KEAMANAN DATA MENGGUNAKAN METODE LSB DAN ENKRIPSI VIGENERE

Thomas Karel Watimena, Mufti

Program Studi Teknik Informatika, Universitas Budi Luhur
Jl. Ciledug Raya, Jakarta Selatan
thomaz300890@gmail.com, muftykayat@gmail.com

Abstract - Security in the delivery of a document is a very important thing in a company. Important documents if read by irresponsible parties become a huge misfortune. To disguise a document that you want to send can use the media of an image. The document is inserted into an image by utilizing the LSB (Least Significant Bit) method and for the next security the contents of the document are encrypted using the Vigenere algorithm. The results of the study showed that the larger the image size, the larger the size of the document to be sent.
Keywords - Document, Vigenere, LSB.

Abstrak - Keamanan dalam pengiriman sebuah dokumen merupakan hal yang sangat penting dalam sebuah perusahaan. dokumen yang penting jika dibaca oleh pihak yang tidak bertanggung jawab menjadi musibah yang sangat besar. Untuk menyamarkan sebuah dokumen yang ingin dikirim dapat menggunakan media sebuah gambar. Dokumen tersebut disisipkan kedalam sebuah gambar dengan memanfaatkan metode LSB (Least Significant Bit) dan untuk keamanan berikutnya maka isi dokumen di enkripsi menggunakan algoritma vigenere. Hasil dari penelitian menunjukan bahwa semakin besar ukuran gambar maka semakin besar pula ukuran dokumen yang akan dikirim.
Kata kunci – Dokumen, Vigenere, LSB.

I. PENDAHULUAN

Pengiriman dokumen yang berisi data rahasia sebuah perusahaan dari unit atau cabang ke perusahaan pusat menjadi hal yang wajib dilakukan setiap periode baik itu setiap bulan, setiap minggu atau setiap hari nya. Untuk menjaga dokumen sampai kepada orang yang dituju maka diperlukan sebuah metode atau cara untuk mengamankannya. Metode LSB atau least significant bit adalah sebuah cara menyisipkan dokumen kedalam sebuah gambar sehingga jika dokumen tersebut diterima oleh orang yang tidak berkepentingan maka hanya berupa gambar, namun jika gambar tersebut diterima oleh orang yang dituju maka gambar tersebut dapat diekstrak menjadi 2 buah file yaitu gambar dan dokumen. Dan untuk mengantisipasi jika dokumen tersebut dapat dibuka oleh pihak yang tidak bertanggung jawab maka isi dari dokumen tersebut akan di enkripsi menggunakan algoritma vigenere, sehingga isi file menjadi sebuah aksara yang tidak beraturan. Hasil riset atau penelitian mampu membantu perusahaan cabang atau unit dalam melaporkan data perusahaan cabang kepada perusahaan pusat. Penelitian serupa juga telah dilakukan oleh fino ardiansyah prayudi dan agus prihanto [1] yang berjudul Penerapan Algoritma Least Significant Bit Untuk Menyembunyikan Vigenere Cipher Text pada Citra Digital. pada penelitiannya tersebut menguji 3 jenis gambar dengan ukuran data teks sebesar 10kb, 50kb, 100kb dan 340kb. hasil PSNR (Peak Signal Noise Ratio) menunjukan angka diatas 40%. hal ini menunjukan bahwa metode lsb berhasil dan baik dalam pengimplementasiannya. Adapun penelitian yang lain juga dilakukan oleh Niria laila dan Anita Sindar RMS [2] yang berjudul Implementasi Steganografi Lsb Dengan Enkripsi Vigenere Cipher Pada Citra. pada penelitian tersebut jenis file yang dapat digunakan sebagai media carier adalah bitmap (BMP) dan JPEG. dan ukuran file citra dibatasi pada ukuran minimal 100 x 100 pixel, dan maksimal 2048 x 1024 piksel. dan ukuran pesan hanya berformat .txt serta Penelitian yang berbeda dilakukan oleh Yudhi Ardian [3] dengan judul "Perbandingan Metode LSB,LSB+1,dan MSB Pada Steganografi Citra Digital". Dimana hasil dari teknik steganografi citra hasil dengan metode LSB(Least Significant Bit) gambar yang sudah disisipkan pesan tidak terlihat berbeda dengan gambar aslinya dan citra hasil dengan metode LSB (Least Significant Bit) +1 yang sudah disisipkan pesan tidak terlihat berbeda dengan gambar aslinya tetapi letak penyisipannya berbeda dengan metode LSB (Least Significant Bit) biasa. Sedangkan citra hasil dengan menggunakan metode MSB(Most Significat Bit) gambar yang sudah disisipkan pesan dengan gambar aslinya terlihat sangat berbeda dan letak penyisipannya juga berbeda.

