PEMANFAATAN METODE LSB PADA CITRA DIGITAL DALAM MENGAPLIKASIKAN STEGANOGRAFI SEBAGAI UPAYA PENINGKATAN JAMINAN KEAMANAN DALAM TRANSAKSI INFORMASI SECARA ONLINE

T. Adi Kurniawan
Prodi Studi Teknik Informatika
Universitas Satya Negara Indonesia
Email : t.adikurniawan@gmail.com

ABSTRAK

E-mail merupakan layanan yang disediakan sistem teknologi informasi sebagai sarana untuk bertukar informasi di dunia digital. Bentuk informasi yang dapat ditukar berupa data teks, citra digital, video, audio. Berkomunikasi menggunakan *e-mail* memiliki banyak kelebihan namun di sisi lain rentan terhadap kegiatan digital *attacker*, seperti penyadapan. Untuk memenuhi aspek kerahasiaan sebuah pesan dapat digunakan teknik steganografi yaitu penyisipan pesan tersembunyi pada file gambar yang berfungsi sebagai media penampung sehingga tampak seperti pesan biasa, dimana pesan yang dikirim hanya dapat dibaca oleh penerima yang memiliki hak untuk mengetahui isi pesan tersebut. Pada Penelitian ini, digunakan suatu metode *steganografi* berbasiskan LSB (*Least Significant Bit*) untuk mengirimkan data rahasia secara aman, karena pesan yang dikirim akan hancur dengan sendirinya apabila di buka paksa atau di ganggu oleh pihak lain. Data yang dapat disisipkan tidak hanya berupa teks dan file yang berformat *.txt saja akan tetapi data yang berbentuk video dan audiopun dapat disisipkan pada citra gambar. Dari penelitian yang dilakukan dapat menjadi alternatif solusi untuk menjamin terpenuhinya aspek-aspek keamanan informasi khususnya *e-mail* yang meliputi confidentiality, integrity, authentication dan non-repudiation.

Kata Kunci: *Steganografi, Citra Digital, LSB (Least Significant Bit*),*E-mai,Embedding Gambar*.

ABSTRACT

*E - mail is a service provided as a means of information technology systems for the exchange of information in the digital world. The shape information can be exchanged in the form of text data, digital images, video, audio. Communicate using e - mail has many advantages, but on the other hand are vulnerable to attackers digital activities, such as wiretapping. To meet the confidentiality of a message can use steganography technique is the insertion of hidden message in an image file that serves as a container for the media so that it looks like a regular message, wherein the message sent can only be read by the recipient who has the right to know the contents of the message. In this study, we used a method based steganography LSB (least significant bit) to securely transmit confidential data, because the message sent will destroy itself if forced open or disturbed by other parties. The data can be inserted not only in the form of text and file format * . Txt only, but the data in the form of video and audio can be pasted on the image of the picture. From the research conducted can be an alternative solution to ensure the security aspects of information, especially e-mail that includes confidentiality, integrity, authentication and non-repudiation, especially at PT. XYZ.*

Keywords: *Steganography, Digital Image, LSB (Least Significant Bit), E-mail, Embedding Image*

PENDAHULUAN

PT. XYZ (Rancang Bangun Teknologi Informasi) merupakan organisasi bisnis dan jasa layanan teknologi informasi yang menangani infrastruktur TI di kalangan instansi pemerintah dan swasta. Dalam melakukan proses komunikasi dan koordinasi, pimpinan dan karyawan PT. XYZ menggunakan layanan *e-mail* untuk saling bertransaksi informasi. Data atau informasi yang biasanya dikomunikasikan bersifat terbatas dan rahasia seperti proyek perusahaan, nama pelanggan, dokumen perusahaan, jenis proyek, nama proyek, dana proyek, pihak yang terlibat dalam proyek, dan lain-lain. Informasi yang demikian tentunya akan berdampak buruk apabila jatuh ke tangan pihak yang tidak berhak, contohnya pihak pesaing bisnis. Pada Penelitian ini, digunakan suatu metode *steganografi* berbasiskan LSB (*Least Significant Bit*) untuk mengirimkan data rahasia secara aman, karena pesan yang dikirim akan hancur dengan sendirinya apabila di buka paksa atau di ganggu oleh pihak lain.

RUMUSAN MASALAH

Bagaimana Rancangan Implementasi metode *Least Significant Bit* dapat menyelesaikan proses steganografi yang digunakan dalam aplikasi yang telah dibuat dan Bagaimanakah perbandingan keamanan dari hasil simulasi sebelum dan sesudah implementasi rancangan tersebut.

