Pengamanan File Dokumen Ujian Dengan *Image Steganography* Metode Lsb

Syaifullah Abdurrahman[1], Aditya Prapanca[2]

[1,3] Jurusan Teknik Informatika Fakultas Teknik Universitas Negeri Surabaya
Kampus Ketintang Surabaya
[1]syaifullah.17051204052@mhs.unesa.ac.id
[2]adityaprapanca@unesa.ac.id

***Abstrak*— Steganografi sendiri adalah sebuah metode untuk menyembunyikan atau menyisipkan sebuah file kedalam sebuah media seperti gambar, audio dan video. Steganografi memiliki beberapa metode salah satunya adalah metode *Least Significant Bit* (LSB). Penggunaan Steganografi sendiri biasanya digunakan untuk menyisipkan pesan rahasia ataupun file rahasia kedalam sebuah media supaya file tersebut tidak diketahui keberadaannya oleh orang yang tidak bertanggung jawab seperti seorang *Man In The Middle Attack* yang akan mendeteksi file – file yang ditransfer dari satu komputer ke komputer yang lainnya dengan bantuan *software Wireshark*. Maka dari itu, dengan steganografi ini peneliti dapat mengamankan file rahasia tersebut kedalam sebuah media.**

Pada kegiatan belajar mengajar di sekolah terdapat sebuah ujian seperti UTS dan UAS. File – file untuk ujian tersebut sangatlah rahasia dan tidak boleh bocor. Maka dari itu dibuatlah progam untuk mengamankan file dokumen ujian sekolah kedalam sebuah media yaitu gambar dengan steganografi metode LSB. Serta di lakukan pengujian implementasi seorang MITM yang akan melakukan pendeteksian terhadap file – file yang di transfer dari komputer satu ke komputer yang lainnya.

Persiapan dari pembuatan progam steganografi dan impementasi seorang MITM terdiri dari MatLab digunakan untuk membuat progam steganografi, GNS3 digunakan untuk merancang topologi jaringan sekolah secara virtual, Wireshark digunakan untuk melakukan tindakan pendeteksian file – file yang ditransfer dan *VirtualBox* digunakan untuk menjalankan beberapa komputer virtual. Dari skenario pendeteksian yang telah dibuat, dihasilkan bahwa jika sebuah file yang akan ditransfer sebelumnya dikemas dalam sebuah media stego maka akan lebih aman dari pada kita mengirim file tersebut secara langsung.

***Kata Kunci*— *Image Steganography*, file dokumen ujian sekolah, *Least Significant Bit*, *Man In The Middle*, *Wireshark*.**

I. PENDAHULUAN

Semakin hari penggunaan teknologi semakin di minati oleh masyarakat. Entah itu untuk kebutuhan sehari hari ataupun membantu dalam memudahkan pekerjaan kita. Dalam teknologi itu sendiri kita biasa menggunakan fitur transfer file, kita dapat dengan mudah mengirim file dari komputer kita ke komputer lainnya. Akan tetapi kita harus lebih berhati – hati terhadap keamanan data atau file yang kita transfer. Banyak data yang berisikan informasi penting dan terbatas untuk diketahui pihak yang terkait saja [1]. Bisa saja file yang berisikan data – data penting tersebut disadap sehingga di ketahui dan disalah gunakan oleh pihak yang tidak bertanggung jawab. Perkembangan teknologi yang sangat pesat saat ini juga diimbangi dengan perkembangan keamanan terhadap teknologi guna untuk mengamankan data dari penyerang dari segi integritas, kerahasiaan, perlindungan, privasi, dan prosedur – prosedur lain mengenai keamanan data itu sendiri [2].

Keamanan dalam hidup saat ini adalah hal yang sangat penting. Arti dari keamanan itu sendiri adalah menjaga suatu unsure yang sangat penting dari tindakan yang tidak diinginkan beberapa contohnya adalah informasi dan pesan [3]. Isu tentang keamanan dalam penggunaan teknologi menjadi sangat penting dan patut untuk diperhatikan, Salah satunya adalah keamanan di transfer file itu sendiri, karena fitur tersebut sering digunakan oleh pengguna teknologi untuk berbagi file yang mereka miliki. Kemudahan ini juga membuat mudahnya tersebar data-data privat seseorang [4]. Maka dari itu dibutuhkan sebuah pengamanan data.