A. Steganografi

Kata Steganografi dapat diartikan seni dan ilmu dalam menulis ataupun dalam menyembunyikan sebuah kata-kata ataupun pesan yang disembunyikan dengan sebuah teknik tertentu sehingga tidak seorang pun yang mengetahuinya bahwa ada pesan yang tersembunyi selain pengirim[4]. kata steganografi berawal dari sebuah bahasa bangsa Yunani, yaitu steganos yang memiliki arti penyamaran sedangkan graphein memiliki arti tulisan. Sehingga kata

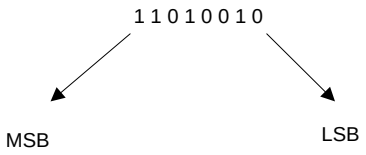
steganografi dapat diartikan sebuah seni yang dapat menyamarkan ataupun menyembunyikan kata-kata ataupun pesan tertulis [5]

B. Kriptografi

Kata Kriptografi dapat diartikan dengan ilmu yang terkait dengan matematika dan aspek dalam keamanan sebuah informasi seperti data-data yang rahasia, data yang benar-benar valid dan absah, serta autentifikasi sebuah data. [6] dan dapat diartikan juga seni serta ilmu dalam menjaga keamanan serta kerahasian pesan. Kata ”seni” pada kalimat awal menunjukan kenyataan dari sejarah awal dari masa-masa kriptografi. Karena tiap-tiap orang memiliki cara yang unik didalam menyampaikan sebuah pesan [7]

C. Proses LSB

Pada proses penyempunyian pesan menggunakan metode LSB dilakukan dengan cara menyisipkan pesan yang akan dikirimkan pada bit rendah yang terletak pada paling kanan pada pixel image yang akan menyusun file pesan tersebut [8]. Pada sebuah bitmap 24 bit akan terdiri dari sebuah susunan warna. Warna tersebut berjumlah tiga yaitu merah, hijau serta biru. dan terdiri atas 8 bit bilangan integer dimulai dari 0 hinga 255. Sedangkan jika dalam bentuk biner yaitu 00000000 sampai dengan 11111111. pada sebuah bentuk bit terdapat bit yang paling penting dan berarti yaitu most significant bit atau MSB, sedangkan bit yang kurang berarti disebut dengan least significant bit atau LSB dapat dilihat pada bentuk gambar biner 8 bit seperti berikut.



Gambar 2. Most Significant Bit (MSB) dan Least Significant Bit (LSB)

Pada penelitian ini bit yang digunakan adalah bit least significant bit (LSB) hal ini dipilih karena bentuk perubahan yang terjadi hanya mengubah sebuah nilai byte ke bentuk yang lebih tinggi atau lebih rendah dari bentuk nilai yang sebelumnya[9]. sebagai contoh jika bentuk byte menyatakan warna merah, maka bentuk perubahan satu buah bit LSB tidak akan mengubah dari warna merah secara berarti dan juga jika dilihat dari mata manusia maka tidak akan dapat membedakan perubahan yang kecil tersebut. karena pada intinya bentuk dari gambar bitmap adalah sekumpulan dari titik-titik yang umum disebut pixel.[10] pada tiap-tiap gambar maka pixelnya adakan berbeda-beda.

