

PENGAMANAN PESAN MENGGUNAKAN TEKNIK STEGANOGRAFI DENGAN ALGORITMA LEAST SIGNIFICANT BIT (LSB)

Securing Messages Using Steganographic Techniques With Least Significant Bit (LSB) Algorithm

Angga Aditya Permana, anggaamt@gmail.com¹⁾

¹⁾Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Tangerang

ABSTRACT

Steganography is a technique or art to hide a secret message into a cover so that the existence of the secret message cannot be known by other people or third parties who do not have the ability to know the contents of the secret message. The Least Significant Bit (LSB) method is one of the methods used in steganography to hide a message by changing the value of the rightmost bit of a stego cover with a secret message. The purpose of this study was to hide a text message into an image using the LSB method.

Keyword : *Steganography, Least Significant Bit, Image, Text Message, Java.*

ABSTRAK

Steganografi merupakan ilmu teknik atau seni untuk menyembunyikan pesan rahasia kedalam sebuah cover sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui oleh orang lain atau pihak ketiga yang tidak mempunyai kewenangan dalam mengetahui isi dari pesan rahasia tersebut. Metode Least Significant Bit (LSB) merupakan salah satu metode yang digunakan dalam steganografi untuk menyembunyikan sebuah pesan dengan cara mengubah nilai bit paling kanan sebuah stego cover dengan pesan rahasia. Tujuan penelitian ini untuk menyembunyikan sebuah pesan teks kedalam sebuah gambar dengan metode LSB.

Kata Kunci: Steganografi, LSB, Image, Pesan Teks, Java

PENDAHULUAN

Pada sekarang ini, dunia globalisasi teknologi mulai meningkat pesat banyaknya penggunaan media digital membuat kita lebih mudah dalam melakukan pengiriman pesan tetapi saat kita mengirimkan sebuah pesan kita tidak tau bahwa apakah pesan kita itu aman atau tidak disaat kita melakukan pengiriman pesan. Dalam mengatasi dan melindungi pesan tersebut kita memerlukan sebuah metode untuk mengamankan sebuah pesan agar kita merasa aman dari orang yang tidak mempunyai 'kewenangan' atau dari seorang 'pembajak.' Salah satu metode yang dapat kita gunakan dalam mengamankan suatu pesan dengan

Steganografi. Steganografi merupakan seni dan ilmu menulis pesan dengan suatu cara sehingga pesan rahasia itu dapat dilindungi dari orang selain pengirim dan penerima pesan rahasia tersebut. Steganografi memiliki beberapa metode salah satunya merupakan metode Least Significant Bit (LSB) yang dengan cara mengubah bit paling kanan sehingga ukuran media akan bertambah sedikit. Media yang digunakan bisa berupa gambar, audio, dan video. Tetapi pada penelitian kali ini akan menggunakan media gambar untuk menyembunyikan sebuah pesan rahasia.

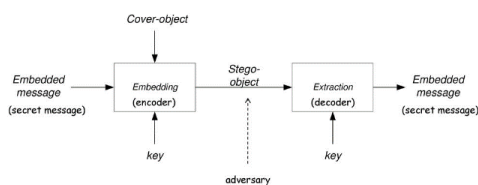
Agar penelitian ini dapat dilakukan lebih fokus, sempurna, dan mendalam maka penulis memandang permasalahan

penelitian yang diangkat perlu dibatasi variabelnya. Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

- Teknik yang digunakan dalam mengemaskan data adalah steganografi.
- Menggunakan metode Least Significant Bit (LSB)
- Menyembunyikan pesan rahasia berupa teks kedalam sebuah gambar
- Menggunakan Bahasa pemrog-raman Java.

Steganografi berasal dari Bahasa Yunani *Steganos* yang artinya “tersembunyi” dan *graphein* yang artinya “menulis”. Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Pada zaman dahulu steganografi dan kriptografi digunakan untuk menyembunyikan pesan saat peperangan. Keunggulan steganografi dari kriptografi adalah dapat menghilangkan kecurigaan karena pada steganografi dia menyembunyikan sebuah pesan kedalam sebuah media sedangkan kriptografi itu mengubah pesan sehingga dapat menimbulkan kecurigaan.

Steganografi membutuhkan dua property yaitu: wadah penampung dan data rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya: voice, video, image dan teks. Data rahasia yang disembunyikan juga dapat berupa voice, video, image dan teks. Dapat dilihat pada Gambar 1.