TUJUAN PENELITIAN

Tujuan dari penelitian ini adalah menerapkan steganografi pada media citra dengan metode *Least Significant Bit* yang akan diimplementasikan pada sebuah aplikasi penyembunyian pesan berupa citra digital ke dalam media citra digital lain sehingga steganalis kesulitan mengetahui keberadaan pesan tetapi mudah untuk diekstraksi oleh pihak yang mempunyai hak akses.

LANDASAN TEORI

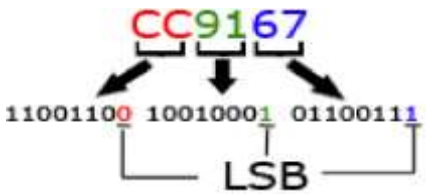
Steganografi

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Kata "steganografi" berasal dari bahasa Yunani *steganos*, yang artinya “tersembunyi atau terselubung”, dan *graphein*, “menulis”.

Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya, kebanyakan pesan disembunyikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya. Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.

Least Significant Beat

Least Significant Bit (LSB) adalah bit-bit yang jika diubah tidak akan berpengaruh secara nyata terhadap kombinasi warna yang dihasilkan oleh komponen warna pada gambar[5]. Metoda yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya, pada berkas image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut. Pada berkas bitmap 24 bit, 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 berkas bitmap 24 bit kita dapat menyisipkan 3 bit data. Bit-bit LSB ini terdapat pada 4 bit akhir dalam 1 *byte* (8 bit).



Gambar 1 *Least Significant Bit* (LSB)

Pada gambar 2.4 terlihat bit-bit LSB pada suatu *pixel* warna dan penyisipan informasi dapat dilakukan pada bit-bit tersebut.

Contoh:

Data awal, tiga *pixel* dari gambar 24-bit, yaitu:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Nilai biner dari karakter'A' adalah sebagai berikut:

(00100111 11101000 11001000) ➔**100**
(00100110 11001000 11101000) ➔**000**
(11001000 00100111 11101001) ➔**11,**

hanya bit-bit yang digaris bawahi yang mengalami perubahan [6]

Review dan Perbandingan Model Kualitas

Dalam Analisa perbandingan kualitas model berdasarkan kriteria dan struktur yang terdapat pada masing-masing model kualitas dibahas pada sub bab ini. Pada Tabel . 1 Tabel perbandingan model kualitas berdasarkan karakteristik dari model kualitas. Kriteria yang dipilih sebagai perbandingan adalah kriteria yang diutamakan dari layer pertama dari masing-masing model kualitas

Tabel 1 Tabel perbandingan model kualitas
berdasarkan karakteristik

Karakteristik Kualitas	ISO 9126	Boehm	Furps	Mc Call
Testability	☑	☑		☑
Integrity	☑			☑
Interoperability	☑			☑
Maturity	☑			
Reliability	☑	☑	☑	☑
Flexibiality		☑	☑	☑
Funcionality	☑		☑	☑
Usability/Human enginnering	☑	☑	☑	☑
Correectness	☑			☑
Efficiency	☑	☑	☑	☑
Understandability	☑	☑		
Porbability	☑	☑		☑
Reusability	☑			☑
Changeability	☑			
Maintainabielity	☑	☑	☑	☑

Berdasarkan Tabel 1, dapat dianalisa berdasarkan karakteristik dari model kualitas sebagaimana berikut:

a. ISO 9126 tidak menganalisa kriteria flexibility.
b. Boehm tidak menganalisa kriteria *correctness, functionality, integrity, interoperability, maturity, changeability* dan *reusability.*
c. FURPS tidak menganalisa *testability, correctness, understandability, integrity, interoperability, maturity, changeability, portability, reusability. Flexibility* pada FURPS berhubungan dengan *extensibility, adaptability* dan *maintainability*.
d. McCall tidak menganalisa kriteria *understandability, functionality, maturity* dan *changeability* dari produk perangkat lunak.

Berdasarkan analisa diatas maka model kualitas yang paling lengkap dan sesuai untuk mengevaluasi aplikasi Steganografi berdasarkan kriteria yang dibutuhkan adalah ISO 9126 dan MC Call.