Contoh akan menyisipkan karakter R, maka pertama-tama adalah mengkonversi karakter R tersebut kedalam sebuah bentuk biner, adapun bentuk biner dari R adalah 01010010 dan jika dalam bentuk ASCII [11] maka bernilai 82. Pada contoh berikut ini adalah bentuk Segmen dari citra sebelum disisipkan

(0 0 1 0 0 1 1 1 1 1 1 0 1 0 0 1 1 1 0 0 1 0 0 0) (0 0 1 0 0 1 1 1 1 1 0 0 0 1 0 0 0 1 1 1 0 1 0 0 1) (1 1 0 0 1 0 0 0 0 0 1 0 0 1 1 1 1 1 1 0 1 0 0 1)

Dan bentuk Segmen citra sesudah disisipkan karakter R adalah sebagai berikut

(0 0 1 0 0 1 1 **0** 1 1 1 0 1 0 0 **1** 1 1 0 0 1 0 0 **0**) (0 0 1 0 0 1 1 **1** 1 1 0 0 1 0 0 **0** 1 1 1 0 1 0 0 **0**) (1 1 0 0 1 0 0 **1** 0 0 1 0 0 1 1 **0** 1 1 1 0 1 0 0 1)

setelah melihat bentuk perubahan yang terjadi pada segmen citra yang ada pada sejumlah bit-bit yang terletak diposisi kanan setelah disisipkan biner karakter R yaitu 01010010. dapat dilihat bahwa perubahan bit yang terjadi hanya bit yang terletak diposisi paling kanan dari 8 bit yang ada. untuk menyisipkan pesan dalam image dengan metode LSB hanya dapat menyimpan sebuah informasi dengan keterbatasan ukuran. sebagai contoh jika terdapat sebuah citra dengan ukuran 24 bit. dan bentuk dari RGB yaitu (R=8 bit, G=8 bit dan B=8 bit) akan digunakan sebagai media untuk menyimpan sebuah data yang berukuran 100 bit, maka setiap pixelnya dapat menyimpan 3 bit informasi sehingga wadah yang dibutuhkan untuk menampung setidaknya berukuran 34 pixel. sehingga ukuran bit adalah 34 x 3 x 8 = 816 bit atau 8 kali lipat dari ukuran aslinya. sehingga untuk menyimpan informasi maksimum berukuran 1/8 dari bentuk citra penampung tersebut.

Secara umum proses proses enkripsi dilakukan dengan menggunakan algoritma Vigenere Cipher terhadap file yang akan disisipkan ke dalam citra bitmap. Sedangkan penyisipan data dilakukan dengan menggunakan metode LSB dengan menggantikan bit-bit LSB pada citra bitmap dengan data hasil proses enkripsi. Pada proses pengungkapan data, proses yang terjadi adalah mengambil, mengumpulkan dan menggabungkan sejumlah nilai dari bit-bit LSB pada citra yang mengandung pesan rahasia. Kemudian nilai-nilai yang telah diperoleh dari proses pengungkapan data akan di dekripsi dengan menggunakan algoritma Vigenere.

D. Proses Enkripsi Dan Penyisipan Data

Aplikasi yang dihasilkan dalam penelitian ini berfungsi sebagai penyembunyian pesan atau informasi dapat berupa data teks ataupun gambar. pada contoh penelitian ini bentuk media yang digunakan adalah bentuk bitmap. untuk menampung pesan informasi dalam objek stego yakni berupa citra bitmap yang pastinya memerlukan sebuah bentuk algoritma untuk memodifikasi bentuk objek stego tersebut. sehingga hasilnya ada bentuk image yang baru yang didalamnya terdapat pesan atau informasi yang disembunyikan yang disebut embedding. pada proses memodifikasi citra yang telah tergabung tidak boleh terlalu mencolok jika dilihat secara kasat mata, dimana perubahan pada