Gambar 1. Skema Steganographi

Secara umum, terdapat dua proses didalam steganografi, yaitu proses embedding untuk menyisipkan pesan ke

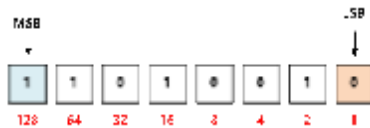
dalam cover-object dan proses decoding untuk ekstraksi pesan dari stego-object. Kedua proses ini mungkin memerlukan kunci rahasia yang dinamakan stego-key agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan.

Penyembunyian data rahasia ke dalam media digital mengubah kualitas media tersebut. Kriteria yang harus diperhatikan dalam menyembunyikan data diantaranya:

- **Fidelity.** Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografimasih terlihat dengan baik pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.
- **Robustness.** Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung (seperti pengu-bahan kontras, penajaman, penem-patan, rotasi, perbesaran gambar, pemotongan (*cropping*), enkripsi, dan sebagainya). Bila pada citra dilakukan operasi pengolahan citra, maka data yang disembunyikan tidak rusak.
- **Recovery.** Data yang disem-bunyikan harus dapat diungkapkkan kembali (recovery). Karena tujuan steganografi adalah data hiding, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

Salah satu metode yang digunakan dalam teknik steganografi pada gambar adalah Least Significant Bit atau disebut juga low bit encoding. Metode ini bekerja dengan cara mengganti *bit* terakhir dari masing-masing piksel dengan pesan yang akan disisipkan. LSB mempunyai kelebihan yakni ukuran gambar tidak akan berubah. Sedangkan kekurangannya adalah pesan/data yang disisipkan terbatas, sesuai dengan ukuran. Salah satu cover yang dapat digunakan untuk menyembunyikan pesan

adalah digital warna 24bit. Setiap piksel 1 pada warna 24bit memiliki warna yang merupakan kombinasi dari tiga warna dasar *Red, green, Blue* (RGB). Sedangkan satu piksel 1 warna 24bit diwakili oleh 3 byte, dimana masing-masing 1 byte merepresentasikan warna *Red, Green, Blue*. Penyisipan pesan ke dalam *cover* dinamakan *encoding* (embedded) sedangkan ekstraksi pesan dari *stego* dinamakan *decoing* (extraction). Ilustrasi MSB dan LSB dapat dilihat pada Gambar 2



Gambar 2. ilustrasi MSB dan LSB

Sebuah merupakan kumpulan dari titik-titik yang disebut piksel 1. Pada warna 24 bit, setiap piksel 1 berukuran 3 byte dimana setiap byte memiliki warna dari setiap komponen *Red, Green, Blue*. Misalkan terdapat 2 piksel 1, dimana nilai intensitas setiap warna pada setiap piksel 1 setelah dikoversikan ke dalam biner memberikan nilai biner seperti pada Gambar 3..

```
00100111 11101001 11001000
00100111 11001000 11101001
```

Gambar 3. Pola Penyisipan LSB

Untuk menyisipkan sebuah karakter "F" dengan bilangan biner 01000110 (kode ASCII 70) ke dalam 2 piksel 1 warna tersebut, setiap 2 bit dari pesan yang dimulai dari MSB disisipkan ke dalam 2 bit LSB dari setiap byte warna. Dan hasil penyisipannya memberikan nilai piksel 1 baru seperti pada Gambar 4.

```
00100101 11101000 11001001
00100110 11001000 11101001
```

Gambar 4. Pola Penyisipan Karakter F

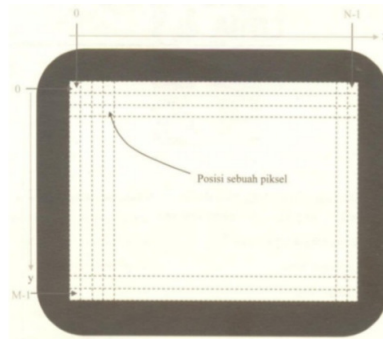
Contoh lain penggunaan metode LSB; asumsikan pesan yang akan disisipkan 5 bit = 11010, maka jumlah byte yang digunakan = 5 byte seperti yang diperagakan pada Gambar 5.

```
00101110 11001001 11111001 1000100 10100011
```

```
Hasil penyisipan menjadi ;
00101110 11001001 11111001 1000100 10100011
```

Gambar 5. Contoh Penggunaan LSB

Citra Digital dibentuk oleh kumpulan titik yang disebut piksel, setiap titik terkecil dalam gambar (piksel) memiliki koordinat posisi. Sistem koordinat ditunjukkan pada gambar 6.