Ujian sekolah adalah hal yang paling penting dalam proses belajar mengajar di sekolah tersebut. Guru biasanya menyusun soal – soal ujian di komputer ataupun laptop masing – masing. Dan kemudian setelah soal tersebut selesai disusun maka soal tersebut akan di tranfer ke bagian Tata Usaha (TU) untuk di cetak dan di sebarkan ke siswa – siswi yang akan mengikuti ujian tersebut. Semua hal itu dapat dilakukan dengan mudah karna banyaknya teknologi yang bisa di gunakan saat ini. Teknologi yang ada sekarang ini tidak sepenuhnya aman dari orang ataupun oknum yang ingin mengetahui aktifitas apa saja yang kita lakukan di gadget kita. Contohnya ketika kita transfer file dari komputer kita ke komputer lainnya, orang lain bisa tahu apa saja yang kita transfer dari komputer kita ke komputer lainnya. Serangan tersebut biasa disebut dengan Man in the Middle Attack (MITM). Man in the Middle Attack (MITM) seperti halnya sebuah pertandingan sepak bola dimana dua orang bermain menangkap sementara orang ditengah berupaya untuk mencegat bola [5]. Dan juga, seperti seseorang yang berpura -pura menjadi salah satu dari yang lainnya untuk mendapatkan informasi dari 2 orang tersebut [6]. Serangan MITM biasanya menargetkan individu, dan, serangan sering tetap tidak ditemukan dan tidak tercatat dalam statistik [7]. Di dalam proses transfer file, orang yang biasa berperan sebagai MITM akan mendeteksi dan mengetahui file apa saja yang kita transfer beserta tujuannya. Lalu orang tersebut akan mengakses komputer yang di jadikan tujuan kita menstransfer file tadi dan mengambil file tersebut tanpa kita ketahui bahwa kita telah dideteksi oleh orang tersebut.

Kriptografi merupakan teknik untuk menyembunyikan atau komunikasi secara aman dari hadirnya atau gangguan pihak ketiga (orang lain). Kriptografi berasal dari dua kata dalam Bahasa Yunani, yaitu kryptos yang memiliki arti tersembunyi atau rahasia dan graphein yang memiliki arti menulis. Maka arti kriptografi itu sendiri adalah menulis dengan cara tersembunyi atau rahasia. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut [8]. Kriptografi yang dibedakan berdasarkan waktunya ada dua yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik adalah kriptografi yang telah di temukan sejak jaman dahulu dan proses analisisnya tidak menggunakan komputer ataupun perangkat mesin lainnya contohnya ada Caesar Cipher,Vignere Cipher, Rot13, dll. Sedangkan Kriptografi modern adalah kriptografi yang saat ini ditemukan dan dikembangkan, biasanya terdapat algoritma matematika di dalam kriptografi tersebut. Kriptografi modern yang ada sekarang dibedakan berdasarkan kuncinya, yaitu kriptografi kunci simetris dan kriptografi kunci asimetris. Saat ini, kriptografi modern diciptakan dengan operasi matematika dan direpresentasikan dengan cara yang tidak mudah untuk dapat diakses oleh manusia [9].

Steganografi adalah seni komunikasi tersembunyi. Steganografi dilakukan dengan menyisipkan informasi rahasia di media sebagai sampul untuk menyamarkan keberadaan komunikasi tersembunyi tersebut [10]. Perbedaan Image Steganografi dan Image Watermarking adalah jika pada image steganografi informasi rahasia disembunyikan di dalam media digital dimana media penampung tidak memiliki arti apa - apa . Sedangkan pada watermarking, media digital tersebut yang lebih berharga dan akan dilindungi kepemilikannya atau biasa disebut pemberian label hak cipta terhadap media digital tersebut. Dengan kata lain steganografi bisa saja disebut sebagai teknik penyisipan sebuah file kedalam sebuah media agar tidak diketahui oleh orang lain. Teknik steganografi tersebut dapat diterapkan untuk menyembunyikan file – file penting kita ke dalam sebuah media seperti gambar supaya tidak terdeteksi dan diketahui orang lain yang akan merugikan kita. Cara orang lain dalam mendeteksi file kita salah satunya dengan skema Man In The Middle (MITM) dengan cara sniffing (mengendus). Dengan teknik tersebut orang yang berperan sebagai Man In The Middle akan mengetahui dimana kita mentansfer, meletakkan ataupun menyembunyikan file rahasia kita di komputer tujuan tersebut.

Penelitian sebelumnya yang menjadi acuan untuk penelitian ini dilakukan oleh Hilman Akhyar Damanik dan Merry Anggraeni [11] yang membahas tentang steganografi dengan kombinasi algoritma Less Significant Bit (LSB) dan kriptografi ROT13. Dalam penelitian tersebut dilakukan pengujian kombinasi antara algoritma ROT13 dan Less Significant Bit (LSB) dalam hal untuk autentikasi, penyalahgunaan dan merusak data teks serta mempersulit para kriptanalis dalam pencurian atau perusakan data teks. Pada penelitian tersebut juga di jelaskan secara detail tentang metode LSB, bagan alir steganografi, pengujian terhadap citra dalam aspek Impercepbility dan Recovery. Penelitian tersebut dikatakan berhasil karena membuktikan bahwa steganografi dengan algoritma LSB memenuhi aspek Impercepbility dan Recovery, artinya penelitian tersebut membuktikan bahwa algoritma LSB dapat menghasilkan stego image yang tidak berbeda jauh dengan gambar aslinya dan setelah di lakukan proses decoding Teks tersebut tidak ada kerusakan jika dibandingkan dengan teks aslinya. Akan tetapi, pada penelitian tersebut pesan rahasia itu tidak dijelaskan berupa file dokumen dengan format yang jelas serta tidak dibahas mengapa steganografi sangat penting dan bisa diaplikasikan di kegiatan ataupun dalam pekerjaan sehari – hari. Oleh karena itu, Pada penelitian ini peneliti akan melakukan implementasi steganografi dengan metode LSB dengan media gambar berformat .bmp dan menggunakan file dokumen ujian sekolah dengan format .pdf serta menjelaskan mengapa diperlukan adanya steganografi dan mensimulasikan bagaimana cara seorang Man In The Middle (MITM) bekerja dengan teknik sniffing (mengendus) dengan software bantuan bernama Wireshark. Software Wireshark ini membantu seorang yang berperan sebagai MITM untuk mendeteksi file – file yang telah di transfer ke komputer lain. Dan juga membuktikan bahwa Teknik Image Steganography dengan metode LSB dapat melindungi file tersebut dari pendeteksian yang dilakukan oleh seorang MITM tersebut. Karena metode LSB menghasilkan Stego-Image yang tidak mengalami perubahan signifikan dari gambar aslinya, maka seseorang MITM tersebut tidak akan mencurigai adanya file dokumen ujian sekolah di dalam gambar yang telah di transfer.