TINJAUAN PUSTAKA

Steganalysis adalah seni mendeteksi keberadaan pesan dan digunakan untuk memblokade atau memecahkan komunikasi rahasia. Berbagai teknik steganografi telah diusulkan dalam berbagai literatur untuk mengamankan sebuah data rahasia. Least Significant Bit (LSB) steganografi adalah salah satu teknik yang paling banyak digunakan oleh beberapa peneliti, diantaranya :

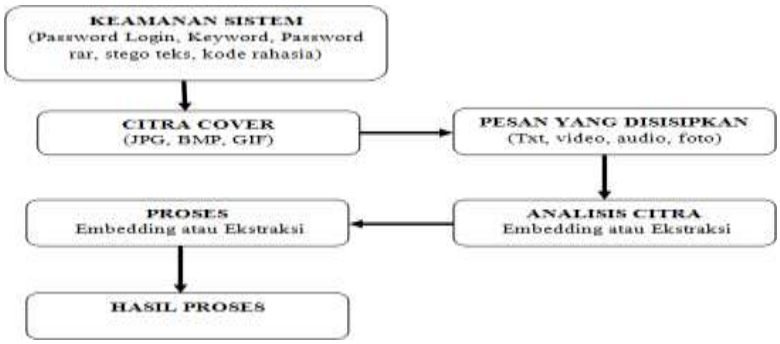
Tabel 2 Tabel Studi Literatur

No	Hasil Penelitian Sebelumnya		
	Judul	**Nama Peneliti**	**Hasil Penelitian**
1	*Steganographi Dengan Metode LSB (Least Significant Bit) Pada Citra Digital*	Ana Sapta Rindi (ANA 2010)	Tidak ada perbedaan pada kualitas image antara stego-image dengan image asli, tetapi ketika pesan rahasia disisipkan pada image yang berlatar belakang kuning polos, stego image mengalami perubahan warna menjadi abuabu.
2	*Steganografi pada Enkripsi Image dengan Menggunakan Least Significant Bit Insertion*	Ronny (RONNY 2009)	Korelasi dan entropi dari sebuah gambar sebelum dan sesudah dilakukannya data mixing dapat meningkatkan level keamanan pada steganografi
3	*Implementasi Teknik Steganografi Dengan Metoe LSB Pada Citra Digital, Jurusan Sistem Informasi*	Putri (PUTRI 2009)	Algoritma LSB (Least Significant Bit) dapat digunakan dengan baik untuk menyembunyikan pesan di dalam pesan sebuah image atau file citra digital sehingga pada proses ekstraksi, pesan atau informasi yang disisispkan pada file citra uji dalam aplikasi Steganografi dapat diperoleh kembali secara utuh
4	*Steganografi Berbasis Least Significant Bit (LSB) Pada Gambar dengan Penyisipan Berukuran Variabel*	Lindaya nti (LINDA 2007)	Least Significant Bit (LSB) pada gambar dengan penyisipan berukuran variabel sudah dapat menghasilkan stego-image yang bila dilihat secara visual memiliki tampilan yang hampir sama dengan covernya
5	*Data Embedding Based on Better Use of Bits in Image Pixels*	Alwan(ALWAN 2005)	Metode embedding gambar adalah salah satu metode kompresi yang cukup baik dalam hal penyediaan ruang memori
6	*Pengembangan Metode Steganografi untuk Penyembunyian, Data di dalam Citra Digital dengan Menggunakan Metode LSB (Least Significant Bit)*	Hartono(HARTONO 2005)	Metode LSB memiliki keunggulan yaitu, tidak dibutuhkan citra digital pembanding untuk mengembalikan data. waktu yang dibutuhkan untuk penyembunyian data cepat dan penurunan kualitas citra digital yang dihasilkan relatif kecil

Berdasarkan tinjauan studi di atas, maka perbedaan penelitian ini dengan penelitian sebelumnya yaitu terletak pada objek dan tujuan penelitian. Pada penelitian sebelumnya hanya menjelaskan deskripsi, analisis dan implementaasi algoritma *Least Significant Bit* (LSB) yang dapat menyimpan pesan rahasia berupa teks dan file berformat*.txt saja. Maka pada penelitian ini akan mengimplementasikan algoritma *Least Significant Bit* (LSB) dengan menyisipkan teks dan file berformat *.txt, video, audio, foto pada citra gambar (citra cover).

