# Kemanan Data Menggunakan Metode LSB dan Enkripsi Vigenere

**Thomas Karel Wattimena[1], Mufti[2]**
[1,2] Teknik Informatika, Teknologi Informasi, Universitas Budi Luhur,
[1,2]Jl. Kenanga no.11, Jakarta pusat
Email: [1]*thomaskarel@gmail.com*, [2]*muftikayat@gmail.com*

***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.*

***Abstrak***

*Security in the delivery of a document is a very important thing in a company. Important documents if read by irresponsible parties becomes 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. 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.*

## 1. PENDAHULUAN

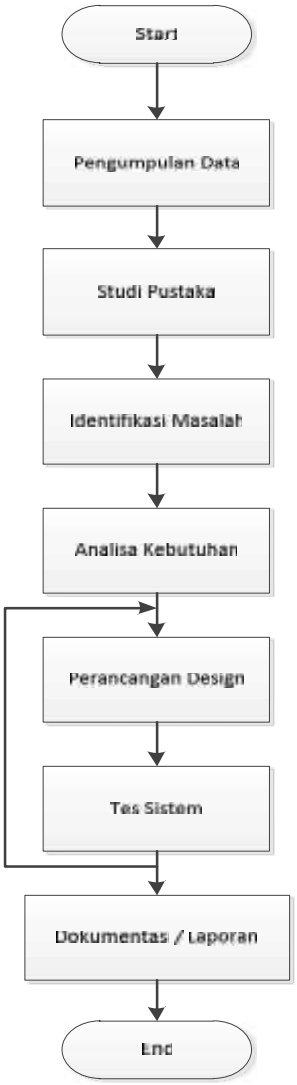
Pengiriman dokumen yang berisi data rahasia sebuah perusahaan dari unit atau cabang ke perusahaan pusat menjadi hal yang wajib dilakukan setiap periode baik itu setiap bulan, setiap minggu atau setiap hari nya. Untuk menjaga dokumen sampai kepada orang yang dituju maka diperlukan sebuah metode atau cara 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

## 2. METODOLOGI PENELITIAN

### 2.1 Metode pada 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.

## 2.1 Steganografi

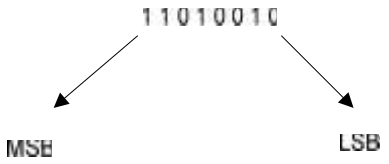
Steganografi merupakan seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan cara tertentu sehingga selain si pengirim dan si penerima, tidak ada seorang pun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia.[4] Istilah steganografi (steganography) berasal dari bahasa Yunani, yaitu steganos yang berarti penyamaran atau penyembunyian dan graphein yang berarti tulisan. Jadi steganografi bisa diartikan sebagai seni menyamarkan/ menyembunyikan pesan tertulis ke dalam pesan lainnya [5]

## 2.2 Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentifikasi data. [6] serta dapat diartika seni dan ilmu untuk menjaga keamanan pesan. Kata ”seni” di dalam definisi di atas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan [7]

## 2.3 Proses LSB

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. [8] Seperti kita ketahui untuk file bitmap 24 bit maka setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna yaitu 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 Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti (least significant bit atau LSB) Terlihat pada Gambar berikut yang mengambarkan contoh nilai biner pada 8 bit.




Gambar 2 *most significant bit* (MSB) dan *least significant bit* (LSB)

Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. [9] Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti, dan mata manusia tidak dapat membedakan perubahan yang sangat kecil itu. Pada dasarnya sebuah gambar bitmap merupakan kumpulan dari titik-titik yang disebut pixel.[10] Pixel-pixel disetiap gambar mempunyai nilai berbeda-beda

Misalkan diambil sebuah nilai pixel dari suatu gambar, dimana nilai pixel dikonversikan dahulu ke dalam biner untuk menyisipkan sebuah karakter R = 01010010 di mana 01010010 adalah kode biner untuk 82 yang merupakan kode ASCII [11] karakter R .

