IMPLEMENTASI ALGORITMA LEAST SIGNIFICANT BIT MACHING UNTUK MENGAMANKAN DATA RAHASIA PERUSAHAAN

Turkhamun Adi Kurniawan [1], Wahyudi Syahputra [2], Safrizal [3]
Fakultas Teknik Informatika Program Studi Teknik Informatika
Universitas Satya Negara Indonesia
E-mail: t.adikurniawan@usni.ac.id, aditiafayakun@yahoo.com

ABSTRAK

Keamanan data merupakan hal yang sangat penting, dimana dibutuhkan sebuah keamanan dalam transaksi data secara online terutama pada surat- surat penting perusahaan yang hanya diperuntukan untuk internal perusahaan, bukan untuk publik. Pertukaran data dapat dilakukan dengan mudah dan cepat sehingga menjadi sangat rentan terhadap penyalahgunaan dari pihak yang tidak berwenang, dengan ini maka dibutuhkan suatu solusi untuk mengamankan surat- surat penting perusahaan. Keamanan tersebut berupa aplikasi dengan Metodesteganografi menggunakan *Least Significant Bit Matching* (LSBM) sehingga dapat digunakan untuk mengamankan surat-surat penting perusahaan. Pengguna juga dapat meng *encrypt* dan *decrypt*.

Kata Kunci: Android, *Steganografi*, *Least Significant Bit Matching* (LSBM)

.

ABSTRAK

Data security is very important, where security is needed in online data transaction, especially in importan company letters which are only intended for internal companies, not for the public, data exchange can be done easly and quickly so that it becomes very vulnerable to abuse from unauthorized parties, with this so we need a solution for important company letters. The security is in the form of a steganographic method using Least Significant Bit Matching (LSBM) so that it can be used to make important companyletters. User can also encrypt and decrypt.

Keywords: *Android, Steganography, Least Significant Bit Matching (LSBM)*

1. PENDAHULUAN

Di era Globalisasi saat ini keamanan data merupakan hal yang sangat penting, dimana dibutuhkan sebuah keamanan dalam transaksi data secara online terutama pada surat- surat penting perusahaan yang hanya diperuntukan untuk internal perusahaan, bukan untuk publik. Pertukaran data dapat dilakukan dengan mudah dan cepat sehingga menjadi sangat rentan terhadap penyalahgunaan dari pihak yang tidak berwenang. Semakin penting suatu data, maka dibutuhkanlah keamanan yang memadai untuk mencegah pihak yang tidak berwenang dalam mengakses suatu data. Ada banyak cara untuk mengamankan data, salah satunya adalah teknik steganografi. Teknik steganografi merupakan teknik menyembunyikan data atau informasi kedalam gambar. Salah satu metode steganografi yang sering digunakan dalam konsep steganografi adalah *Least Significant Bit* (LSB). Metode LSB Pada Citra Digital dapat digunakan Sebagai Upaya Peningkatan Jaminan Keamanan Dalam Transaksi Informasi Secara Online (Kurniawan, 2017). Algoritma *Least Significant Bit* (LSB) adalah salah satu metode steganografi pada domain spesial yang melakukan penyisipan pesan dengan cara mengubah nilai bit terkecil (J. C., Handoko, Sari, & Moses Seiadi, 2018). Algoritma steganografi yang menyisipkan data pada bit- bit terakhir *byte* tertentu pada gambar sehingga perubahan dari penyisipan data- data tersebut tidak memberikan dampak yang terlihat secara kontras dalam pandangan mata manusia. Sebelumnya telah dilakukan penelitian mengenai penerapan algoritma LSB ini oleh (Anti, Kridalaksana, & Khairina, 2017) yang berjudul "Steganografi Pada Video Menggunakan Metode *Least Significant Bit* (LSB) dan *End of File (*EOF)". Berdasarkan penjelasan dari permasalahan diatas, peneliti mencoba membuat pengembangan pengenkripsian pesan yaitu metode *least significant bit matching* LSBM.. Pada prinsipnya hampir sama dengan LSB biasa hanya saja sedikit modifikasi dengan menambahkan metode pencocokan atau *Maching* pada bit yang terakhir.