KERANGKA PEMIKIRAN

Kerangka pemikiran merupakan urut-urutan logis proses untuk dapat memecahkan suatu masalah penelitian. Gambar 2 menunjukkan kerangka pemikiran aplikasi yang akan dibangun. Langkah pertama yaitu masuk ke menu login dengan memasukkan user name dan paswor login, selanjutnya memanggil atau membuka citra cover dalam format (JPG, BMP, GIF). Langkah selanjutnya citra cover disisipi sebuah pesan rahasia atau stego teks dan kita bisa tambahkan keyword sebagai keamanan data. Setelah itu dilakukan analisa citra yang terbagi atas dua proses yaitu *embedding* dan ekstraksi. Pada analisa citra *embedding* dan ekstraksi akan dianalisa bahwa *stegoimage* yang dibuka adalah hasil dari *embedding* sebelumnya . Kemudian dilakukanlah proses *embedding* atau ekstraksi yang akan menghasilkan *stegoimage* dari proses *embedding* dan *hiddenimage* dari proses ekstraksi.



Gambar 2 Kerangka Pemikiran.

Hipotesis Penelitian

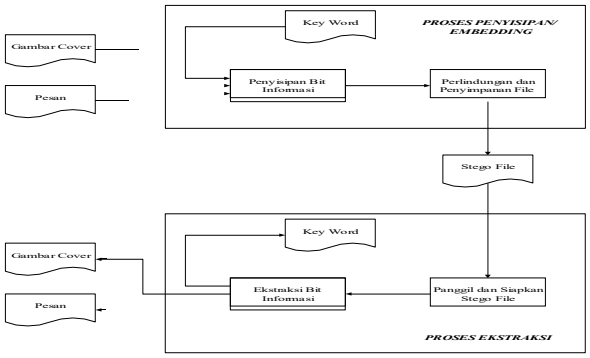
Berdasarkan kerangka pemikiran diatas, maka dapat di ambil hipotesis bahwa system yang dibangun dilengkapi dengan security ganda sehingga keamanan informasi yang meliputi aspek confidentiality, authentication, integrity dan non-repudiationpun lebih terjamin. System juga dilengkapi dengan algoritma *Least Significant Bit* (LSB) dengan menyisipkan teks dan file berformat *.txt, video, audio, foto pada citra cover yang hasilnya tidak bisa di tangkap dengan indera manusia biasa.

PERANCANGAN SISTEM

Dalam perkembangan dunia informasi, keamanan suatu informasi merupakan suatu hal yang sangat vital. Hal ini dikarenakan tidak semua pihak, berhak untuk mengakses informasi yang bersangkutan. Oleh karena itu diperlukan suatu aplikasi yang dapat digunakan untuk menyembunyikan atau menyamarkan suatu informasi ke dalam media lain.

Pada bagian ini akan dijelaskan mengenai gambaran umum dari proses kerja aplikasi steganografi yang akan dibuat sebelum kita memulai fase perancangan sistem. Sebelum masuk ke dalam proses penyisipan (hiding), ada beberapa hal yang harus dilakukan terlebih dahulu oleh aplikasi ini nantinya. *Pertama* user memasukkan Gambar yang bertindak sebagai cover. *Kedua* user selanjutnya memasukkan pesan. Dalam proses ini akan dilakukan penghitungan ukuran file informasi yang akan disisipkan. Jika ukuran file pesan lebih kecil dari ukuran file cover, proses akan dilanjutkan, sebaliknya user akan diminta untuk memasukkan pesan lain. *Ketiga* aplikasi akan melakukan penyisipan bit

informasi. *Keempat* aplikasi akan menghasilkan file berupa *stegno file*. Proses penyisipan dan ekstraksi informasi dapat dilihat pada **Gambar 3**



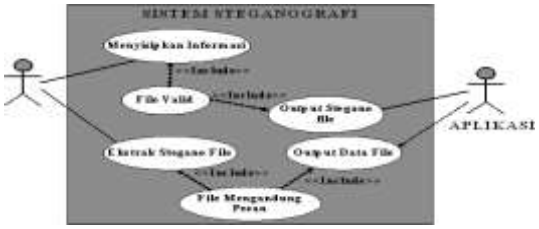
Gambar 3 Skema proses penyisipan dan Ekstraksi

Proses

Perancangan proses yang dimaksudkan adalah bagaimana sistem akan bekerja, proses-proses yang digunakan, mulai dari user melakukan input kemudian hingga aplikasi mengeluarkan output berupa stego file pada proses penyisipan (hiding). Dan juga saat user melakukan input stego file dan key file hingga aplikasi memberikan output berupa secret file dan carrier file pada proses penguraian (extracting).