(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 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)

Segmen citra sebelum disisipkan

(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)

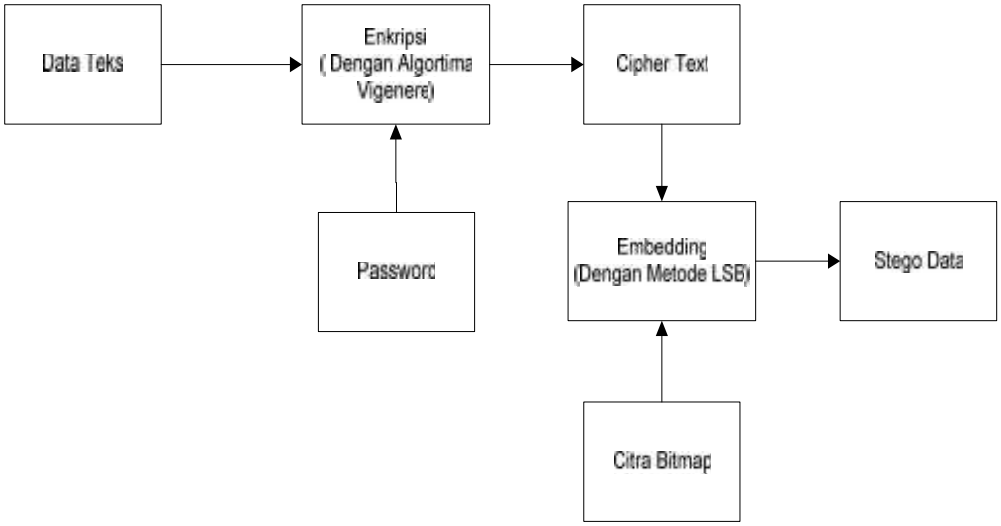
Segmen citra sesudah disisipkan R

Terlihat di atas perubahan pada contoh segmen data citra yang terdapat pada bit- bit yang paling kanan, setelah disisipkan 01010010 sebagai data yang disembunyikan , bahwa perubahan bit hanya terjadi pada sisi yang paling kanan dari 8 bit yang ada. Steganografi dengan metode LSB juga hanya mampu menyimpan informasi dengan ukuran yang sangat terbatas. Misalnya suatu citra 24-bit (R=8-bit, G=8-bit, B=8-bit) digunakan sebagai wadah untuk menyimpan data berukuran 100 bit, jika masing masing komponen warnanya (RGB) digunakan satu pixel untuk menyimpan informasi rahasia tersebut, maka setiap pixelnya disimpan 3 bit informasi, sehingga setidaknya dibutuhkan citra wadah berukuran 34 pixel atau setara 34 x 3 x 8 = 816 bit (8 kali lipat). Jadi suatu citra 24-bit jika digunakan untuk menyimpan informasi rahasia hanya mampu menampung informasi maksimum berukuran 1/8 dari ukuran 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

2.4 Proses Enkripsi Dan Penyisipan Data

Aplikasi yang dihasilkan dalam penelitian ini mempunyai fungsi untuk menyembunyikan pesan informasi berupa data teks dan gambar, dalam hal ini media yang digunakan adalah citra bitmap. Untuk menampung pesan informasi ke dalam objek stego yakni berupa citra bitmap tentunya membutuhkan suatu algoritma yang dapat memodifikasi objek stego tersebut. Hasilnya adalah citra baru yang berisi pesan informasi tersembunyi yang disebut dengan istilah embedding. Dalam proses modifikasi perubahan yang terjadi antara media penampung dengan hasil modifikasi media penampung tidak boleh terlalu mencolok 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. Untuk lebih jelasnya dapat dilihat pada gambar berikut ini.

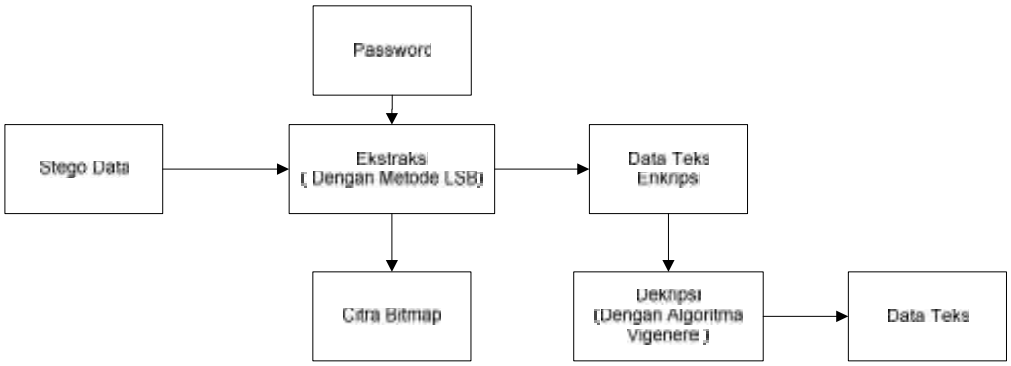



Gambar 3 Bagan proses penyembunyi File Pada Citra Bitmap

Dari gambar diatas dapat dilihat proses enkripsi menggunakan algoritma Vigenere. Untuk proses embedding digunakan metode LSB, sehingga dihasilkan data ataupun file yang sudah melalui proses stego