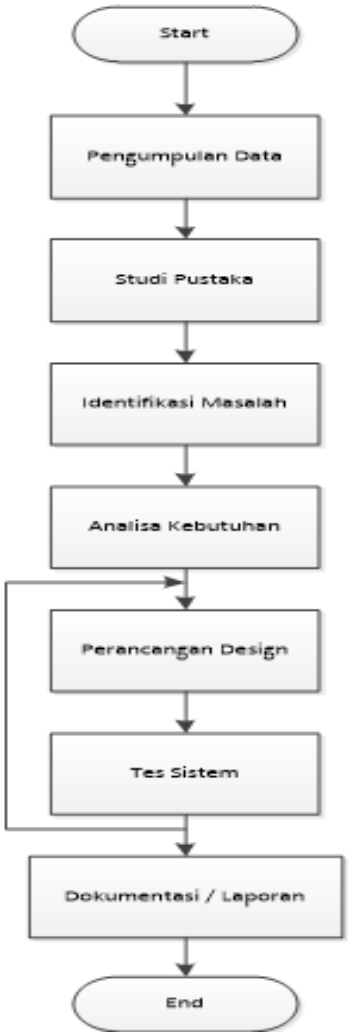
citra penampung yang telah termodifikasi tidak terlalu terlihat. Agar suatu kerahasiaan pesan informasi yang terkandung dalam objek citra penampung tetap terjaga (integrity), maka pesan informasi tersebut sudah di enkripsi terlebih dahulu dengan metode kriptografi sebelum pesan informasi tersebut disembunyikan ke dalam objek citra penampung. Dengan terenkripsinya pesan informasi tersebut, kerahasiaannya tetap terjaga meskipun ada pihak-pihak yang tidak berwenang mendapatkan pesan informasi yang terkandung dalam citra penampung karena pesan informasi tersebut tidak memiliki makna dan harus didekripsi terlebih dahulu agar dapat diketahui isi dari pesan informasi tersebut. Untuk menghasilkan objek citra yang sudah dimodifikasi yang berisi pesan informasi rahasia, yang disebut dengan istilah stego data/stego file [12], yang dibutuhkan adalah media penampung berupa citra bitmap, pesan informasi rahasia berupa data teks, kunci enkripsi berupa sandi algoritma Vigenere dan metode LSB.

E. Algoritma Ekstraksi File

Pada saat pengambilan pesan informasi yang terdapat pada stegodata maka dibutuhkan sebuah proses ekstraksi data berupa algoritma pendeteksi dan kunci enkripsi. Algoritma untuk mengecek atau pendeteksi tersebut kebalikan dari metode embedding, jika metode embedding berguna untuk memasukan pesan rahasia kedalam bentuk image maka metode atau algoritma pendeteksi berguna untuk mengambil sebuah pesan dari bentuk image. Algoritma steganografi ini memodifikasi beberapa pixel yang terdapat di dalam file citra bitmap. didalam masing-masing pixel yang terdapat pada file citra bitmap terdapat bentuk intensitas nilai dari tiga warna dasar yaitu R G B atau Red Green Blue. sehingga pada suatu bentuk pixel adalah kombinasi intensitas atas ketiga warna itu. sebuah warna memiliki intensitas nilai 0 - 255. dan setiap warnanya terdapat 8 bit atau 1 byte. sehingga pada 24 bit terdapat 8 bit warna merah, 8 bit warna hijau serta 8 bit warna biru [13] pada sebuah informasi yang diwakili 8 bit ini terdapat pengelompokan-pengelompokan bit. sebagai contoh misal ada 1 buah byte informasi yang terdapat bit 10111001 dapat kita lihat bit yang terletak paling depan adalah bit yang sangat paling berpengaruh pada informasi yaitu angka 1 yang disebut Most Significant Bit atau MSB. [14] posisi yang terletak akhir memiliki pengaruh yang kecil atau disebut dengan Least Significant Bit (LSB). algoritma steganografi dengan metode Least Significant Bit (LSB) ini diproses dengan cara mengganti bit-bit yang termasuk kedalam bit LSB .nilai pada bit LSB ini nantinya akan digantikan dengan bit-bit informasi yang hendak disembunyikan [15] Setelah berhasil menggantikan bit-bit yang ada pada posisi LSB, maka pesan atau informasi berhasil disembunyikan. Dan jika pesan atau informasi rahasia itu hendak dibuka kembali, maka bit-bit yang ada pada posisi LSB tersebut diambil satu persatu dan digabung kembali sehingga menjadi sebuah informasi, metode ini disebut dengan ekstraksi data.