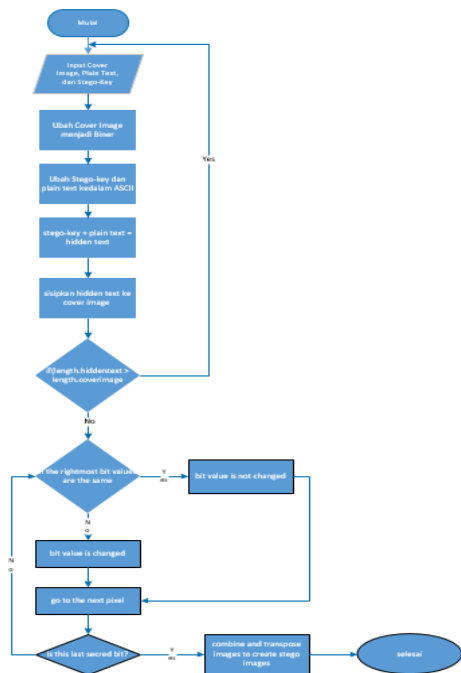
Gambar 6. Ilustrasi citra digital

Sebuah piksel memiliki koordinat berupa (x,y) dalam hal ini, x menyatakan posisi kolom dan y menyatakan posisi baris.

Citra gambar memiliki 3 jenis citra yang umum digunakan dalam pengolahan citra, diantaranya adalah :

- **Citra Biner (monokrom)**
 Citra biner adalah citra dengan setiap pikselnya hanya dinyatakan dengan sebuah nilai 0 (nol) dan 1 (satu). Nilai 0 (nol) menyatakan warna hitam dan 1 (satu) menyatakan putih.
- **Citra Berskala Keabuan (greyscale)**
 Citra ini menangani gradasi warna hitam dan putih, yang menghasilkan efek warna abu-abu. Warna dinyatakan dengan intensitas, intensitas berkisar antara 0-255 atau 8 (delapan) bit. Nilai 0 menyatakan hitam dan nilai 255 menyatakan putih.
- **Citra berwarna (RGB)**
 Citra berwarna merupakan jenis citra yang menyajikan warna dalam komponen R (Red), G (Green), B (Blue). Setiap komponen warna menggunakan 8 (delapan) bit nilainya

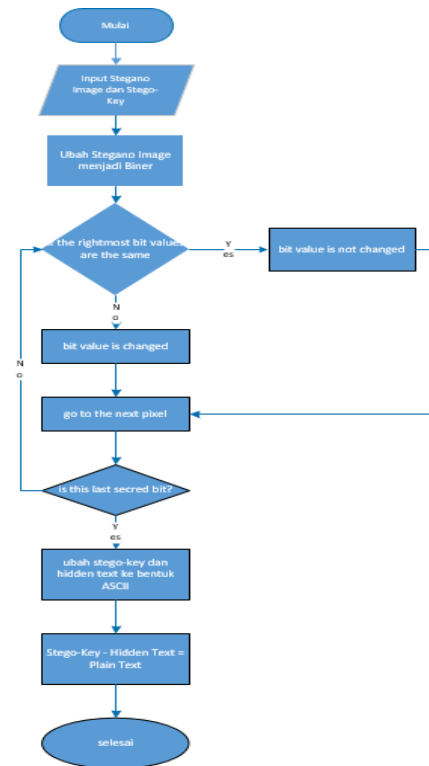
berkisar antara 0-255. Dengan semikian, kemungkinan warna yang dapat disajikan mencapai $256 \times 256 \times 256$ atau 16.777.216 warna.



Gambar 7. Flowchart Algoritma Encoding Message

Java merupakan Bahasa pemrograman tingkat tinggi yang dipelopori oleh James Gosling yang merupakan engineer di Sun Microsystem. Java mulai dibangun pada tahun 1991. Versi alpha dan beta dari java dirilis pada tahun 1995, 4 tahun setelah project Jaa diinisiasi. Pada tahun 2010, Sun Microsystem diakuisisi oleh Oracle dan menjadikan Java dikembangkan di bawah kuasa Oracle.

