di dalam file-file lain yang mengandung teks, image, bahkan audio tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari file 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 diselesaikan 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. Pada metode steganografi cara ini sangat berguna jika digunakan pada cara steganografi komputer karena banyak format file digital yang dapat dijadikan media untuk menyembunyikan pesan. Format yang biasa digunakan diantaranya:

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

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.

Metode Steganografi

Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari bidang jenis teknik untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan): menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungi data dan penyelubungan data dalam bits dipilih sebelumnya. Ada empat jenis metode Steganografi, yaitu :

1.**LSB (*Least Significan Bit Insertion*)**

Metode yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya pada file image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data *pixel* yang menyusun file tersebut. Seperti kita ketahui untuk file *bitmap* 24 bit maka setiap *pixel* (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian pada setiap *pixel* file *bitmap* 24 bit kita dapat menyisipkan 3 bit data.

Keuntungan dari LSB Insertion :
Keuntungan yang paling besar dari algoritma LSB ini adalah cepat dan mudah. Dan juga algoritma tersebut memiliki software steganograpi yang mendukung dengan bekerja diantara unsur pokok warna LSB melalui manipulasi pallete (lukisan).

Kekurangan dari LSB Invertion :
LSB Insertion dapat secara drastis merubah unsur pokok warna dari *pixel*. Ini dapat

menunjukkan perbedaan yang nyata dari cover image menjadi stego image, sehingga tanda tersebut menunjukkan keadaan dari steganograpi. Variasi warna kurang jelas dengan 24 bit image, bagaimanapun file tersebut sangatlah besar. Antara 8 bit dan 24 bit image mudah diserang dalam pemrosesan image, seperti *cropping* (kegagalan) dan *compression* (pemampatan).

2.*Algorithms and Transformation*

Metode Steganograpi yang lain adalah menyembunyikan data dalam fungsi matematika yang disebut *algoritma compression.* Dua fungsi tersebut adalah *Discrete Cosine Transformation (DCT)* dan *Wavelet Transformation*. Fungsi DCT dan *Wavelet* yaitu mentransformasi data dari satu tempat (*domain*) ke tempat (*domain*) yang lain. Fungsi DCT yaitu mentransformasi data dari tempat spatial (*spatial domain*) ke tempat frekuensi (*frequency domain*).

3 Redundant Pattern Encoding

Redundant Pattern Encoding adalah menggambar pesan kecil pada kebanyakan gambar. Keuntungan dari metode ini adalah dapat bertahan dari *cropping* (kegagalan), kerugiannya yaitu tidak dapat menggambar pesan yang lebih besar.

4 *Spread Spectrum Method*

Spread Spectrum steganografi terpencar-pencar sebagai pesan yang diacak (*encrypt*) melalui gambar (tidak seperti dalam LSB). Untuk membaca suatu pesan, penerima memerlukan algoritma yaitu *crypto-key* dan *stego-key*. Metode ini juga masih mudah diserang yaitu penghancuran atau pengrusakan dari kompresi dan proses *image* (gambar).

Steganografi menyembunyikan pesan dalam gambar

Steganografi adalah seni dan ilmu menyembunyikan pesan, sehingga pesan tersebut sampai kepada penerima tanpa ada orang lain, selain pengirim dan penerima, yang menyadari keberadaan pesan tersebut. *Steganography* termasuk ke dalam *security through obscurity*. Steganografi biasa digunakan oleh teroris, intelijen, atau militer dalam menyampaikan pesan sehingga tidak diketahui orang lain. Steganografi digital adalah suatu steganografi dengan cara menyembunyikan pesan ke dalam suatu file digital. Pesan yang terkirim melalui internet sangat rentan terhadap adanya pencuri dengan paket oleh orang lain. *Steganography* digital merupakan salah satu cara untuk menjaga aspek *confidentiality* tersebut. Berbagai macam steganografi digital antara lain menyembunyikan pesan ke dalam file gambar, file audio, file video, dalam percakapan *VoIP*, dalam kode suatu program, status di social *networking,* dan masih banyak lagi.

Steganografi berbeda dengan kriptografi. Pada steganografi, sniffer tidak dapat melihat pesan yang benar-benar ingin disampaikan, yang terlihat adalah file atau pesan lain yang menjadi persembunyian pesan sebenarnya. Pada kriptografi, *sniffer* menyadari keberadaan pesan tersebut, hanya saja pesan tersebut tidak terbaca karena telah terenkripsi. Dengan enkripsi yang bagus mungkin *sniffer* akan kesulitan membaca pesan tersebut, tetapi dengan menyadari keberadaan pesan tersebut, *sniffer* bisa berusaha untuk mendekripsikannya. Dengan steganografi, *sniffer* tidak menyadari keberadaan pesan, namun bila ditemukan, pesan akan mudah dibaca.Terkadang kedua teknik tersebut dipakai bersamaan. Pesan dienkripsi terlebih dahulu menjadi suatu *ciphertext*, kemudian *ciphertext* tersebut disembunyikan ke dalam file lain. *Sniffer* akan lebih sulit mengetahui keberadaan pesan karena *ciphertext* hanya terlihat seperti kode-kode ASCII tidak beraturan. Meskipun keberadaannya diketahui, *ciphertext* tersebut harus didekripsi terlebih dahulu. Meskipun demikian penulis tetap melampirkan landasan teori tentang kriptografi sebagai dasar dan pengembangan dari steganografi, karena kedua teknik tersebut tetap saling berkaitan. Dalam menjalankan aplikasi penyisipan *text* didalam *image*/gambar, penulis menggunakan program aplikasi MATLAB.