2. LANDASAN TEORI

a. Steganografi

Menurut (Riadi, Sunardi, & Aryanto, 2020) steganografi adalah ilmu dan seni untuk menyembunyikan informasi sehingga informasi yang bersifat rahasia tidak dapat diketahui oleh orang lain, kecuali pengirim dan penerima. Tujuan dari steganografi adalah merahasiakan atau menyamarkan keberadaan dari sebuah pesan tersembunyi. Metode steganografi hanya dapat dibaca oleh si pengirim dan si penerima karena pesan rahasia memiliki kunci yang hanya diketahui oleh si pengirim.

b. Least Significant Bit Matching (LSBM)

Least Significant Bit Matching (LSBM) adalah modifikasi kecil pengganti LSB. Pada LSBM, setiap bit-bit data yang disembunyikan dibandingkan dengan bit terakhir dari bit cover image yang berkoresponden. Jika cocok jangan lakukan apapun, jika tidak cocok, bit pada cover image ditambah satu atau dikurang satu secara acak (Kecuali untuk byte yang ukurannya 0 tidak dapat dikurangi dan byte yang ukurannya 255 tidak dapat di tambah).

Penggunaan metode pencocokan LSB dianggap mampu mengatasi permasalahan pada file cover. Hal ini karena pada pencocokan LSB nilai LSB tidak diubah, tetapi hanya dicocokan dengan bit pesan. (Amri, Suta Wijaya, & Bimantoro, 2017)

Adapun tahapan algoritma dari *Bit Matching* ini adalah sebagai berikut:

1. Mengkonversi pesan dan citra ke dalam bentuk biner
2. Mengambil nilai citra
3. Melanjutkan pencocokan pesan pada citra. Jika bit pesan terdapat pada citra, maka dilanjutkan dengan menyimpan posisi indeks bit. Penyimpanan indeks terdiri dari posisi indeks bit awal (*start*) dan posisi indeks akhir (*end*). Jika proses pencocokan tidak terjadi di lanjutkan ke proses 4
4. Membagi pesan menjadi 2 (dua) bagian sama Panjang kiri (L[i]) dan kanan (R[i]).
5. Mengulangi Langkah yang sama seperti pada Langkah nomor 2, dengan L [i] dan R [i] sebagai masukan. Jika semua bit pesan terdapat pada citra, maka pencocokan selesai.
6. Menyimpan semua indeks bit hasil pencocokan
7. Keluaran berupa vector yang memuat susunan indeks posisi bit

c. Kerangka Pemikiran

Merupakan suatu gambaran secara jelas akan pembahasan yang akan dipecahkan hingga mendapatkan suatu solusi yang baik. Dimana setiap alur dan tahapanya dibuat untuk membantu peneliti memusatkan pada permasalahan yang diteliti untuk memahami hubungan antar variable tertentu yang telah dipilih dan mempermudah peneliti memahami dari penelitian yang dilakukan. Adapun kerangka berpikir dalam penulisan ini, Sebagai berikut:

Gambar 1 Kerangka Pikir

d. Android

Android adalah perangkat lunak yang digunakan untuk perangkat *mobile* yang meliputi sistem operasi, middleware, dan aplikasi inti yang di rilis oleh Google. Android merupakan *mobile operating system* yang mengadopsi sistem operasi linux. Pada tahun 2005 Android diambil alih oleh Google dari Android,Inc sebagai strategi untuk mengisi pasar sistem operasi bergerak. Google mengambil alih seluruh hasil kerja Android termasuk tim yang mengembangkan Android modifikasi operasi linux. Pada tahun 2005 Android diambil alih oleh Google dari Android,Inc sebagai strategi untuk mengisi pasar sistem operasi bergerak. Google mengambil alih seluruh hasil kerja Android termasuk tim yang mengembangkan Android (Zulius & Daulay, 2019)

.