2.5 Algoritma Ekstraksi File

Untuk mengambil pesan informasi rahasia yang terkandung di dalam stegodata/ stego file, dibutuhkan proses ekstraksi pesan berupa algoritma pendeteksi dan kunci enkripsi. Algoritma pendeteksi ini merupakan kebalikan dari algoritma embedding, bila algoritma embedding ini digunakan untuk menyisipkan pesan informasi rahasia ke dalam file citra bitmap, maka algoritma pendeteksi digunakan untuk mengambil pesan informasi rahasia dari file citra bitmap. Algoritma steganografi ini memodifikasi beberapa pixel yang terdapat di dalam file citra bitmap. Di dalam setiap pixel yang terdapat pada file citra bitmap, memiliki intensitas nilai dari ketiga warna dasar yaitu warna merah, warna hijau dan warna biru. Jadi suatu warna pada pixel merupakan kombinasi dari intensitas ketiga warna tersebut. Intensitas warna memiliki nilai 0 sampai 255 yang mengambil 8 bit atau 1 byte untuk setiap warnanya, sehingga dalam satu pixel terdapat 24 bit yaitu 8 bit warna merah, 8 bit warna hijau dan 8 bit warna biru [13] Di dalam satu byte informasi yang diwakili oleh 8 bit ini, ada penggolongan-penggolongan bit berdasarkan urutan dan pengaruhnya di dalam byte tersebut, misalnya ada 1 byte informasi yang berisikan bit 10111001. Bit yang paling berpengaruh terhadap informasi yang dikandungnya biasanya adalah angka 1 yang terletak paling depan. Bit ini sering disebut dengan Most Significant Bit (MSB). [14] Semakin ke kanan, bit-bit tersebut semakin kecil pengaruhnya terhadap keutuhan informasi yang dikandung, bit inilah yang disebut dengan Least Significant Bit (LSB). Teknik steganografi modifikasi dengan Least Significant Bit (LSB) ini dilakukan dengan memodifikasi bit-bit yang tergolong bit LSB pada setiap byte warna pada sebuah pixel. Bit-bit LSB ini akan dimodifikasi dengan meggantikan setiap LSB yang ada dengan bit-bit informasi lain yang ingin disembunyikan [15] Setelah semua bit-bit informasi menggantikan bit-bit LSB di dalam file-file tersebut, maka pesan informasi telah berhasil disembunyikan. Ketika pesan informasi rahasia tersebut ingin kembali dibuka, maka bit-bit LSB yang sekarang ada diambil satu persatu dan disatukan kembali menjadi sebuah informasi. Proses ini disebut dengan istilah extraction atau ekstraksi data, yang digambarkan pada gambar berikut ini