Untuk memudahkan dalam memahami cara kerja Algoritma Least Significant Bit (LSB), penulis membuat flowchart Encoding Message dan Decoding Message, diperagakan pada gambar 7 dan gambar 8.



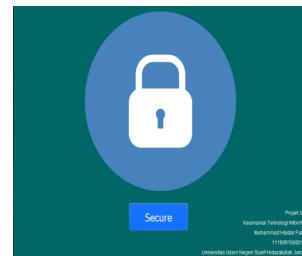
Gambar 8. Flowchart Algoritma Decoding Message

METODE PENELITIAN

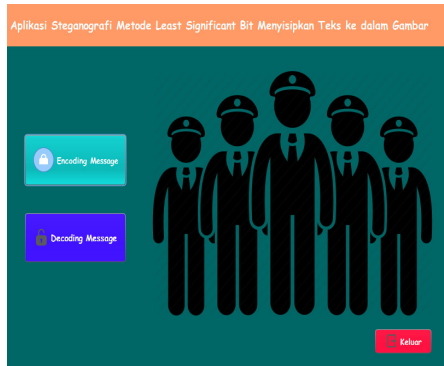
Untuk membuktikan keberhasilan metode LSB pada steganography ini dibuatlah sebuah aplikasi.

Aplikasi ini merupakan tampilan yang akan digunakan dalam Aplikasi Steganografi metode Least Significant Bit (LSB) menggunakan bahasa pemrograman java.

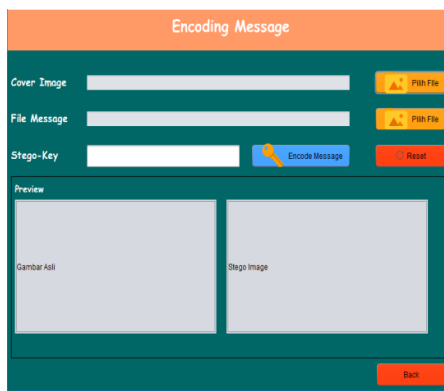
Tampilan aplikasi terdiri dari Play Button seperti yang diperagakan pada gambar 9, play button ini untuk memulai proses