3. METODE PENELITIAN

a. Analisis Sistem Berjalan

Analisis sitem berjalan adalah suatu tahapan penelitian terhadap sistem yang telah ada untuk mengetahui segala permasalahan yang terjadi dan bertujuan untuk merancang sistem baru. Pada analisa sistem berjalan pada perusahaan saat ini yaitu pada saat mengirimkan sebuah dokumen rahasia pada suatu perusahaan yaitu menggunakan jasa kurir ataupun via email sehingga rentan terhadap peretasan terhadap dokumen tersebut. Sehingga dibutuhkan sebuah keamanan ganda untuk menghindari peretasan dari pihak yang tidak bertanggung jawab.

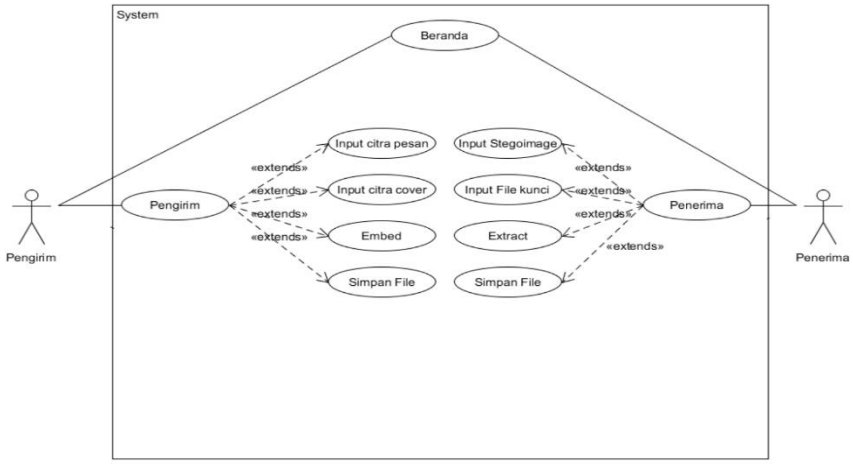
b. Analisa Masalah

Masalah yang dibahas dalam penlitian ini adalah bagaimana mengurangi resiko yang dapat terjadi dari sebuah pertukaran data yang bersifat rahasia yang dilakukan dengan cara pengkodean terhadap informasi yang akan disimpan atau dikirim dengan cepat dan akurat.

4. ANALISA DAN PERANCANGAN SISTEM

a. Usecase Diagram.

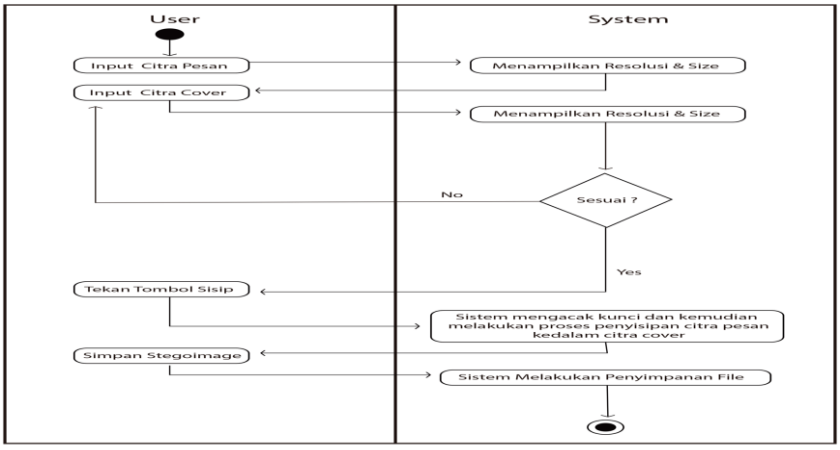
Pada gambar 1 dijelaskan bahwa pengguna atau *user* menjalankan sistem, dimana user pengirim menggunakan menu pengirim untuk menginput pesan citra dan citra cover yang kemudian dilakukan proses penyisipan. Kemudian *user* pengirim menyimpan hasil *file* citra tersebut. *User* penerima dapat mengembalikan *file* citra kebentuk semula dengan menginput citra stego dan menginput *file* kunci.