II. METODE PENELITIAN

Jenis penelitian ini merupakan penelitian kuantitatif, yaitu menganalisa pengamanan dari steganografi terhadap file dokumen ujian sekolah. Beberapa tahap yang telah dilakukan dalam pembuatan aplikasi dan perancangan topologi jaringan secara virtual, yaitu:

A. *Analisa Kebutuhan*

Dalam pengembangan aplikasi ini, terdapat beberapa kebutuhan yang perlu dianalisa. Kebutuhan tersebut selanjutnya akan digunakan sebagai bahan untuk membantu pengembangan aplikasi. Analisa kebutuhan dibagi menjadi beberapa bagian, yaitu:

1. Kebutuhan Data

Data yang diperlukan dalam penelitian ini diperoleh dari beberapa referensi. Untuk pengembangan aplikasi steganografi diambil dari literatur yang sumbernya, yaitu jurnal, situs resmi dan sumber dari internet. Dan untuk perancangan topologi jaringan sekolah tersebut di bangun dengan cara melakukan rekayasa virtualisasi jaringan di sekolah. Pengumpulan data pada penelitian ini terbagi menjadi dua jenis, yaitu studi literatur dan observasi.

a.Studi literatur

Pada penelitian ini mengamabil referensi dari berbagai macam literatur yang relevan dengan pengembangan aplikasi tentang steganografi

metode LSB dan metode *Man In The Middle Attack* untuk lebih mendalami pengetahuan tentang hal tersebut. Literatur yang digunakan diantaranya adalah laporan, jurnal, makalah, situs resmi dan sumber dari internet.

b. Observasi

Penelitian ini juga melakukan observasi secara offline dengan mengunjungi sebuah Yayasan Pendidikan Kanzul Ulum untuk mendapatkan file dokumen ujian sekolah sebagai objek penelitian.

2. *Kebutuhan Alat*

Berikut adalah spesifikasi perangkat keras dan perangkat lunak yang diperlukan untuk mendukung penelitian dalam melakukan pembuatan aplikasi steganografi, pembuatan topologi, dan implementasi pendeteksian seorang MITM adalah :

a. Processor Intel Core i5-8300H 2.3 GHz
b. RAM 8 GB
c. Hardisk 1 TB
d. Sistem Operasi Windows 10 64-bit

Sedangkan perangkat lunak yang diperlukan dalam penelitian ini adalah sebagai berikut :

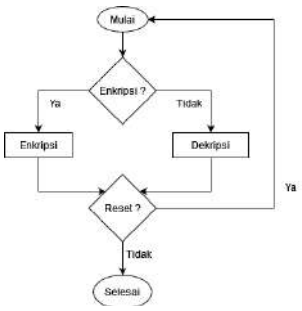
a. MatLab 2016a sebagai media untuk menulis kode progam serta membangun aplikasi steganografi.
b. GNS3 sebagai media untuk merancang topologi jaringan di sekolah secara virtual.
c. Wireshark sebagai alat untuk implementasi penyerangan dengan cara mendeteksi file – file yang ditransfer yang dilakukan oleh seorang MITM.
d. Oracle VM VirtualBox sebagai alat untuk menjalankan komputer virtual yang digunakan saat proses transfer file dari satu komputer ke komputer yang lainnya

B. *Desain Aplikasi dan Topologi Jaringan*

Aplikasi steganografi dan topologi jaringan memiliki rancangan yang akan di buat terlebih dahulu. Rancangan desain aplikasi dan topologi adalah sebagai berikut :

