

IMPLEMENTASI KRIPTOGRAFI DAN STEGANOGRAFI MENGUNAKAN METODE *VIGÈNERE CIPHER* DAN *LEAST SIGNIFICANT BIT* BERBASIS ANDROID

Oliffatur Rizki Susanto¹⁾, Ari Eko Wardoyo S. T, M. Kom²⁾,

Mudafiq Riyan Pratama, S. Kom³⁾

*Program Studi Teknik Informatika – S1, Fakultas Teknik
Universitas Muhammadiyah Jember*

ABSTRAK

Perkembangan teknologi saat ini begitu pesat dibidang teknologi komunikasi khususnya, karena perkembangan ini, maka dibutuhkan kemampuan untuk dapat mengakses informasi dengan cepat. Perkembangan ini sangat terlihat khususnya pada media elektronik, dimana salah satu faktor penting yang sangat berperan didalamnya adalah internet. Dengan internet manusia dapat bertukar informasi dengan menggunakan media elektronik, seperti PC (Personal Komputer) maupun dengan perangkat mobile, seperti smartpone, maupun tablet. Karena banyaknya orang yang menggunakan media internet atau sosial media, maka kebutuhan akan keamanan dalam berkomunikasi semakin diperlukan. Karena inilah dibutuhkan adanya cara untuk mengamankan data yang dikirim dengan aman. Salah satu caranya dengan menyembunyikan data sebelum data itu dikirimkan,. Pada penelitian ini akan dirancang aplikasi penyembunyian pesan atau steganografi yang dikombinasikan dengan pengacakan pesan atau kriptografi pada image berbasis platform android. Algoritma LSB (Least Significant Bit) merupakan salah satu dari algoritma yang digunakan untuk keperluan steganografi pada citra JPEG. Aplikasi steganografi ini dibangun dengan menggunakan bahasa pemrograman java android. Berdasarkan hasil perancangan dan implementasi, didapat citra yang tidak jauh dengan citra aslinya, sehingga keamanan data yang dikirimkan dengan menggunakan program aplikasi tersebut melalui media BBM terjamin.

Kata Kunci : Steganografi, Kriptografi, Android, BBM, Gambar.

Implementasi Kriptografi Dan Steganografi Menggunakan Metode Vigènere Cipher Dan Least Significant Bit Berbasis Android

ABSTRACT

Current technological developments in the field of communications technology is so rapid in particular, because of these developments, it takes the ability to be able to access information quickly. This development is very visible, especially in the electronic media, which is one important factor that was instrumental in it is the internet. With the internet people can exchange information using electronic media, such as a PC (Personal Computer) as well as with mobile devices, such as smartphones or tablets. Because many people are using the internet or social media, the need for security in communication increasingly necessary. Because this is the way to secure the necessary data to be transmitted securely. One way to hide data before it is transmitted. This research will be designed applications concealment or steganographic message combined with randomization message or image-based cryptography on android platform. Algorithm LSB (Least Significant Bit) is one of the algorithms used for steganography in a JPEG image. Steganography application is built using android java programming language. Based on the result of design and implementation, which did not come away with the image of the original image, so that the security of data sent using the application program through the medium of fuel is assured.

Keywords : Steganography, Cryptography , Android , Least Significant Bit , image.

1.1 Latar Belakang

Dengan berkembangnya telekomunikasi yang ada saat ini penyampaian informasi sangatlah mudah dan cepat. Hampir disemua kalangan masyarakat memiliki telepon seluler *smartphone* android misalnya, yang penggunaanya sudah hampir mencapai 44.62%. Mayoritas media sosial yang biasa masyarakat gunakan yaitu *BBM (BlackBerry Messenger)* karena sosial media ini bisa mengirim pesan teks maupun gambar. Keamanan suatu informasi pada jaman global ini makin menjadi sebuah kebutuhan vital dalam berbagai aspek kehidupan. Suatu informasi akan memiliki nilai lebih tinggi apabila menyangkut tentang aspek-aspek keputusan bisnis, keamanan, ataupun kepentingan umum. Dimana informasi-informasi tersebut tentunya akan diminati oleh berbagai pihak yang juga memiliki kepentingan di dalamnya.