Gambar 2. *Usecase Diagram*

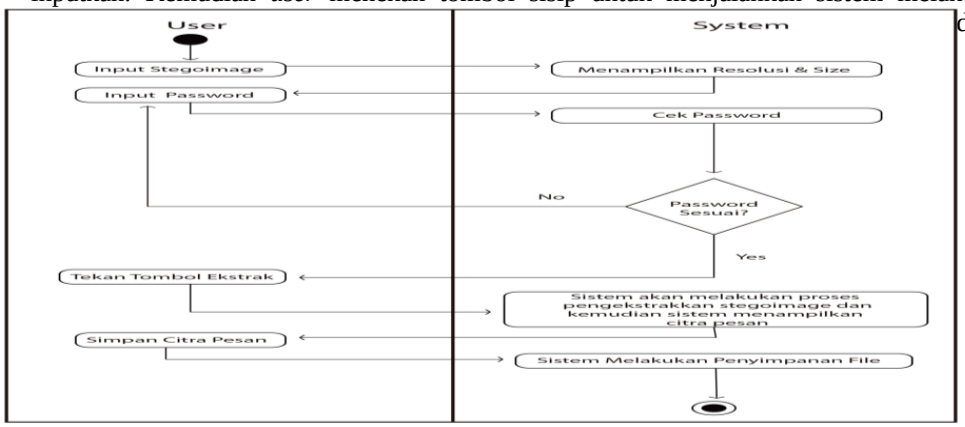
b. Activity Diagram

Menurut Satzinger et al (2010:141) Activity diagram merupakan sebuah tipe dari diagram workflow yang menggambarkan tentang aktivitas dari pengguna ketika melakukan setiap kegiatan dan aliran sekuensial.



Gambar 3 Activity diagram Penyisipan

Pada gambar 3 menunjukan proses user pengirim melakukan penyisipan citra pesan kedalam citra cover. Hal pertama yang dilakukan adalah menginputkan citra pesan dan citra cover yang kemudian sistem akan menampilkan resolusi dan *size* pada citra yang di inputkan. Kemudian *user* menekan tombol sisip untuk menjalankan sistem melakukan