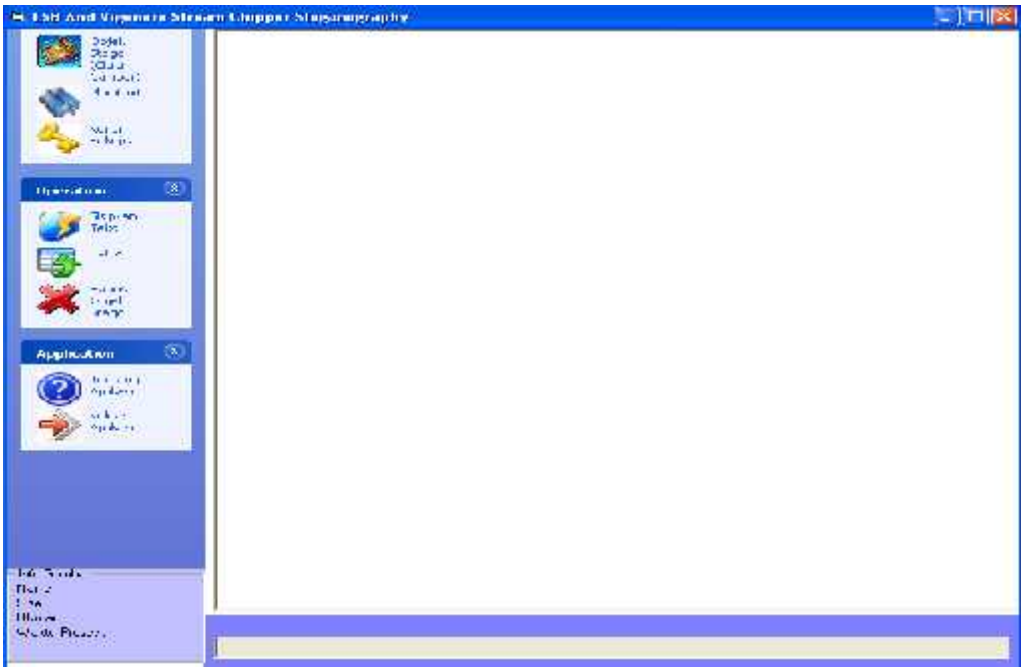



Gambar 4 Bagan Proses Ekstraksi File Pada Citra Bitmap

## 3. HASIL DAN PEMBAHASAN

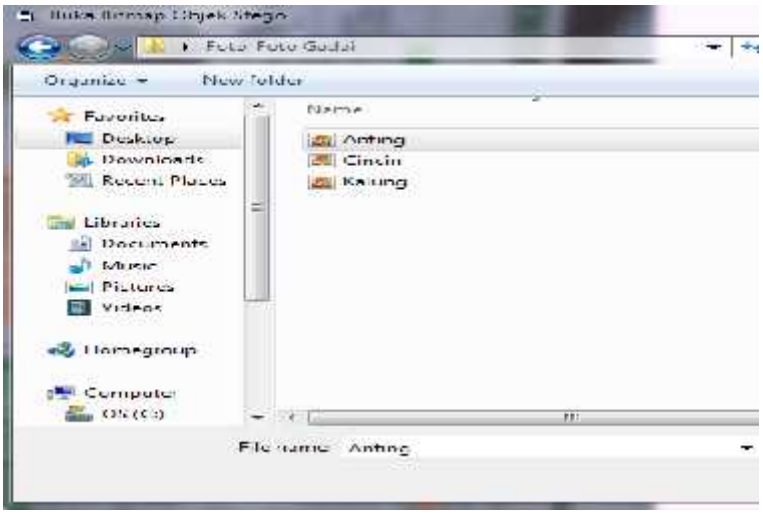
3.1 Proses Steganografi.

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 dibawah ini.