Keamanan pada suatu informasi atau data pada saat ini dapat dibagi menjadi dua, yakni: Kriptografi dan Steganografi. Kriptografi adalah suatu seni untuk mengacak suatu informasi atau data yang memiliki arti, menjadi sesuatu yang tidak dapat dimengerti atau seakan-akan tidak berarti. Berbeda dengan kriptografi, Steganografi adalah seni untuk menyembunyikan

suatu data, dimana data tersebut disembunyikan ke dalam suatu media yang tampak biasa saja. Media informasi yang dipakai adalah media gambar atau citra. Sehingga untuk melakukan penyembunyian pesan ke suatu citra tidak akan menimbulkan banyak kecurigaan dari pihak-pihak yang tidak dikehendaki.

rahasia dalam sebuah gambar/citra digital. Pesan rahasia dienkripsi dengan kunci. Dengan mengkombinasikan Steganografi dan Kriptografi untuk memberikan proteksi ganda pada pesan lalu disembunyikan dalam citra, dan pesan dapat diekstraksi dan didekripsi kembali persis sama seperti aslinya dengan menggunakan kunci yang sama. Pesan rasasia terlebih dahulu dienkripsi dengan sebuah algoritma *Vigenere cipher*, algoritma *Vigenere cipher* menggunakan substitusi angka maupun bujursangkar *vigènere*. Teknik susbtitusi *vigènere* dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser. Sedangkan metode lain untuk melakukan proses enkripsi dengan metode *vigènere cipher* yaitu menggunakan *tabula recta* (bujur sangkar *vigènere*). Bujursangkar *vigènere* digunakan untuk memperoleh

ciphertert dengan menggunakan kunci yang sudah ditentukan. Algoritma *vigenere cipher* memiliki keunikan dalam melakukan enkripsi menggunakan key yang ada. Kemudian cipherteks hasil kriptografi tersebut disembunyikan di dalam media gambar dengan metode LSB (*Least Significant Bit*) yaitu menyisipkan pesan di *bit* yang kurang berarti di gambar. Kelebihan LSB adalah ukuran citra yang mengandung pesan tidak berubah atau hampir mirip dengan citra asli.

1.2 Rumusan Masalah

Adapun permasalahan yang dihadapi dalam penelitian ini adalah :

- a. Bagaimana mengimplementasikan sistem untuk melakukan enkripsi dengan Algoritma Vigenere Cipher ?
- b. Bagaimana Menyisipkan objek ke dalam sebuah gambar dengan menggunakan metode LSB (*Least Significant Bit*) ?
- c. Bagaimana melakukan ekstraksi pada image/citra dan mendekripsi Algoritma Vigenere cipher ?

1.3 Batasan Masalah

Diperlukan suatu batasan permasalahan agar tidak menyimpang jauh dari permasalahan yang dibahas. Adapun batasan masalah untuk permasalahan pengiriman pesan gambar BBM adalah sebagai berikut :

- a. Enkripsi menggunakan algoritma kriptografi Vigenere cipher.
- b. Penyisipan cipherteks ke dalam gambar menggunakan algoritma LSB.
- c. Aplikasi BBM harus terbaru dan di Android.
- d. Gambar yang diterima harus *request HD*
- e. Pengiriman citra harus pada kontak BBM.
- f. Format gambar yang bisa yaitu .jpg .jpeg .png
- g. Tidak membahas mengenai pengiriman kunci.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai penulis dalam penelitian ini yaitu sebagai berikut :

- a. Mampu mengimplementasikan sistem untuk melakukan enkripsi dengan algoritma Vigenere cipher dan menyisipkan pada sebuah citra dengan metode LSB (*Least Significant Bit*).
- b. Menghasilkan sebuah sistem untuk mendekripsi hasil enkripsi dengan Algoritma Vigenere cipher dan mengekstraksi citra dengan metode (*Least Significant Bit*).

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah :

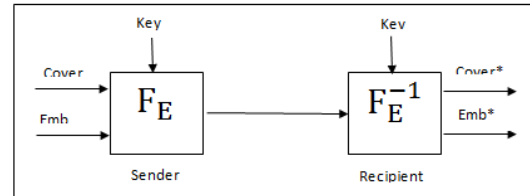
- a. Mengkombinasikan antara Kriptografi dan Steganografi untuk mengamankan pesan yang disisipkan di dalam citra.
- b. Menjaga kerahasiaan pesan yang dikirim ke penerima.

2. LANDASAN TEORI

Steganography adalah ilmu dan seni menulis atau menyembunyikan pesan kedalam sebuah media sedemikian rupa sehingga keberadaan pesan tidak diketahui atau tidak disadari oleh orang selain pengirim dan penerima pesan tersebut. Kata *Steganography* berasal dari bahasa Yunani, yaitu “*steganos*” yang berarti tersembunyi atau terselubung dan “*grapto*” yang berarti tulisan (Alatas, 2009).