II. METODE PENELITIAN

Pada penelitian ini menggunakan metode sebagai berikut :



Gambar 1. Metode Penelitian

a. Pengumpulan Data
   Pada tahap ini adalah mengumpulkan data-data dari sebuah pokok permasalahan dari topik yang diangkat oleh penulis, yaitu dengan Observasi yang terdiri dari wawancara
b. Studi Pustaka
   Setelah data – data yang dibutuhkan terkumpul, selanjutnya adalah mencari data atau fakta yang real melalui studi pustaka
c. Identifikasi Masalah
   Dari data nyata yang tekumpul maka selanjutnya dapa diidentifikasi suatu masalah dan permasalahannya yang ada dengan pembatasan
d. Analisa Kebutuhan
   Dari hasil identifikasi masalah yang diatas, selanjutnya baru dapat dilakukan analisa kebutuhan

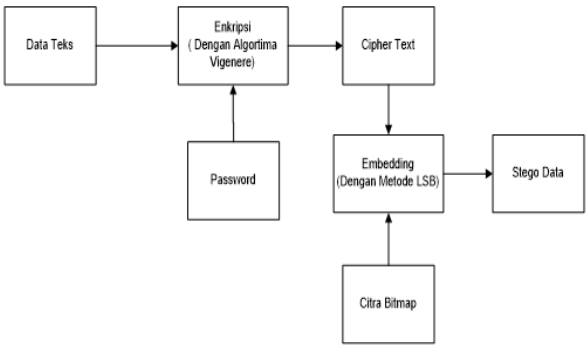
yang menunjang dalam perancangan system steganografi dan kriptografi ini berdasarkan tinjauan pustaka, yaitu meliputi kebutuhan materi stegano dan kriptografi, teori perancangan sistem atau program yang interaktif serta template atau platform dimana perancangan akan dilakukan

e. Perancangan Desain
Pada tahap ini adalah merancang tampilan tatap muka pengguna yang mudah digunakan menurut kaidah interaksi manusia dengan komputer dan konten-konten yang ada didalamnya seperti, struktur menu, tombol.

f. Tes Sistem
Pada tahap ini adalah mengujikan apa saja yang telah diteliti kemudian dirancang kedalam bentuk model program. Jika belum sesuai dan atau masih ada kekurangan dalam perancangan model program ini dapat ditambah dalam rancangannya bahkan dirancang ulang pada tahap perancangan disain untuk mendapatkan hasil yang sesuai

g. Dokumentasi / pembuatan Laporan
Tahap dokumentasai atau pembuatan laporan adalah memaparkan hasil penelitian yang dilakukan dari tahap awal hingga akhir dan diimplementasikan kedalam bentuk laporan jurnal.

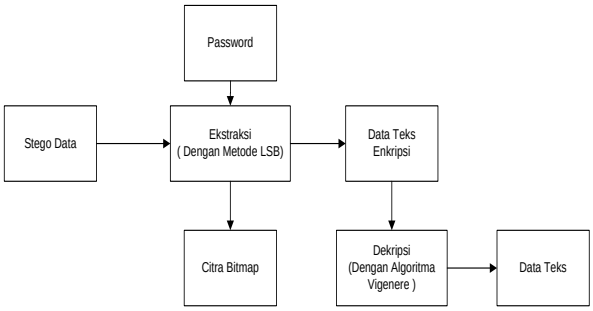
Adapun proses penyembunyi File Pada Citra Bitmap atau steganografi dapat dilihat pada gambar 3 berikut ini.



Gambar 3. Bagan Proses Penyembunyi File Pada Citra Bitmap

Dari gambar diatas dapat dilihat proses enkripsi menggunakan algoritma Vigenere dimulai dari pilih data teks, kemudian teks tersebut di enkripsi menggunakan algoritma vigenere dan masukan password enkripsi sehingga menjadi cipher text. Kemudian untuk proses stegano, langkah pertama adalah pilih image yang akan dijadikan media carrier, kemudian gabung cipher text dengan gambar tersebut. Hasil penggabungan gambar dengan cipher text menjadi stego data.

Sedangkan proses ekstraksi file dapat dilihat pada gambar 4 berikut.