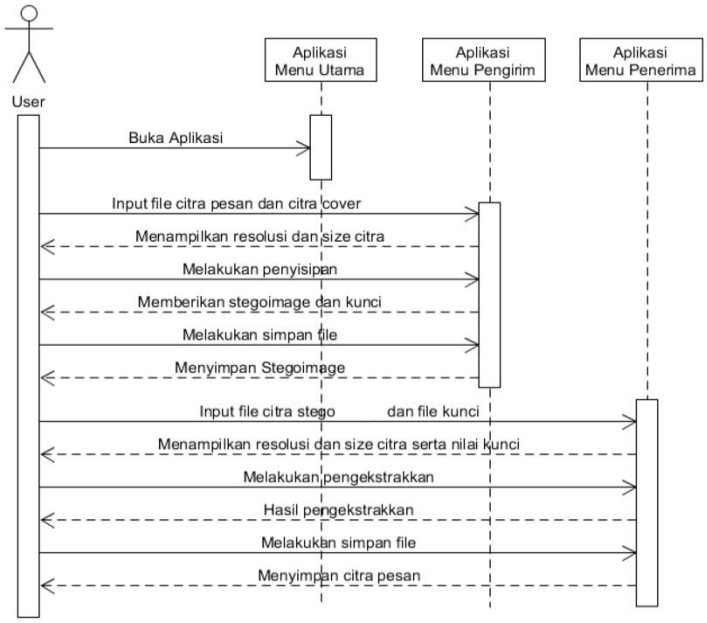
dapat

Gambar 4 Activity Diagram Pengekstrakan

Berdasarkan Gambar 4 menunjukan proses user penerima pesan melakukan pengektrakan citra stego untuk mendapatkan citra pesan yang diinginkan. Hal pertama yang dilakukan adalah penginputan citra stego dan file kunci yang dibutuhkan untuk melakukan pengektrakan. Kemudian user menekan tombol ektrak untuk menjalankan sistem melakukan proses pengektrakan citra stego untuk mendapatkan pesan. Setelah citra pesan di dapat, user dapat menyimpan file tersebut dengan menekan tombol simpan.

c. Sequnce Diagram

Sequence diagram adalah "Diagram yang memodelkan logika sebuah usecase dengan cara menggambarkan interaksi diantara objek-objek rangkaian waktu" (*whitten et al, 2004)*

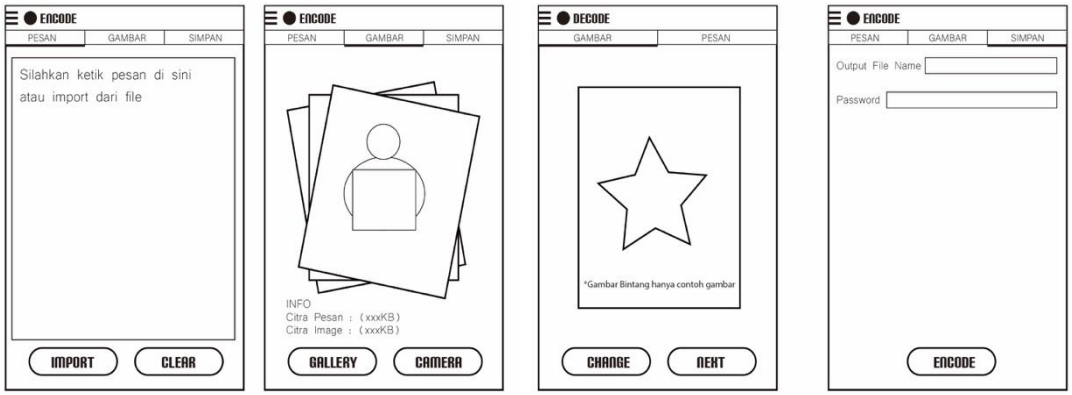


Gambar 5 Sequence diagram

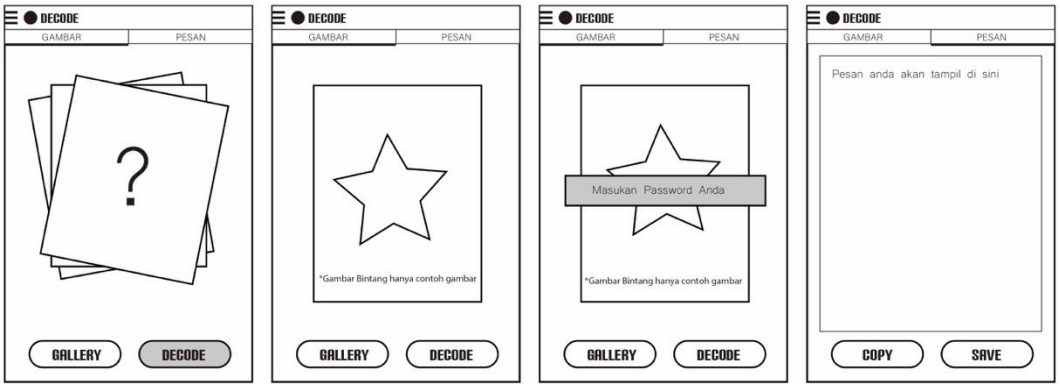
d. Desain Aplikasi

Desain Aplikasi yang dimaksud adalah tampilan dan *interface* dari aplikasi yang dibuat yang berisi fitur-fitur sebagaimana yang telah dijelaskan pada pembahasan sebelumnya. Berikut adalah desain tampilan Halaman pengirim dimana dalam halaman tersebut digunakan untuk melakukan proses pembangkitan kunci, proses enkripsi gambar dan proses penyisipan gambar. Gambar 6 menunjukan rancangan halaman pengirim. Pada gambar 7 merupakan halaman penerima digunakan untuk melakukan proses ektraksi chipertext dari stegano image dan proses dekripsi chipertext.