Steganography membutuhkan dua aspek yaitu media penyimpanan dan rahasia yang akan disembunyikan. Metode *steganography* sangat berguna jika digunakan pada *steganography compute* karena banyak format file digital yang dapat dijadikan media untuk menyembunyikan pesan. *Steganography* digital menggunakan media digital sebagai wadah

penampung, misalnya teks, citra, suara, dan video. Data rahasia yang disembunyikan juga dapat berupa teks, citra, suara, atau video.



2.1.1 Konsep dan Terminologi

Terdapat beberapa istilah yang berkaitan dengan steganografi:

- a. *Hiddentext* atau *embedded message*: pesan yang disembunyikan.
- b. *overttext* atau *cover-object*: pesan yang digunakan untuk menyembunyikan *embedded message*.
- c. *Stegotext* atau *stego-object*: pesan yang sudah berisi *embedded message*

2.1.2 Manfaat Steganography

Manfaat penggunaan *Steganography* sebagai suatu teknik penyembunyian data pada data digital lain adalah sebagai berikut :

- a. *Tamper-proofing*
Steganography digunakan sebagai alat indikator untuk memeriksa integritas data

dengan menunjukkan apakah data digital yang asli telah mengalami perubahan dari aslinya.

b. *Feature location*

Steganography sebagai alat identifikasi isi dari data digital pada lokasi-lokasi tertentu, misalnya penamaan suatu objek tertentu dari beberapa objek yang ada pada data digital.

c. *Annotation/caption*

Steganography berisi keterangan tentang data digital itu sendiri, misalnya pada broadcast monitoring pada penayangan iklan di stasiun TV. Selain itu, *Steganography* juga dapat digunakan untuk mengirimkan informasi rahasia.

d. *Copyright-labeling*

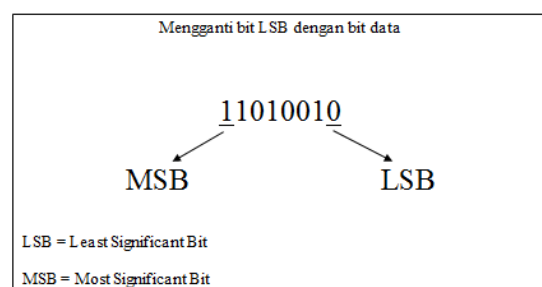
Steganography digunakan sebagai metode untuk menyembunyikan label hak cipta pada data digital atau sebagai bukti otentik kepemilikan atas data digital tersebut, yang dikenal sebagai *watermark*.

menyembunyikan pesan. LSB dilakukan dengan memodifikasi *bit-bit* yang termasuk bit LSB pada setiap byte warna pada sebuah piksel. Bit-bit LSB ini akan dimodifikasi dengan menggantikan setiap LSB yang ada dengan *bit-bit* pesan rahasia yang ingin disembunyikan. Setelah semua *bit* pesan rahasia menggantikan *bit* LSB file tersebut, maka pesan rahasia telah berhasil disembunyikan. Metode ini memodifikasi nilai yang paling kurang signifikan dari jumlah bit dalam 1 *byte* file carrier.

Sebagai contoh, akan dilakukan proses penyembunyian karakter “G” (ASCII 71) pada berkas carrier yang berukuran 8 *byte*. *Least Significant Bit* dari *file carrier* ditandai dengan garis bawah. Berkas carrier dalam biner dengan ukuran 8 *byte* : ”10010101 00001101 11001001 10010110 00001111 11001011 10011111 00010000” Karakter “G” dalam biner dengan ukuran 1 *byte* : “01000111” Proses *Least Significant Bit Modification* : “10010100 00001101 11001000 10010110 00001110 11001011

2.1.3 *Least Significant Bit (LSB)*

Least Significant Bit (LSB) adalah cara paling umum untuk



10011111 00010001”

2.2 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani “*cryptos*” artinya “*secret*” (rahasia), sedangkan “*graphein*” artinya “*writing*” (tulisan). Jadi, kriptografi berarti “*secret writing*” (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam beberapa literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.

2.2.1 Vigènere Cipher

Kode vigènere termasuk kode abjad-majemuk (*poly alphabetic substitution cipher*). Dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16, tahun 1586. Sebenarnya Giovan Batista Belaso telah menggambarannya untuk pertama kali pada tahun 1533 seperti ditulis di dalam buku *La Cifra del Sig.* Teknik untuk menghasilkan ciphertext bisa dilakukan menggunakan substitusi

angka maupun bujursangkar vigènere. Teknik substitusi vigènere dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser.