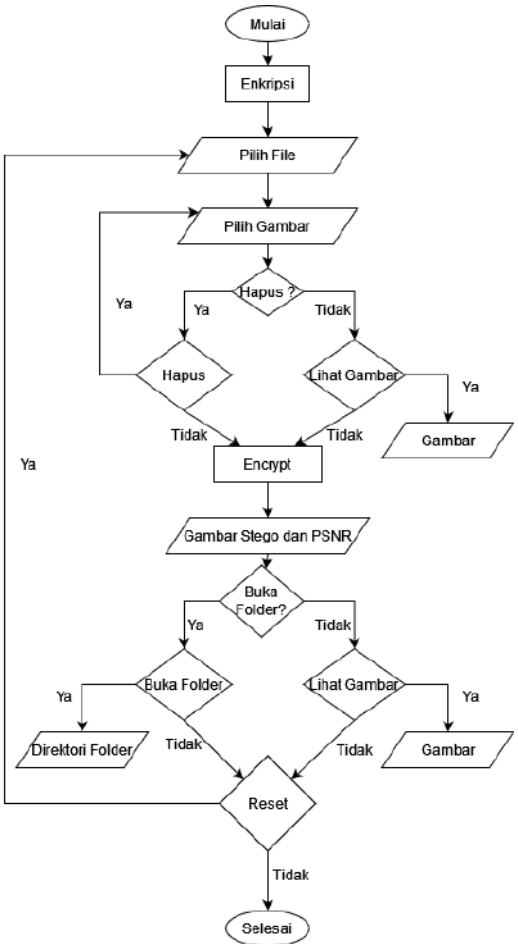
1. *Flowchart*

Flowchart atau bagan alur adalah suatu bagan yang berfungsi untuk menjelaskan suatu alur progam bekerja dari awal hingga akhir progam. Selain itu, *flowchart* juga berfungsi memudahkan orang lain untuk memahami progam tersebut



Gbr 1. Flowchart Progam Steganografi

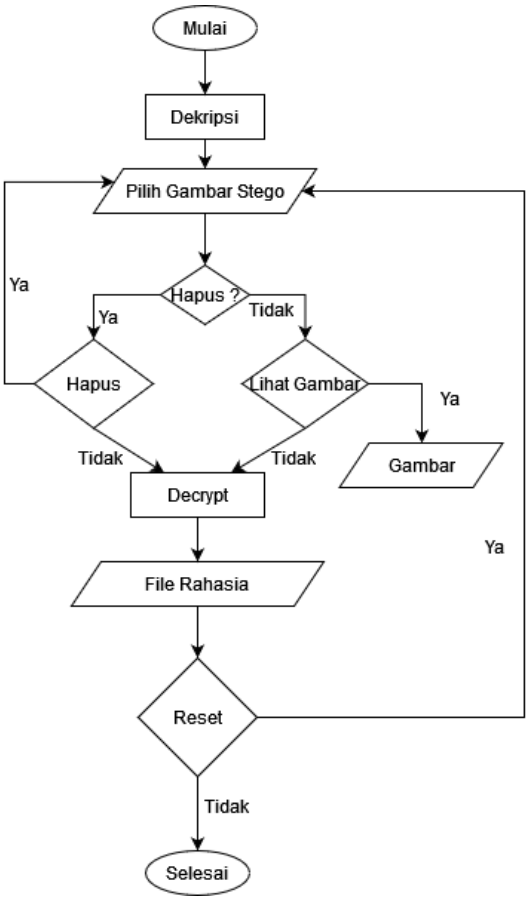
Gambar diatas adalah alur progam atau flowchart dari progam yang akan di buat yaitu progam steganografi. Terdapat dua menu utama yaitu *encrypt* dan *decrypt*. Enkripsi adalah proses untuk memasukkan atau menyatukan sebuah pesan rahasia atau file rahasia ke dalam sebuah wadah media yaitu gambar yang nantinya menjadi sebuah gambar stego yang mirip dengan gambar aslinya. Dekripsi adalah proses untuk mengeluarkan atau mengekstrak file rahasia yang berada dalam sebuah wadah atau gambar stego tanpa merusak isi dari file rahasia tersebut.



Gbr 2. Flowchart menu *encrypt*

Flowchart pada gambar 2 adalah menu *encrypt* dari progam steganografi. Dalam flowchart tersebut bisa dilihat setelah memilih menu *encrypt*, bisa langsung memilih media gambar dan sebuah file dokumen yang akan disisipkan kedalam gambar tersebut. Jika terdapat kesalahan dalam memilih gambar untuk yang nantinya menjadi sebuat media steganografi, terdapat tombol hapus untuk menghapus serta mengganti gambar yang diinginkan dan juga terdapat tombol untuk melihat gambar yang dipilih. Jika gambar dan file dokumen sudah benar maka dilakukan proses enkripsi dengan menekan tombol *encrypt*. Proses enkripsi tersebut dilakukan dengan metode LSB, metode tersebut bekerja dengan cara mengubah sebuah file menjadi bit,