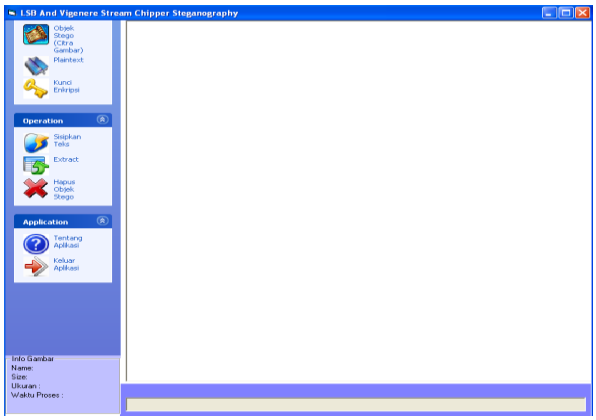
Gambar 4. Bagan Proses Ekstraksi File Pada Citra Bitmap

Pada gambar 4 dapat dilihat untuk mengekstraksi data dimulai dari memilih stego data (image yang berisi pesan yang disembunyikan) kemudian masukan password untuk membuka pesan yang dienkripsi. Kemudian pisahkan gambar dengan pesan.

III. HASIL DAN PEMBAHASAN

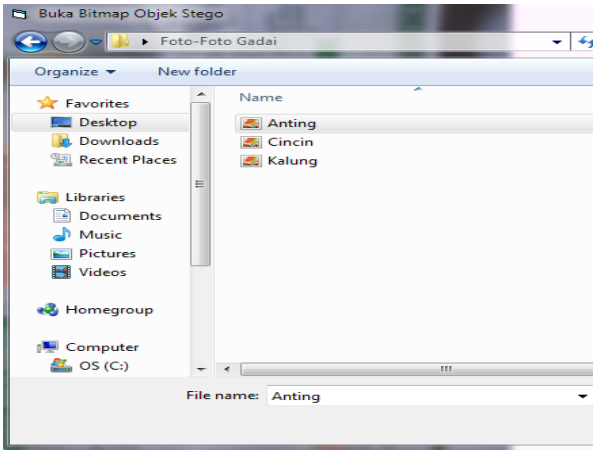
A. Proses Steganografi.

Proses awal adalah dengan memilih object gambar yang akan di jadikan media untuk mengirimkan pesan. Kemudian pilih pesan yang akan kirim, kemudian masukan kunci enkripsi text. Untuk menu utama aplikasi akan berisi keseluruhan fungsi yang terdapat pada proses steganografi dan kriptografi seperti gambar 5 berikut.

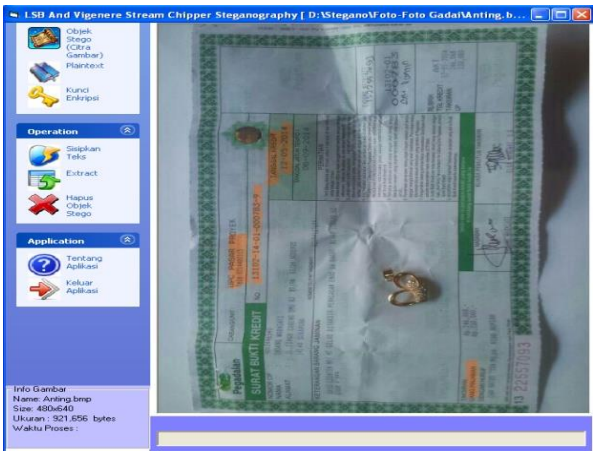


Gambar 5. Menu Utama Aplikasi

Langkah pertama untuk memulai langkah steganografi adalah memilih gambar yang akan dijadikan media pengirim pesan. Adapun pemilihan gambar seperti gambar 6 berikut.

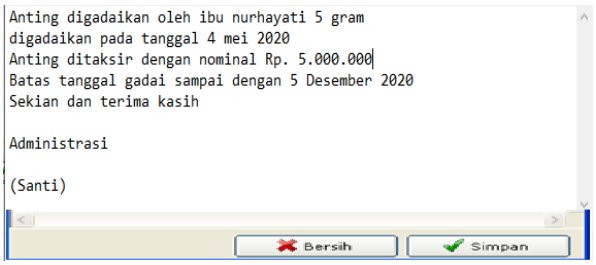


Gambar 6. Pemilihan Lokasi Gambar



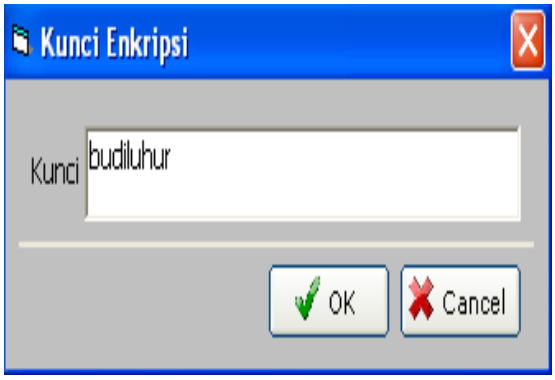
Gambar 7. Tampilan Gambar Yang Berhasil Di Ambil