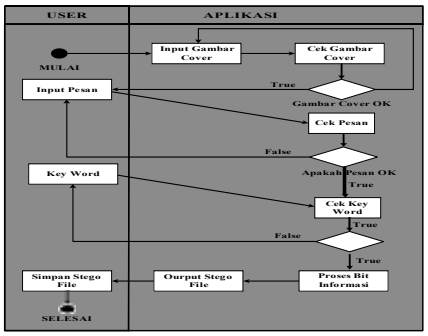
Antar Muka

Perancangan antarmuka mengandung penjelasan tentang desain dan implementasi sistem yang digunakan dalam sistem yang dibuat dan diwujudkan dalam tampilan antarmuka yang menghubungkan user dengan aplikasi. Gambar 4 menunjukkan use case diagram dari sistem yang akan dibangun.



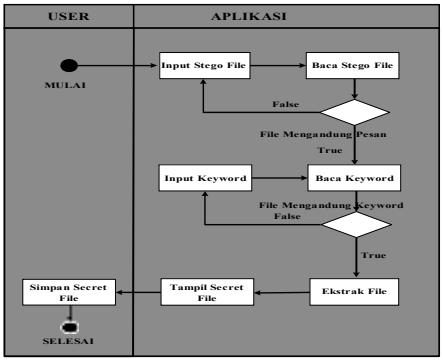
Gambar 4 Use Case Diagram Aplikasi

Proses utama yang dilakukan ada empat yaitu proses penyisipan informasi, proses output stego image, proses penguraian informasi dan proses output informasi file. Berikut activity diagram dari keempat proses tersebut:



Gambar 5. Activiti Diagram Penyisipan Informasi

Proses yang dijelaskan oleh gambar 5 berlangsung saat user ingin melakukan penyisipan informasi ke dalam file gambar. Dari proses penyisipan informasi maka diperoleh hasil output file berupa stego-file.

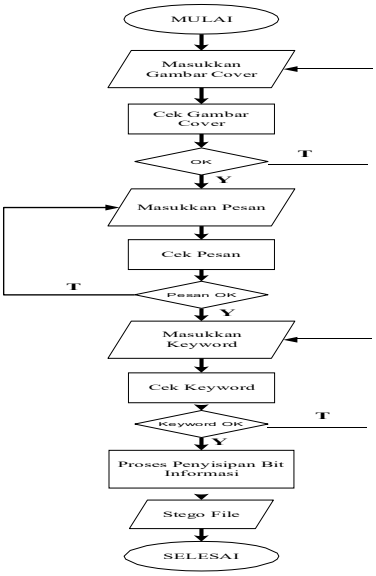


Gambar 6 Activity Diagram Penguraian Informasi

Dari hasil proses penguraian informasi, diperoleh hasil keluaran berupa secret file yang telah disisipkan pada proses sebelumnya.

Perancangan Antar Muka

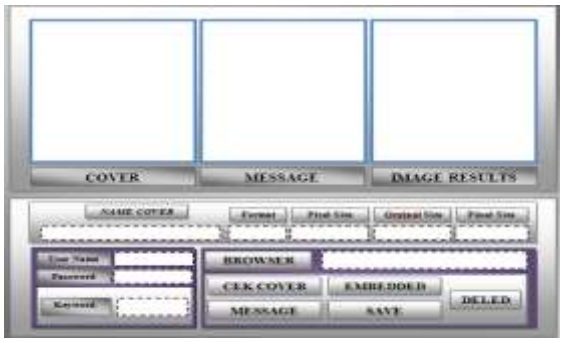
Sesuai dengan algoritma dan flowchart maka dibuatlah tampilan-tampilan yang bertujuan untuk memudahkan pengguna untuk menjalankan aplikasi ini. Tampilan-tampilan yang ada dibuat semenarik mungkin namun tetap sederhana dan bersifat fungsional. Tahap penyisipan informasi merupakan tahap penyisipan atau penyamaran suatu informasi ke dalam file gambar (stegno file) yang bertujuan untuk menyembunyikan informasi tersebut agar tidak terlihat oleh pihak yang tidak berhak.



Gambar 7 Diagram Alir penyisipan Informa

Perancangan menu utama dalam rancangan sistem ini akan memberikan gambaran umum tentang program yang akan dibuat. Perancangan menu berisi pokok-pokok input dari proses yang akan dijalankan sehingga mendapat informasi yang diharapkan.

Racangan menu Utama menggambarkan keseluruhan menu utama dalam aplikasi. Menu Utama terdiri dari Browser, Cek Cover, Message, Embedded, Save, Deled, dan Ekstrak.