kemudian bit tersebut disipkan kedalam bagian bit kecil dari gambar yang dipilih sebagai *cover*. Setelah bit dari file tersebut disisipkan ke dalam gambar maka dihasilkan sebuah gambar stego yang tidak berbeda jauh secara kasat mata jika dibandingkan dengan gambar aslinya. Selain menghasilkan gambar stego, proses enkripsi tersebut juga menghasilkan rasio PSNR (*Peak Signal to Noise Ratio*) dari gambar asli dan gambar stego. Terdapat tombol untuk melihat gambar stego yang dihasilkan dari proses enkripsi tersebut yang bisa berguna untuk membandingkan antara gambar asli dan gambar stego seberapa jauh perbedaannya tampilannya secara kasat mata dan juga tombol buka folder untuk langsung menuju direktori dimana gambar stego tersebut disimpan. Di bagian bawah menu *encrypt* tersebut terdapat tombol reset yang berguna untuk mereset gambar dan file yang telah selesai dienkripsi sehingga kita bisa memilih gambar dan file yang lain untuk di enkripsi dan juga mereset tampilan gambar stego hasil dari proses enkripsi yang sebelumnya yang muncul di tampilan progam sehingga tampilan pada bagian gambar stego tersebut akan kosong seperti semula ketika baru dibuka.

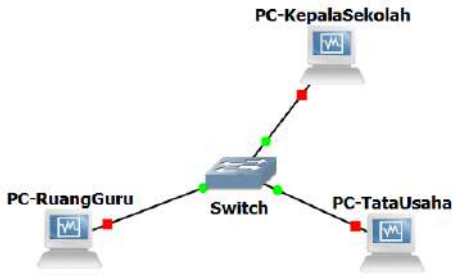


Gbr 3. *Flowchart* menu *decrypt*

Flowchart pada gambar 3 adalah menu *decrypt* dari progam steganografi. Dalam *flowchart* tersebut bisa dilihat setelah memilih menu *decrypt*, bisa langsung memilih gambar stego yang akan di dekripsi. Jika gambar stego yang di masukkan salah, dapat langsung di hapus dan mengganti dengan gambar stego yang benar. Terdapat juga tombol untuk melihat gambar stego yang telah dipilih sebelumnya. Setelah memilih gambar stego yang benar maka dilakukan proses dekripsi dengan menekan tombol *decrypt*. Proses dekripsi menggunakan metode LSB, metode tersebut bekerja dengan cara mendeteksi adanya bit dari sebuah file yang disisipkan ke dalam gambar stego tersebut, kemudian bit tersebut di keluarkan dan di bangun ulang sehingga menjadi file yang sebelumnya disisipkan di proses enkripsi. Proses dekripsi tersebut menghasilkan file rahasia yang sebelumnya di masukkan ke dalam gambar dalam proses enkripsi. Di bagian bawah menu *decrypt* tersebut terdapat juga tombol reset yang berguna untuk mereset gambar stego yang telah selesai di dekripsi sehingga tampilan progam menjadi seperti semula ketika baru di buka.

2. *Topologi Jaringan*

Topologi jaringan adalah suatu metode atau cara yang diterapkan supaya suatu komputer bisa terhubung dengan komputer yang lainnya. Dalam menguhubungkan komputer - komputer tersebut bisa dengan menggunakan kabel atau nirkabel (tanpa kabel).



Gbr 4. Contoh topologi jaringan sekolah

Topologi pada gambar 4 merupakan contoh topologi jaringan yang ada di sekolah yang di rancang secara virtual. Topologi tersebut merupakan topologi star yang dimana semua PC atau komputer yang ada di sekolah terhubung satu sama lain dengan *switch* dan melalui kabel. Di gambar tersebut terlihat bahwa komputer ruang guru, komputer kepala sekolah dan komputer ruang tata usaha terhubung melalui kabel dan terhubungkan satu sama lain ke sebuah *switch*.

C. *Implementasi Sistem*

Setelah merancang sistem dan topologi. Tahap selanjutnya adalah mengaplikasikan hasil rancangan desain aplikasi tersebut untuk melakukan pembuatan aplikasi steganografi di MatLab dan serta membuat topologi jaringan di sekolah secara virtual di aplikasi GNS3.

D. *Pengujian dan Implementasi Penyerangan*

Pada tahap ini, setelah aplikasi selesai dibuat selanjutnya dilakukan pengujian. Pengujian ini dilakukan dengan tujuan

untuk mengetahui dan membuktikan bahwa aplikasi yang sudah dibuat sudah sesuai dengan yang diharapkan dan pengaplikasian steganografi terhadap file dokumen ujian sekolah bisa dibuktikan aman dalam implementasi penyerangan yang dilakukan oleh seorang MITM dengan *software wireshark*.

III. Hasil dan Pembahasan

Setelah aplikasi dibuat, selanjutnya adalah melakukan pengujian aplikasi steganografi terhadap penyisipan file ke dalam sebuah gambar dan implementasi seorang MITM mendeteksi file – file yang dikirimkan dari satu komputer ke komputer lainnya.

A. *Kebutuhan Data*

Setekah melakukan observasi secara offline di Yayasan Pendidikan Kanzul Ulum didapatkan file dokumen ujian sekolah yang bisa digunakan sebagai objek dalam penyisipan file kedalam sebuah gambar dengan steganografi LSB dan implementasi seorang MITM mendeteksi file Ketika ditransfer dari satu komputer ke komputer yang lainnya. Berikut ini merupakan kumpulan file dokumen ujian sekolah yang terdapat pada tabel I.