Matlab

Nama Matlab merupakan singkatan dari *matrix laboratory*. Matlab pada awalnya ditulis untuk memudahkan

akses perangkat lunak matrik yang telah dibentuk oleh *LINPACK* dan *EISPACK*. Saat ini perangkat MATLAB telah menggabung dengan *LAPACK* dan *BLAS library,* yang merupakan satu kesatuan dari sebuah seni tersendiri dalam perangkat lunak untuk komputasi matrik.

Dalam lingkungan pendidikan, khususnya perguruan tinggi teknik, Matlab merupakan perangkat standaruntuk memperkenalkan dan mengembangkan penyajian materi matematika, rekayasa dan komputasi. Di industri, MATLAB merupakan perangkat pilihan untuk penelitian dengan produktifitas yang tinggi, pengembangan dan analisanya.

Penggunaan Matlab meliputi bidang - bidang :

- Matematika dan Komputasi
- Pembentukan Algorithm
- Akusisi Data
- Pemodelan, simulasi, dan pembuatan prototipe
- Analisa data, explorasi, dan visualisasi
- Grafik Keilmuan dan bidang Rekayasa

Fasilitas Matlab

Fitur-fitur MATLAB sudah banyak dikembangkan, dan lebih kita kenal dengan nama *toolbox*. Sangat penting bagi seorang pengguna Matlab, *toolbox* mana yang mandukung untuk *learn* dan *apply technology* yang sedang dipelajarinya. *Toolbox-toolbox* ini merupakan kumpulan dari fungsi-fungsi seperti: *sum, sin, cos*, dan *complex arithmetic*, sampai dengan fungsi-fungsi yang lebih kompek seperti *matrix inverse, matrix eigen values, Bessel functions,* dan *fast Fourier transforms.*

c. MATLAB *Language*

Merupakan suatu *high-level matrix/ array language* dengan control *flow statements, functions,* data *structures, input/output, dan fitur-fiturobject-oriented programming*. Ini memungkinkan bagi kita untuk melakukan ke-dua hal baik "pemrograman dalam lingkup sederhana " untuk mendapatkan hasil yang cepat, dan "pemrograman dalam lingkup yang lebih besar" untuk memper-oleh hasil-hasil dan aplikasi yang komplek.

MATLAB (*M-files*) yang telah dikembangkan ke suatu lingkungan kerja MATLAB untuk memecahkan masalah dalam kelas particular. Area-area yang sudah bisa dipecahkan dengan *toolbox* saat ini meliputi pengolahan sinyal, sistem kontrol, *neural networks, fuzzy logic, wavelets*, dan lain-lain.Selain *toolbox*, matlab juga dilengakapi dengan *Simulink* yang sangat *powerfull* untuk mensimulasikan dan menyelesaikan masalah - masalah yang berhubungan dengan Pemodelan Matematika. Dengan *Simulink*, kita dapat dengan mudah mengecek kestabilan suatu model Matematika yang kita punya.

Sebagai sebuah sistem, MATLAB tersusun dari 5 bagian utama:

a. Development Environment.

Merupakan sekumpulan perangkat dan fasilitas yangmembantu anda untuk menggunakan fungsi-fungsi dan file-file MATLAB. Beberapa perangkat ini merupakan sebuah *graphical user interfaces (GUI).* Termasuk di dalamnya adalah MATLAB *desktop* dan *Command Window, Command history,* se-buah editor dan *debugge*r, dan *browsers* untuk melihat *help, workspace, files,* dan *search path.*

b. MATLAB *Mathematical Function Library*

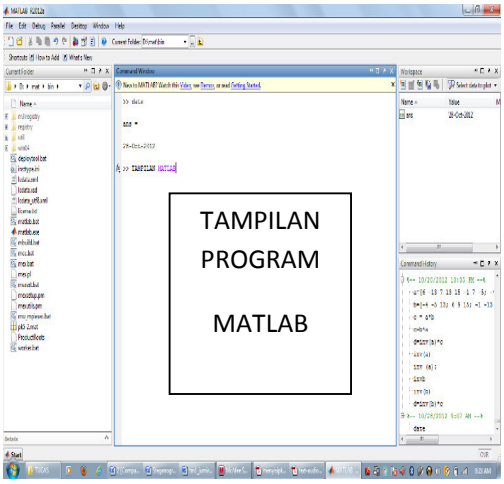
Merupakan sekumpulan algoritma komputasi mulai dari fungsi-fungsi dasar