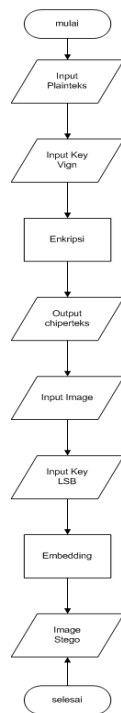
2.3 BlackBerry Messenger

BlackBerry Messenger disingkat *BBM* adalah aplikasi pengirim pesan instan yang disediakan untuk para pengguna perangkat *BlackBerry* pada awalnya. Aplikasi ini mengadopsi kemampuan fitur untuk aktifitas populer di kalangan pengguna perangkat telepon genggam. Layanan *Messenger* ini dibuat khusus bagi pemilik *BlackBerry* dan dirancang untuk berkomunikasi di antara pengguna.

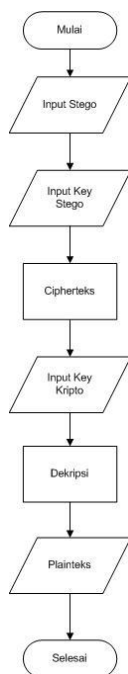
1. METODE PENELITIAN

3.1 Perancangan Sistem

Pada proses ini akan menjelaskan bagaimana program akan berjalan serta menjalankan fungsi – fungsinya. Gambar 3.2 berikut ini merupakan gambaran umum dari sistem yang akan dibangun.



Pada gambar diatas menunjukkan Alur Proses Enkripsi aplikasi vgnLSBstego.



Pada gambar diatas menunjukkan Alur Proses Dekripsi aplikasi vgnLSBstego.

4. Hasil Aplikasi

4.1 Pengujian

Pengujian akan dilakukan dengan :

- Pengujian dengan gambar yang memiliki resolusi kecil sampai besar dan dengan ukuran yang berbeda
- Pengujian dengan gambar yang memiliki ekstensi yang berbeda.
- Pengujian enkripsi dengan memasukkan angka, huruf dan karakter yang ada di keyboard hp android

4.2.1 Pengujian dengan mengenkripsi dan mendekripsi

Pengujian akan dilakukan dengan menggunakan seluruh karakter input yang ada keyboard android, dan untuk gambar menggunakan gambar dengan ukuran kecil, sedang dan besar serta menggunakan ekstensi yang berbeda.

5. KESIMPULAN

5.1 Kesimpulan

Dari hasil pengujian sistem yang dilakukan pada bab sebelumnya, maka dapat disimpulkan ke dalam beberapa hal antara lain:

- Metode Least significant bit berhasil untuk mengenkripsi dan

dekripsi pada semua ekstensi gambar yang telah diujikan.

- b. Metode Least Significant Bit berhasil di ujicobakan untuk menyisipkan pesan pada gambar standar beresolusi antara 100×100 sampai dengan 4000×2000 atau lebih.
- c. Metode Least Significant Bit berhasil di ujicobakan pada gambar standar berukuran 10 kb sampai dengan 2 MB, namun gagal pada file gambar berukuran lebih dari 2 MB.

5.2 Saran

- a. Aplikasi VigLSB stego hanya memuat file image kurang dari 2 MB dirapkan nantinya bisa dikembangkan untuk memuat file yang lebih dari itu.
- b. Aplikasi VigLSB stego dikirim melalui media BBM di android diharapkan nantinya dikembangkan untuk media lain dan platform OS lain.

DAFTAR PUSTAKA

Alatas, P. (2009). *Implementasi teknik steganografi dengan metode lsb pada citra digital*. Tugas Akhir. Jurusan Sistem Informasi, Fakultas

Ilmu Komputer & Teknologi Informasi, Universitas Gunadarma.

Ghare, R. Bansode, P. Bombale S. Chandargi B. (2015). *LSB Steganography Using Android Phone*. Undergraduate thesis. Information Technology Department, Savitribai Phule Pune University KJ's Educational Institute.

Kirom, M. S. (2012). *Hubungan penggunaan black berry messenger dengan intensitas komunikasi antar karyawan bagian marketing pt. Temprina media grafika surabaya*. Undergraduate thesis, UIN Sunan Ampel Surabaya.

Masita, G. Ismandoko T. (2015). *Pengamanan Pesan Steganografi dengan Metode LSB Berlapis Enkripsi dalam PHP*. Tugas Akhir. Program Studi Ilmu Komputer, Fakultas Pasca Sarjana, Universitas Budi Luhur

Muchbarak, A. Harvianto, F. (2013). *Pendekatan metode Least Significant Bit untuk merancang aplikasi steganography pada file PNG dengan metode huffman code dalam kompresi pesan*. Tugas Akhir. Magister Ilmu Komputer, Teknik Informatika, Universitas Budi Luhur.