Tabel I
Tabel File Dokumen soal ujian

No.	File Dokumen Ujian	
	Nama File	**Ukuran**
1	soal_ujian_1.pdf	138,932 bytes
2	soal_ujian_2.pdf	149,155 bytes
3	soal_ujian_3 .pdf	52,254 bytes

B. *Progam Steganografi LSB*

Progam steganografi LSB telah berhasil dibuat sesuai dengan rancangan desain aplikasi, dalam progam tersebut terdapat 2 menu utama yaitu *Encrypt* dan *Decrypt*. Berikut adalah *User Interface* dari progam steganografi yang telah dibuat.

Gbr 5. UI menu *Encrypt*

User Interface pada gambar 5 adalah UI menu *encrypt*. Pada tampilan tersebut terlihat beberapa bagian yaitu gambar asli, pilih file dan gambar stego. Pada bagian gambar asli, terlihat gambar yang telah dipilih sebagai media penyisipan, tombol pilih gambar untuk memilih gambar yang akan dipakai sebagai media penyisipan, lihat gambar yang berfungsi melihat gambar secara jelas, tombol hapus untuk menghapus gambar jika gambar yang diinginkan tidak sesuai dan keterangan direktori dari gambar yang dipilih. Selanjutnya pada bagian file terdapat tombol pilih file yang berfungsi untuk memilih file dokumen yang akan disisipkan serta keterangan direktori dan ukuran dari file dokumen yang dipilih. Terakhir bagian gambar stego yang terdapat gambar stego yang dihasilkan dari proses *encrypt*, tombol buka folder untuk menuju langsung ke folder dimana gambar stego disimpan, tombol lihat gambar untuk melihat gambar stego secara jelas, dan keterangan direktori dimana gambar stego tersebut disimpan. Pada bagian 3 bagian tersebut terdapat tombol *encrypt* yang berfungsi untuk memproses penyisipan file kedalam gambar yang telah dipilih. Pada bagian bawah menu *encrypt* tersebut terdapat tombol reset yang berguna untuk mereset gambar dan file yang telah selesai di enkripsi serta gambar stego hasil proses enkripsi tersebut sehingga tampilan pada menu *encrypt* tersebut akan terlihat seperti semula ketika baru dibuka.

Gbr 6. UI menu *Encrypt*

User Interface pada gambar 6 adalah UI menu *decrypt*. Pada tampilan tersebut terdapat hanya 1 bagian yaitu gambar stego. Pada bagian gambar stego tersebut terdapat tampilan gambar stego yang dipilih, tombol pilih gambar stego untuk memilih gambar stego yang akan di proses, tombol lihat gambar untuk melihat gambar stego secara jelas, tombol hapus untuk menghapus gambar stego yang telah dipilih dan keterangan direktori gambar stego yang dipilih. Di bawah bagian gambar stego terdapat tombol *decrypt* yang berfungsi untuk mengeluarkan file rahasia dari gambar stego yang sebelumnya disisipi file tersebut. Pada bagian bawah menu *decrypt* tersebut terdapat juga tombol reset yang berguna untuk mereset gambar stego yang telah selesai di dekripsi sehingga tampilan progam menjadi seperti semula ketika baru di buka.

C. *Skenario Pengamanan File*

Setelah progam berhasil dibuat langkah selanjutnya adalah selanjutnya melakukan implementasi skenario pengamanan file dokumen ujian sekolah. Berikut adalah tahapan skenario dari pengamanan file dokumen ujian sekolah :

1) Pertama memilih file dokumen ujian sekolah dan sebuah gambar sebagai media yang akan dienkripsi. Proses enkripsi tersebut menghasilkan sebuah gambar stego yang nantinya akan dijadikan objek untuk melakukan implementasi pendeteksian oleh seorang MITM. Berikut adalah hasil dari proses enkripsi dari sebuah gambar asli dengan file dokumen ujian sekolah yang terdapat pada tabel II:

TABEL II
TABEL HASIL PROSES ENKRIPSI

No.	Ukuran Gambar Asli	Ukuran File	Ukuran Gambar Stego	PSNR
1	23,888,010 bytes	138,932 bytes	23,887,926 bytes	64,4482
2	23,888,010 bytes	149,155 bytes	23,887,926 bytes	64,1371
3	23,888,010 bytes	52,254 bytes	23,887,926 bytes	68,6925

Berikut adalah perbandingan tampilan dari gambar asli dan gambar stego:

Gbr 7. Perbandingan gambar asli dan gambar stego hasil proses enkripsi pertama

Gbr 8. Perbandingan gambar asli dan gambar stego hasil proses enkripsi kedua

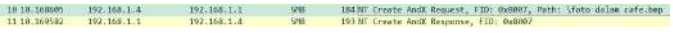
Gbr 9. Perbandingan gambar asli dan gambar stego hasil proes enkripsi ketiga

Dari gambar 7, 8, dan 9 dapat dilihat bahwa gambar asli dan gambar stego tidak ada perbandingan yang mencolok jika dilihat secara kasat mata. Gambar stego tersebut di dapatkan dari hasil enkripsi gambar asli dengan kumpulan file dokumen ujian yang terdapat pada tabel I. Kemudian dari segi perbandingan ukuran file gambar asli dan gambar stego tidak berbeda jauh meski telah disisipi oleh file dokumen ujian sekolah. Yang terakhir adalah dari ketiga proses enkripsi tersebut dihasilkan rasio PSNR seperti pada tabel II, yang artinya jika nilai rasio PSNR tersebut lebih dari 30 maka gambar stego tersebut memiliki kualitas yang baik dan tidak terlihat seperti disisipi oleh sebuah file atau pesan rahasia [12].