Gambar 8 Rancangan Menu Utama

IMPLEMENTASI DAN PENGUJIAN

Pengujian

Pengujian merupakan bagian yang penting dalam siklus pembangunan perangkat lunak. Pengujian di lakukan untuk menjamin kualitas dan juga mengetahui kelemahan dari perangkat lunak. Tujuannya dari pengujian ini adalah untuk menjamin bahwa perangkat

lunak memiliki kualitas yang baik yaitu mampu untuk mempersentasikan kajian pokok dari spesifikasi, analisis, perancangan dan pengkodean dari perangkat lunak itu sendiri. Untuk mengetahui keberhasilan dari program yang telah dirancang, maka perlu dilakukan pengujian terhadap aplikasi ini. Dalam bab ini akan dibahas mengenai proses pengujian yang dilakukan untuk mengetahui keakuratan, efektifitas, efisiensi, dan lain-lain dari aplikasi ini.

Implementasi Program

Program Aplikaasi Steganografi ini dibuat menggunakan bahasa pemrograman PHP. Dasar pertimbangan menggunakan PHP adalah karena *Life Cycle* yang singkat, sehingga PHP selalu *up to date* mengikuti perkembangan teknologi internet selain itu PHP dapat dipakai di hampir semua *web server* yang ada di pasaran seperti Apache, AOLServer, fhttpd, phttpd, Microsoft IIS, dan lain-lainnya yang dijalankan pada berbagai sistem operasi seperti Linux, FreeBSD, Unix, Solaris dan Windows, juga PHP mendukung banyak paket database baik yang komersil maupun non-komersil, seperti postgreSQL, mSQL, MySQL, Oracle, Informix, Microsoft SQL Server, dan banyak lagi.

Gambar 9 Tampilan *Form Message*

Hasil Pengujian

Berikut ini adalah tampilan hasil uji dari 10 sample dan jumlah karakter yang dimasukkan berfariasi.

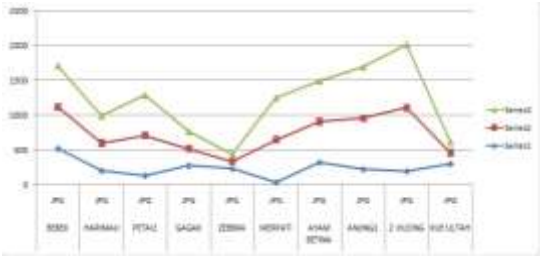
Tabel 3 Sample Pengujian

NO	NAME PICTURE	FORMAT PICTURE	PIXEL SIZE	PESAN	SIZE A	SIZE B
1	BEBEK	JPG	1280 X 960	520	595	595
2	HARIMAU	JPG	1024 X 768	200	395	395
3	PETAI2	JPG	293 X 356	133	576	576
4	GAGAK	JPG	650 X 530	275	242	242
5	ZEBBRA	JPG	500 X 375	232	103	103
6	MERPATI	JPG	800 X 500	34	607	607
7	AYAM BETINA	JPG	633 X 557	322	585	585
8	ANJING1	JPG	1024 X 768	223	731	731
9	2 KUCING	JPG	1024 X 768	197	909	909
10	KUE ULTAH	JPG	259 X 194	300	158	158

Dari sample diatas tidak terdapat perbedaan ukuran atau size antara citra yang sebelum di sisipi pesan (Size A) dengan citra yang sudah disisipi pesan atau di embedded (size B).

Grafik Sample Pengujian

Dari Tabel sample pengujian di atas dapat di peroleh sebuah grafik yang menunjukkan perbedaan antara ukuran atau size pada cover sebelum disisipi pesan dengan ukuran cover setelah disisipi pesan serta pengaruh dari banyaknya karakter huruf yang di sisipkan pada citra cover.



Gambar IV.7 Grafik Sample Pengujian

Keterangan :

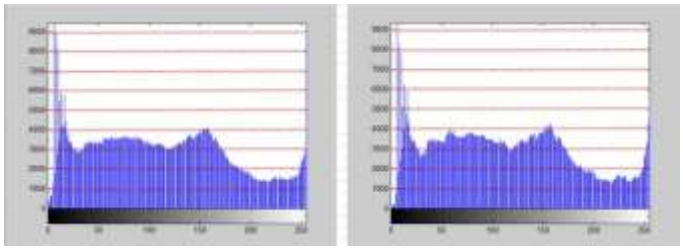
Series 1 : Banyaknya karakter huruf yang disisipkan pada citra cover