.



Gambar 6 Tampilan halaman pengirim



Gambar 7 Gambar *desain* tampilan halaman penerima

5. KESIMPULAN

a. Kesimpulan

Berdasarkan hasil penelitian yang telah peneliti uraikan pada penelitian yang telah dibuat, maka dapat disimpulkan sebagai berikut: Implementasi aplikasi Steganografi dengan menggunakan metode *Least Significant Bit Matching* (LSBM) berjalan dengan baik dari proses penyisipan sampai dengan proses penguraian informasi. Dari hasil simulasi yang dilakukan antara sebelum dan sesudah menggunakan aplikasi melalui steganografi, dapat diambil kesimpulan bahwa data atau informasi yang kita kirimkan melalui email akan lebih aman menggunakan aplikasi steganografi dibandingkan dengan pengiriman informasi tanpa menggunakan aplikasi steganografi

b. Saran

Agar kemanfaatan dari penelitian ini dapat dirasakan oleh beberapa perusaan lain maka dapat dikembangkan sesuai dengan kebutuhan perusahaan terkait. Adapun saran-saranya adalah sebagai berikut:

1. Menambahkan jenis ekstensi file lainnya
2. Cover image dengan ekstensi selain dari .*Jpeg*

DAFTAR PUSTAKA

M. O., & Azman Maricar. (2018). Pemampatan Citra Pas Foto Dengan Menggunakan Algoritma Kompresi Joint-Photograpic Experts Group (JPEG) dan Principal Component Analysis (PCA). *Majalah Ilmiah Teknologi Elektro*, 102-106.

G. I., & Sumarno. (2018). Penggunaan Algoritma Kriptografi Least Significant Bit untuk pengamanan pesan teks dan data video. *Jurnal Sains Komputer & Informatika*, 57-65.

Damanik, A. H., & A. M. (2018). Teknik Pengujian Keamanan Data Teks Bertingkat Dengan Metode Stagenography LSB dan Teknik Enksipsi. *Jurnal Penelitian Pos dan Informatika*, 109-122.

Kurniawan. T. (2017). Pemanfaatan Metode LSB pada Citra Digital dalam mengaplikasikan steganografi sebagai upaya peningkatan jaminan keamanan dalam transaksi secara online. *Jurnal Satya Informatika*, 22-35.

Anti, A. U., Kridalaksana, H. A., & Khairina, M. D. (2017). Steganografi Pada Video Menggunakan Metode Least Significant Bit (LSB) dan End of File (EOF). *Jurnal Informatika Mulawarman*, 104-111.

N. Y. (2019). Pengolahan Citra digital Perbandingan Metode Histogram Equalization dan Spesification Pada Citra Abu-abu. *Jurnal Komputer & Informatika*, 87-95.

A. U., S. I., & B. F. (2017). Steganografi Teks Menggunakan Metode Pencocokan LSB dan Karakter Non-Breaking Space Sebagai penanda pesan. *J-Cosine*, 23-32.

T. A. (2017). Pemanfaatan Metode LSB Pada Citra Digital Dalam Mengaplikasikan Steganografi Sebagai Upaya Peningkatan Jaminan Keamanan Dalam Transaksi Informasi Secara Online. *Jurnal Satya Informatika*, 22-35.

A.S, R., & Shalahuddin, M. (2011). *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek.* Bandung: Informatika.

M. S. (2016). *Analisis Dan Perancangin Sistem Informasi Manajemen Keuanga*