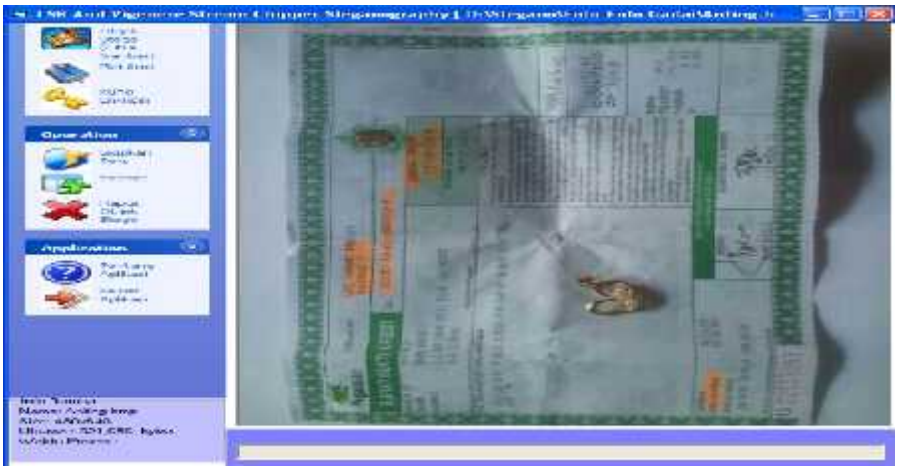


Gambar 5 menu utama aplikasi

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

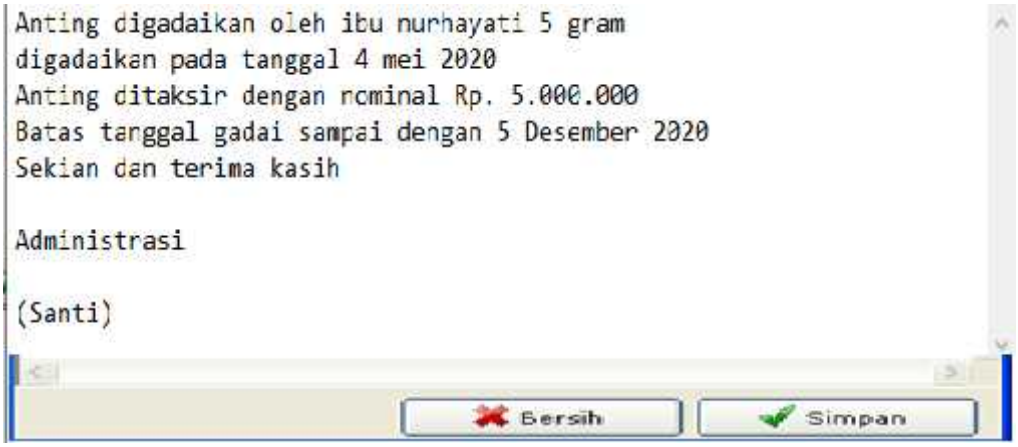



Gambar 6 pilih object gambar



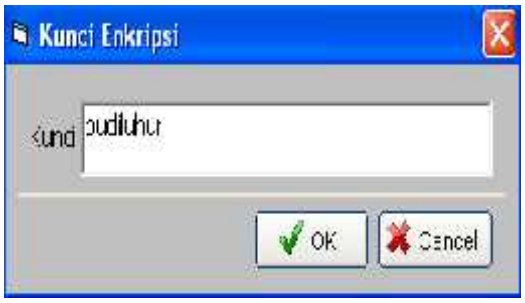
Gambar 7 gambar yang dipilih untuk dijadikan media pengirim pesan

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.




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 dibawah ini.


Gambar 11 text yang dienkripsi

3.2 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.

## 4. KESIMPULAN

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] Fino Ardiansyah prayudi and agus 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] Niria Laila and Anita Sindar RMS. Implementation of LSB Steganography with Vigenere Cipher Encryption in Image. Computer Science Informatics Jo urnal Vol. 1, No. 2, 2018. pp. 47- 58.

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

[4] Achmad Ardiansyah and Mepa 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] Rama Aria Megantara and Fauzi Adi Rafrastara. Super Enkripsi Teks Kriptografi Menggunakan Algoritma Hill Cipher Dan Transposisi Kolom. Prosiding SENDI_U. pp. 85-92. 2019.
[7] Putu H. Arjana. dkk. Implementasi Enkripsi Data Dengan Algoritma Vigenere Chiper. Seminar Nasional Teknologi Informasi dan Komunikasi. pp.164-169. 2012.
[8] Ruri Suko Basuki and Elkana Nungki 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] Kemal Ade Sekarwati and Ariep Budiman. Mplementasi Algoritma Rivest-Shamir-Adleman (Rsa) Dan Metode Least Significant Bit (LSB) Untuk Keamanan File Teks Dan Dokumen Menggunakan Visual C#. Jurnal Teknologi Rekayasa Volume 22 No.1, pp. 54-62. 2017..
[10] Dedy Agung 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 Achmad Fauzi. Implementasi Pengamanan Data Menggunakan Enkripsi Caesar Cipher Dengan Kombinasi Tabel ASCII. Seminar Nasional Teknologi Informasi dan Multimedia. STMIK AMIKOM Yogyakarta, 8 Februari 2014.
[12] Dian Gustina and Achmad Sumbaryadi. Pembuatan Aplikasi Steganografi Pada Citra Digital. Jurnal Sistem Informasi. pp. 20-27. 2018.
[13] Barry Wilkinson and Michael Allen. Parallel Programming-Teknik dan Aplikasi menggunakan jaringan workstation & Komputer paralel. Andi Publisher. Yogyakarta, 2010.
[14] Darmayanti1, Awang Harsa.K, Sistem Steganografi Pada Citra Digital Menggunakan Least Significant Bit, Prosiding Seminar Sains dan Teknologi FMIPA Unmul Vol. 1 No. 1 Juli 2016
[15] Rohmat Nur 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.