Langkah berikutnya adalah memasukan pesan yang akan dikirimkan kepada penerima pesan, seperti gambar 8 berikut



Gambar 8. Pesan Yang Akan Disisipkan

Kemudian setelah pesan yang akan dikirim telah disimpan, maka tahap berikutnya adalah memasukan kata kunci untuk mengenkripsi pesan agar pesan tidak dapat dibaca oleh pihak yang tidak diinginkan, seperti pada gambar 9 berikut



Gambar 9. Kunci Enkripsi

Setelah memasukan kunci enkripsi, maka terakhir adalah menggabung gambar dengan pesan yang akan dikirim. Hasil penggabungan gambar dengan pesan seperti gambar 10 berikut ini

Gambar 10. Gambar Hasil Gabung

Jika ingin melihat pesan yang telah dienkripsi maka dapat dilihat pada gambar 11 berikut.

Gambar 11. Text Yang Dienkripsi

B. Tabel Perbandingan

Tabel perbandingan digunakan untuk mengecek apakah terjadi perubahan ukuran data sesudah enkripi dan sesudah dekripsi serta ukuran file aslinya.

Tabel 1. Enkripsi Data

Plaintext	Besar (byte)	Ciphertext	Besar (byte)	Waktu proses
Test.txt	2 Kb	Hasil	2 Kb	5 Detik
File 5 Kb	5 Kb	Cipher 5 Kb	5 Kb	12 Detik
File 44 Kb	44 Kb	Cipher 44 Kb	44 Kb	35 Detik
File 10 KB	10 Kb	Cipher 10 Kb	10 Kb	25 Detik

Dari hasil tabel 1 dapat disimpulkan bahwa tidak terdapat perbedaan ukuran sebuah data ketika data tersebut digabung kedalam sebuah image.

Tabel 2. Dekripsi data

Ciphertext	Besar (byte)	Plaintext	Besar (byte)	Waktu proses
Cipher 2 Kb	2 Kb	Hasil Plaintext 2 Kb	2 Kb	12 Detik
Cipher 5 Kb	5 Kb	Hasil Plaintext 5 Kb	5 Kb	70 Detik
Cipher 44 Kb	44 Kb	Hasil Plaintext 44 Kb	44 Kb	601,200 Detik
Cipher 10 Kb	10 Kb	Hasil Plaintext 10 Kb	10 Kb	145 Detik

Dari tabel 2 dapat disimpulkan bahwa waktu yang diperlukan untuk mengektrak sebuah image memerlukan waktu yang lebih lama daripada ketika menggabungkan image dengan data.

IV. KESIMPULAN

Berdasarkan penelitian, implementasi dan pengujian, maka dapat diambil kesimpulan sebagai berikut :

1. Dengan menggunakan metode Least Significant Bit (LSB), penyisipan data kedalam media citra yang digunakan sebagai wadah penampung (cover) tidak terlalu mempengaruhi kualitas dari citra tersebut bila dilihat secara kasat mata
2. Semakin besar ukuran media citra yang digunakan maka semakin baik dan semakin besar pula kapasitas atau ukuran penyembunyi datanya
3. Dari Data pengujian pertama sampai pengujian ke empat, perbandingan ukuran data media citra tanpa data dan ukuran media citra dengan data memiliki perbandingan ukuran yang sama sebesar 2 byte. Begitu pula dengan ukuran file yang akan disisipkan dan ukuran file yang telah diekstraksi juga memiliki perbandingan ukuran sekitar 2 – 3 KB.
4. Penggabungan teknik steganografi dan kriptografi dapat dilakukan dengan cara mengenkripsi file yang akan disisipkan sebelumnya, kemudian hasil proses enkripsi (chiphertext) disisipkan ke dalam media citra. Dan sebaliknya untuk memperoleh data dari media citra, pertama kali dilakukan proses ekstraksi data dari media citra kemudian data didekripsi kembali.
5. Untuk penelitian kedepannya enkripsi bisa ditambahkan dengan penggabungan metode lainnya seperti RSA, Blowfish, Base64 dan yang lainnya