2) Langkah selanjutnya adalah mentransfer file dari satu komputer ke komputer yang lainnya. Topologi yang digunakan sama seperti gambar 4 dan dirancang secara virtual di GNS3. Objek yang di gunakan untuk proses transfer ini adalah file dokumen ujian sekolah dan gambar stego yang dihasilkan dari tiga proses enkripsi pada langkah pertama. Objek tersebut di transfer dari komputer di ruang guru ke komputer ruang tata usaha. Proses transfer file ini dilakukan dengan komputer virtual yang di jalankan dengan *software* Oracle VM VirtualBox.

3) Langkah terakhir adalah proses dan hasil seorang MITM mendeteksi file dokumen ujian sekolah dan gambar stego yang saat ditransfer. Seorang MITM tersebut menggunakan *software wireshark* untuk melakukan pendeteksian kedua objek tersebut ketika di transfer Berikut adalah hasil *capture packet* atau mendeteksi paket yang berjalan di *wireshark* tersebut:

Gbr 10. Pendeteksian terhadap gambar stego hasil enksripsi pertama

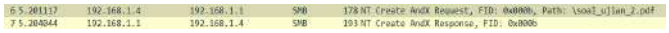


Gbr 11. Pendeteksian terhadap gambar stego hasil enksripsi kedua

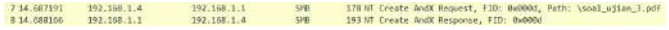
Gbr 12. Pendeteksian terhadap gambar stego hasil enksripsi ketiga

Dari gambar 10, 11, dan 12 dapat dilihat bahwa disaat gambar stego tersebut di transfer, maka yang terlihat hanyalah nama file dan format gambar stego tersebut. Yang artinya seorang MITM yang sedang mendeteksi tidak akan curiga dengan sebuah gambar atau foto tersebut

Gbr 13. Pendeteksian terhadap file soal_ujian_1.pdf



Gbr 14. Pendeteksian terhadap file soal_ujian_2.pdf



Gbr 15. Pendeteksian terhadap file soal_ujian_3.pdf

Dari gambar 13, 14, dan 15 dapat dilihat bahwa disaat file dokumen ujian tersebut di transfer, maka yang nama dan format file dokumen ujian tersebut terlihat jelas. Artinya, ketika seorang MITM akan langsung mengetahui adanya file dokumen ujian yang sedang ditransfer.

Dapat dilihat dari gambar 10 sampai gambar 15 bahwa, jika mentransfer gambar stego seorang MITM tersebut tidak curiga dan aman dan jika mentransfer file dokumen ujian tersebut secara langsung maka seorang MITM akan dengan mudah mengetahuinya. Untuk lebih jelasnya dapat dilihat pada tabel III adalah sebagai berikut :

TABEL IIII
TABEL KESIMPULAN PENELITIAN

Objek yang ditransfer	Ukuran file	Menggunakan Steganografi LSB		Aman dari pendeteksian	
		Iya	Tidak	Aman	Tidak

foto di cafe.bmp yang disisipi soal_ujian_1.pdf	23,887,926 bytes	√		√	
foto dalam cafe.bmp yang disisipi soal_ujian_2.pdf	23,887,926 bytes	√		√	
foto saat di café.bmp yang disisipi soal_ujian_3.pdf	23,887,926 bytes	√		√	
soal_ujian_1.pdf	138,932 bytes		√		√
soal_ujian_2.pdf	149,155 bytes		√		√
soal_ujian_3.pdf	52,254 bytes		√		√