d. Graphics

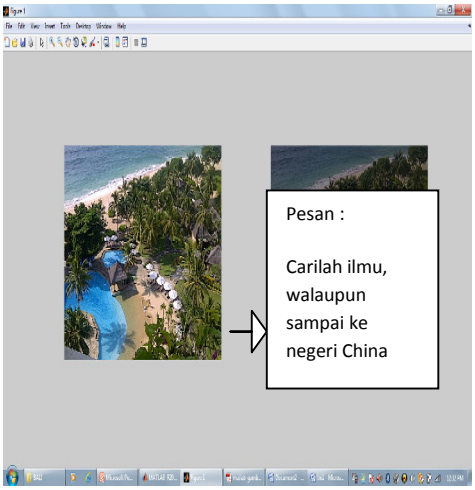
MATLAB memiliki fasilitas untuk menampilkan vektor dan matrik se-bagai suatu grafik. Di dalamnya melibatkan *high-level functions* (fungsi-fungsi level tinggi) untuk visualisasi data dua dimensi dan data tiga dimensi, *image pro-cessing, animation*, dan *graphics presentation*. Ini juga melibatkan fungsi level rendah yang memungkinkan bagi anda untuk membiasakan diri untuk memunculkan grafik mulai dari bentuk yang sederhana sampai dengan tingkatan *graphical userinterfaces (GUI)* pada aplikasi MATLAB anda.

e. MATLAB *Application Program Interface (API)*

Merupakan suatu *library* yang memungkinkan program yang telah anda tulis dalam bahasa C dan *Fortran* mampu berinterakasi dengan MATLAB. Ini melibatkan fasilitas untuk pemanggilan *routines* dari MATLAB (*dynamic linking*), pemanggilan MATLAB sebagai sebuah *computational engine,* dan untuk membaca dan menuliskan MAT-files



GAMBAR 2.4
Tampilan MATLAB



GAMBAR 2.5
Penyisiapn Text pada Image

3.Kesimpulan

Kiranya cukup penulis paparkan berbagai teori dan analisa sampai kesemua aspek teknologi informasi terkait dengan perkembangan keilmuan mengenai kekurangan dan kelebihan dari Penyisipan *Text* pada *image*/gambar dengan metode steganografi menggunakan program Matlab. Berdasarkan hasil analisa dari beberapa sumber referensi mengenai teknologi informasi terutama yang menyangkut dengan keamanan, kerahasiaan pada aplikasi staganografi secara umum dapat disimpulkan sebagai berikut :

1. Steganografi adalah Tehnik menyembunyikan
   atau menyamarkan keberadaan pesan rahasia dalam suatu media penampung sehingga orang lain tidak menyadari adanya pesan didalam media tersebut.
2. Kata steganografi berasal dari kata *Steganus* yang sebenarnya merupakan kata dari bahasa yunani mempunyai nilai arti penyamaran atau penyembunyian dan *Grafine* atau *grapthos* yang memiliki arti tulisan.

Itulah beberapa kesimpulan terkait dengan steganografi yang digunakan dalam mengirimkan pesan rahasia lewat gambar agar dapat mengirim pesan tanpa diketahui orang banyak.

Saran yang dapat penulis sampaikan antara lain :

1. Masih diperlukan pengembangan sehingga steganografi dapat diaplikasikan lebih luas para pengguna TI.
2. Perlu ditingkatkan penelitian yang lebih luas dan dalam, sehingga peningkatan dan kehandalan program dapat di tingkatkan.

Demikian kesimpulan dan saran yang dapat penulis sampaikan semoga dapat bermanfaat sebagai bahan referensi pengetahuan dan wawasan yang terkait teknologi informasi terutama Teknik komputasi Terapan , bagi penulis semoga menambah wawasan dan kelimuan yang dapat dipergunakan ditempat lain.

Daftar Acuan

[1] *Apa yang anda ketahui tentang Matlab* http://www.yangcanggih.com
[2] *Steganografy,* http://www.Wikepedia.org

[3] *Kriptografy*, http://www/kriptologi.wekia.com
[4] *Matlab pemrograman citra digital*, http://www.tomshardware.com
[5] *Sekilas tentang Matlab 7*, http://www.infokomputer.com
[6] http://www.rsa.com (RSA Inc.)
[7] http://theory.lcs.mit.edu/~rivest/ (Donald L. Rivest-the R in RSA)
[8] http://www.cryptography.com
[9] *Matlab 7*, http://en.wikipedia.org
[11] *Computer Organization Matlab Programing*, William Stallings, Edition 9 *Review Pemrograman_Matlab,* http://www.notebookcheck.net