DAFTAR PUSTAKA

[1] F.A. Prayudi and A. Prihanto, "Penerapan Algoritma Least Significant Bit Untuk Menyembunyikan Vigenere Cipher Text pada Citra Digital,"*Journal of Informatics and Computer Science*, vol. 1, pp. 144–149, 2020.

[2] N. Laila and A. S RMS. "Implementation of LSB Steganography with Vigenere Cipher Encryption in Image". *Computer Science Informatics Journal* Vol. 1, No. 2, 2018. pp. 47- 58.

[3] Y Andrian, "Perbandingan metode LSB, LSB+1, dan MSB pada steganografi citra digital,"Seminar Nasional Ilmu Komputer (*SNIKOM*) *2013.* STMIK potensi Utama. Medan.

[4] A. Ardiansyah and M. Kurniasih. "Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganograpi Menggunakan Metode Least Significant Bit". *Jurnal Teknologi Informasi*, Vol XIII Nomor 3, pp. 96 - 101, 2018.

[5] Irfan, "Penyembunyian Informasi (Steganography) Gambar Menggunakan Metode LSB (Least Significant Bit)". *Rekayasa Teknologi*. Vol. 5, No.1, pp. 1 - 6. 2013.

[6] R.A. Megantara and F.A. Rafrastara. "Super Enkripsi Teks Kriptografi Menggunakan Algoritma Hill Cipher Dan Transposisi Kolom". *Prosiding SENDI_U*. pp. 85-92. 2019.

[7] P. H. Arjana. dkk. "Implementasi Enkripsi Data Dengan Algoritma Vigenere Chiper". *Seminar Nasional Teknologi Informasi dan Komunikasi*. pp.164-169. 2012.

[8] R.S Basuki and E.N Maranggani. "Embedding Pesan Rahasia Di Dalam Suatu Gambar Dengan Metode Least Significant Bit Insertion (LSB)". *Seminar Nasional Teknologi Informasi & Komunikasi Terapan*. pp. 1 -5. 2011.

[9] K.A. Sekarwati and A.Budiman. "Implementasi Algoritma Rivest-Shamir-Adleman (Rsa) Dan Metode Least Significant Bit (LSB) Untuk Keamanan File Teks Dan Dokumen Menggunakan Visual C#". J*urnal Teknologi Rekayasa* Volume 22 No.1, pp. 54-62. 2017..

[10] DA. Prabowo, dkk. "Deteksi Dan Perhitungan Objek Berdasarkan Warna Menggunakan Color Object Tracking". *Jurnal Pseudocode*, Volume V. Nomor 2. pp. 85-91. 2018.

[11] Zulfidar and A. Fauzi. "Implementasi Pengamanan Data Menggunakan Enkripsi Caesar Cipher Dengan Kombinasi Tabel ASCII". *Seminar Nasional Teknologi Informasi dan Multimedia*. STMIK AMIKOM Yogyakarta, 2014.
[12] D. Gustina and A. Sumbaryadi. "Pembuatan Aplikasi Steganografi Pada Citra Digital". *Jurnal Sistem Informasi*. pp. 20-27. 2018.
[13] B. Wilkinson and M. Allen. "Parallel Programming-Teknik dan Aplikasi menggunakan jaringan workstation & Komputer paralel". Andi Publisher. Yogyakarta, 2010.
[14] Darmayanti, K. A Harsa, "Sistem Steganografi Pada Citra Digital Menggunakan Least Significant Bit", *Prosiding Seminar Sains dan Teknologi FMIPA Unmul* Vol. 1 No. 1 Juli 2016
[15] R.N Ibrahim, Ilham M.S, "Perancangan Aplikasi Stegakrip Dengan Metode Lsb Dan Algoritma Rsa Berbasis Web", *Jurnal Computech & Bisnis*, Vol. 11, No 1, , 98-109, Desember 2017.