IV. KESIMPULAN

Berdasarkan penelitian yang telah dilaksanakan oleh peneliti, peneliti berhasil membuat progam steganografi dan mengaplikasikan progam tersebut untuk mengenkripsi sebuah file dokumen ujian sekolah ke dalam sebuah media gambar dan menghasilkan sebuah gambar stego. Ukuran dari gambar stego tersebut tidak terlalu besar perbedaannya dengan gambar aslinya dan juga tampilan gambar stego tersebut terlihat mirip dengan gambar asli. Selanjutnya peneliti membuat sebuah implementasi penyerangan seorang MITM dengan cara mendeteksi file – file yang telah di transfer dari satu komputer ke komputer yang lainnya. Topologi yang digunakan adalah topologi star yang di rancang secara virtual di aplikasi GNS3. Setelah topologi sekolah tersebut terbentuk, langkah selanjutnya peneliti melakukan proses transfer file via file sharing. Dan juga peneliti juga yang bertindak sebagai seroang MITM yang akan mendeteksi file – file yang di transfer tersebut. Dalam pengujian pendeteksian tersebut dapat dilihat bahwa file yang ditransfer tersebut terlihat jelas nama file beserta format file tersebut. Hat ini membuktikan bahwa jika kita mentransfer file dokumen ujian sekolah secara langsung tanpa mengemasnya dengan *image steganography*, maka hal tersebut akan bisa diketahui oleh seorang MITM yang sedang mendeteksi pada trafik tersebut. Dan jika sebelum ditransfer file dokumen ujian sekolah tersebut dikemas kedalam sebuah media gambar dengan *image steganograpy*, maka seorang MITM saat mendeteksi akan menganggap hanyalah sebuah gambar yang ditransfer pada trafik tersebut dan terbukti aman.

V. SARAN

Berdasarkan hasil penelitian yang telah dilaksanakan oleh peneliti, peneliti menyarankan untuk menggunakan media steganografi lain seperti media audio dan video. Dan juga menggunakan metode steganografi lainnya.

UCAPAN TERIMA KASIH

Peneliti senantiasa mengucapkan syukur kepada Tuhan YME atas rahmat, hidayah dan pertolongannya sehinhga peneliti dapat menyelesaikan progam dan artikel ilmiah ini dengan baik dan lancar. Terimah kasih di ucapkan kepada kedua Orang tua dan Saudara peneliti yang selalu memberi semangat dan dukungan, kepada Dosen Pembimbing Skripsi yang selalu memberi nasihat, masukan dan saran yang membangun, kepada teman – teman peneliti yang selalu memberi semangat, saran dan dukungan yang positif sehingga pengerjaan proyek dan artikel menjadi lancar dan cepat.

REFERENSI

[1] Pratiwi, dan Dwi Atmodjo WP. 2016. Peningkatan Keamanan Data dengan Metode *Cropping Selection Pseudorandom*. Jurnal TICOM, Vol.4, No. 3, Mei..

[2] Thabit, Fursan, Sharaf Alhomdy, Abdulrazzaq H.A. Al-Ahdal, dan Shudir Jagtap. 2021. *A new lightweight cryptographic algorithm for enhancing data security in cloud computing*. Global Transitions Proceedings, Volume 2, Issue 1, Pages 91-99, June 2021

[3] Sakti, Nur. 2018. Sistem Keamanan Data Menggunakan Algoritma Kriptografi *Blowfish* Pada Aplikasi Chatting. Jurnal Ilmiah Sistem Informasi dan Teknik Informatika "JISTI", Vol. 1, No. 1, April 2018..

[4] Arief, Muhammad, Fitriyani, dan Nurul Ikhsan. 2015. Kriptografi RSA pada Aplikasi *File Transfer Client – Server Based*. Jurnal Ilmiah Teknologi Informasi Terapan (JITTER) Volume I, No 3, 10 Agustus 2015.

[5] Mallik, Avijit, Abid Hasan, Mhia Md, Zaglul Sahadat, dan Jia-Chi Tsou. 2018. *Man in the Middle Attack : Understanding in Simple Words*. International Journal of Data and Network Science 3, 77–92.

[6] Y. Desmedt, *Man-in-the-middle attack, in: Encyclopedia of cryptography and security, Springer*, 2011, 759–759.

[7] Wahanani, Heni Indah, Firza Prima Aditiawan, dan Retno Mumpuni. 2020. Uji Coba Serangan *Man in the Middle* Pada Keamanan SSL Protokol HTTP. Jurnal Sistem Informasi dan Bisnis Cerdas (SIBC), Vol. 13, No. 1, Februari 2020.

[8] Hasugian, Buyung Solohin. 2017. Peranan Kriptografi Sebagai Keamanan Sistem Informasi pada Usaha Kecil dan Menengah. Jurnal Warta Edisi : 53, Juli 2017.

[9] Halunen, Kimmo, dan Outi-Marja Latvala. 2020. *Review of the use of human senses and capabilities in cryptography*. Computer Science Review, Volume 39, 100340, Februari 2021.

[10] Shah, Pratik D., Rajankumar S.Bichkar. 2020. *Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure*. Engineering Science and Technology, an International Journal, Volume 24, Issue 3, Pages 782-794, June 2021.

[11] Damanik, Hilman Akhyar, Merry Anggraeni. 2017. Techniques for Text Data Security Testing Increased by LSB Steganography Method and Encryption Enginering. Jurnal Penelitian Pos dan Informatika, Vol.08 No 02 : hal 109- 122, Desember 2018.

[12] Pamungkas, Adi. 2017. Cara Menghitung Nilai MSE, RMSE, dan PSNR pada Citra Digital, https://pemrogramanmatlab.com/2017/06/04/cara-menghitung-nilai-mse-rmse-dan-psnr-pada-citra-digital/. Diakses pada 10 Oktober 2021 pukul 14.00 WIB