Series 2 : Besarnya ukuran atau size cover sebelum disisipi pesan

Series 3: Besarnya ukuran atau size cover sesudah disisipi pesan

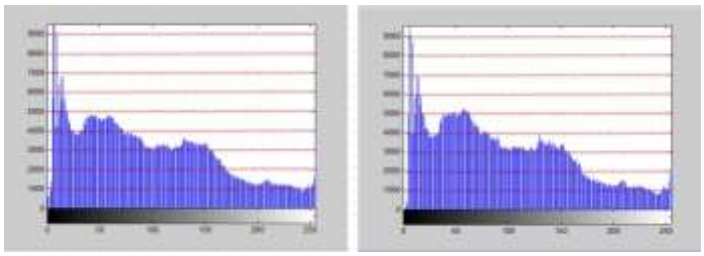
Histogram

Untuk melihat perbedaan antara citra cover asli (citra gambar yang belum disisipi pesan) dengan citra cover hasil embedded (citra gambar yang sudah disisipi pesan), maka kita bisa lihat besaran nois antara citra asli dengan citra embedded. Dalam hal ini bisa di implementasikan dengan gambar histogram yang terbagi menjadi RGB (Red , Green, Blue).



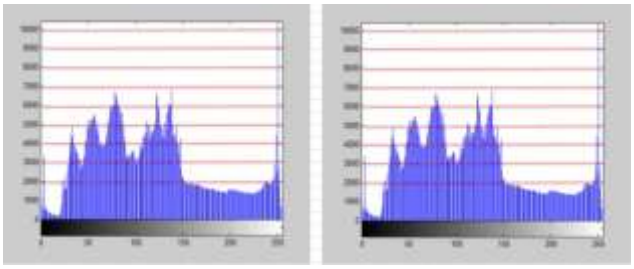
(a) (b)

Gambar IV.8 Histogram dengan warna red



(c) (d)

Gambar IV.9 Histogram dengan warna green



(e) (f)

Gambar IV.10 Histogram dengan warna blue

Keterangan :

Gambar IV.8 Histogram dengan warna red

Pada gambar (a) dan (b) terlihat perbedaannya yang tidak terlalu banyak dimana gambar (a) merupakan citra gambar asli, sedangkan citra gambar (b) adalah citra gambar yang telah disisipi pesan.

Gambar IV.9 Histogram dengan warna green

Pada gambar (c) dan (d) terlihat perbedaan nois yang tidak terlalu banyak seperti dengan sample (a dan b).

Gambar IV.10 Histogram dengan warna blue

Pada gambar (e) dan (f) tidak terlalu banyak perubahan noisnya, bahkan bisa dikatakan hampir tidak ada perbedaan antara gambar (e) dengan gambar(f).

Dari sampel gambar histrogram diatas terlihat bahwa nois terjadi pada warna merah, dan hijau sedangkan warna blue tidak terlalu banyak perubahanya.

Rencana Implementasi

Jika rancangan implementasi Steganografi yang peneliti ajukan diterima oleh PT. XYZ, maka peneliti akan menyusun rencana untuk mewujudkan implementasi tersebut. Berikut ini adalah rencana implementasi yang akan dilakukan:

1. Mengidentifikasi perangkat server, perangkat jaringan termasuk koneksi internet, serta aplikasi *mail server* yang terinstal. Namun demikian, dikarenakan saat penelitian seluruh perangkat tersebut sudah teridentifikasi maka bisa dilanjutkan ke rencana berikutnya.
2. Melakukan simulasi pengiriman dokomen rahasia yang sebenarnya. Ada perbedaan antara rencana simulasi dengan simulasi yang dilakukan pada saat penelitian, yang

membedakan adalah dokumen yang digunakan untuk simulasi. Saat penelitian dokumen yang digunakan adalah murni sebuah dokumen untuk percobaan, bukanlah dokuen PT. XYZ yang sebenarnya.

3. Merekomendasikan kepada PT. XYZ untuk melakukan penilaian *risk management* (manajemen resiko). Hal ini bertujuan agar mengetahui sisi-sisi mana saja di PT. XYZ yang memliki tingkat kerawanan bocornya informasi berklasifikasi biasa atau rahasia.
4. Merekomendasikan kepada PT. XYZ untuk membuat kebijakan tata kelola keamanan informasi. Hal ini bertujuan agar seluruh entitas/*user* yang berada di PT. XYZ baik itu direktur sampai dengan staf agar memiliki kesadaran untuk menjaga aset data/informasi yang berada di PT. XYZ.
5. Merekomendasikan kepada PT. XYZ untuk membuat kebijakan standar kualifikasi Administrator CA, hal ini bertujuan agar personil yang ditunjuk sebagai pihak yang dipercaya untuk mengelola seluruh keamanan data yang ada di PT. XYZ memiliki integritas dan profesional dalam melaksanakan tugasnya.
6. Melakukan sosialisasi ke seluruh karyawan PT. XYZ tentang pengamanan e-mail sebagai sarana bertransaksi data/informasi menggunakan aplikasi steganografi. Hal ini bertujuan untuk memberikan wawawasan kepada karyawan yang nantinya sebagai entitas/*user* mengenai apa itu steganografi, dan bagaimana cara kerja steganografi dalam mengamankan transaksi data/informasi melalui e-mail.
7. Melakukan training manajemen CA. Dalam hal ini hanya dilakukan kepada personil yang ditunjuk sebagai Administrator CA.
8. Melakukan training pengamanan e-mail menggunakan Aplikasi Steganografi. Hal ini dilakukan kepada personil yang akan ditetapkan untuk melakukan transaksi data/informasi yang berklasifikasi rahasia (asumsinya tidak semua karyawan akan melakukan transaksi data/informasi rahasia).
9. Asistensi Administrator CA dalam membangun sertifikat digital yang nantinya sertifikat digital tersebut akan digunakan untuk operasional pengamanan e-mail.
10. Operasional pengamanan e-mail dengan cara mengimplementasikan Aplikasi steganografi telah siap dilaksanakan.

KESIMPULAN

Dari uraian bab pertama hingga bab terakhir, maka dapat diambil kesimpulan sebagai berikut: Implementasi aplikasi Steganografi dengan menggunakan metode *Least Significant Bit* (LSB) berjalan dengan baik dari proses pengembeddan sampai dengan proses penguraian informasi atau ekstraksi. Dari hasil simulasi yang dilakukan antara sebelum dan sesudah menggunakan aplikasi steganografi, dapat di ambil kesimpulan bahwa data atau informasi yang kita kirimkan melalui email akan lebih aman atau lebih terjaga kerahasiaannya dengan menggunakan aplikasi steganografi di bandingkan dengan pengiriman informasi tanpa menggunakan aplikasi steganografi.

SARAN

Perlu dilakukan penelitian lebih lanjut dari segi efisiensi dan efektifitas pada rancangan implementasi steganografi yang dibuat oleh peneliti

DAFTAR PUSTAKA

[1] Aeni Jamilia, Moedjiono, Hadi Syahrial, *Rancangan Implementasi Protokol S/MIME pada Layanan E-Mail Sebagai Upaya Peningkatan Jaminan Keamanan dalam Transaksi Informasi Secara Online: Studi Kasus PT. XYZ,* Program Studi Magister Ilmu Komputer, Universitas Budi Luhur, 2012

[2] Ana Sapta Rindi, Sihar N.M.P. Simamora, Isa Puncuna, *Steganographi Dengan Metode LSB (Least Significant Bit) Pada Citra Digital,* Politeknik Telkom Bandung,2010

[3] Herry Totalis, Yuli Christyono, Ajub Ajulian Zahra, *Aplikasi Pengolahan Citra Digital Untuk Mengontrol Saklar Berdasarkan Letak Dan Warna Huruf*, Jurusan Teknik Elektro, Fakultas Teknik, Universitas Diponegoro, Tembalang, Semarang, Indonesia, 2011.

[4] Alwan, R. H., Kadhim, F. J. dan Al-Taani, A. T. 2005. *Data Embedding Based on Better Use of Bits in Image Pixels. International Journal of Signal Processing 2(2): 104 – 108*.

[5] Lindayanti, *Steganografi Berbasis Least Significant Bit (LSB) Pada Gambar dengan Penyisipan Berukuran Variabel,* Departemen Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Pertanian Bogor-BOGOR 2007.

[6] Johnson NF, jajodia S.1998. *Exploring Steganography : Seeing the Unseen.* George Mason University. http://www.jjtc.com/pub/r2026.pdf [04 Oktober 2006]..

[7] Ronny. 2009. *Steganografi pada Enkripsi Image dengan Menggunakan Least Significant Bit Insertion: 1 – 6.* Institud Teknologi Bandung.

[8] Putri Alatas. 2009. *Implementasi Teknik Steganografi Dengan Metoe LSB Pada Citra Digital, Jurusan Sistem Informasi, Universitas Gunadarma*.

[9] Roman Arubusman, Yusrian, "Skripsi – *AUDIO STEGANOGRAPHY*", Universitas Gunadarma, Jakarta, Agustus2007