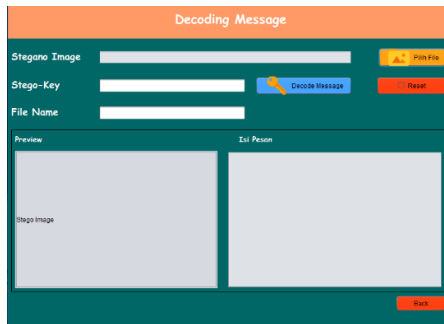
Gambar 9. Play Button



Gambar 10. Halaman Utama

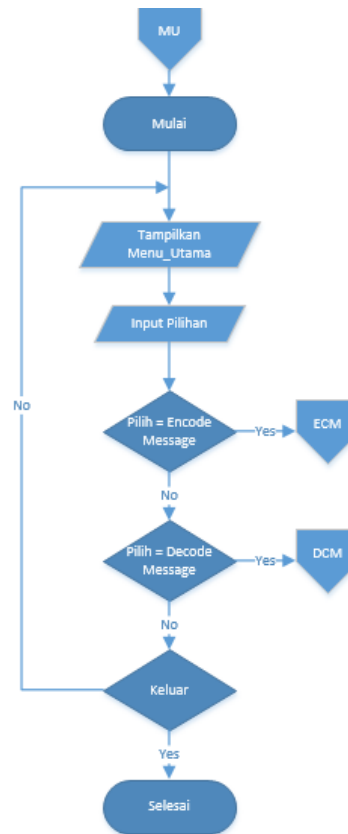


Gambar 11. Menu Encoding Message

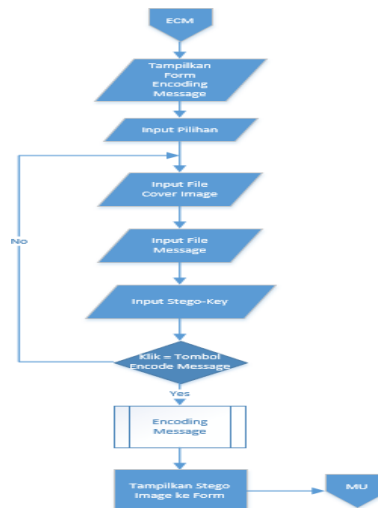


Gambar 12. Menu Decoding Message

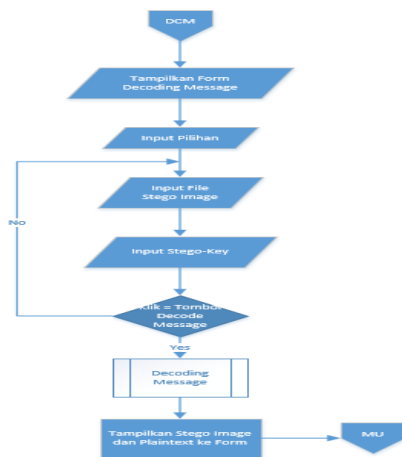
Untuk memahami cara penggunaan Aplikasi Steganografi ini, penulis membuat flowchart penggunaan Aplikasi agar memudahkan dalam menggunakan Aplikasi Steganografi metode LSB, seperti yang tercantum pada gambar 13 dan Gambar 14.



Gambar 13. Flowchart Menu Utama



Gambar 14. Flowchart Encoding Message


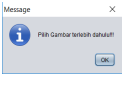





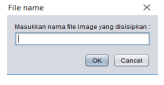

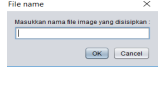
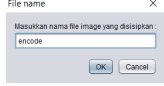

Gambar 15. Flowchart Decoding Message



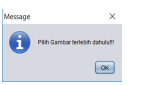




HASIL DAN PEMBAHASAN

Tabel 1 merupakan hasil pengujian yang dilakukan terhadap sistem. Dengan scenario pengujian yang dilakukan secara berbeda untuk tiap kasusnya, sehingga dapat mencerminkan kondisi pengujian yang telah dilakukan.

Tabel 1. Hasil pengujian Nama Tabel

No	Skenario Pengujian	Hasil Yang Diharapkan	Kesimpulan
1	Mengosongkan Cover Image, lalu langsung klik tombol "Encode Message". Test Case : 	Sistem akan menolak akses encode dan menampilkan pesan "pilih gambar terlebih dahulu!!!". Hasil Pengujian : 	V al i d
2	Mengosongkan File Message, lalu langsung klik tombol	Sistem akan menolak akses encode dan	V a l

	"Encode Message". Test Case : 	menampilkan pesan "pilih teks pesan terlebih dahulu!!!". Hasil Pengujian : 	i d
3	Mengosongkan Stego-Key dengan cover gambar dan pesan yg sudah dipilih, lalu klik tombol "Encode Message". Test Case : 	Sistem akan menerima akses encode dan menampilkan untuk mengisi file name untuk disave. Hasil Pengujian : 	V a l i d
4	Mengisi Stego-Key dengan cover gambar dan pesan yg sudah dipilih, lalu klik tombol "Encode Message". Test Case : 	Sistem akan menerima akses encode dan menampilkan untuk mengisi file name untuk disave. Hasil Pengujian : 	V a l i d
5	Mengisi nama file, lalu klik tombol "OK". Test Case : 	Sistem akan menerima akses dan menampilkan pesan sukses dan menampilkan stego image Hasil Pengujian : 	V a l i d

			
6	Mengosongkan Stegano Image, lalu langsung klik tombol "Decode Message". Test Case : 	Sistem akan menolak akses encode dan menampilkan pesan "pilih gambar terlebih dahulu!!!". Hasil Pengujian : 	V a l i d
7	Salah/berbeda memasukan Stego-key, lalu klik tombol "Decode Message". Test case : 	Sistem tetap akan menampilkan pesan "sukses" tetapi hasil yang keluar akan tidak sesuai dengan aslinya/acak. Hasil Pengujian : 	V a l i d
8	Memasukan stego-key yang benar, lalu klik tombol "Decode Message". Test case : 	Sistem akan menampilkan pesan "sukses" dan hasil yang keluar akan sesuai dengan aslinya. Hasli pengujian : 	V a l i d

SIMPULAN

Kesimpulan yang dapat diperoleh dari hasil perancangan, pembuatan, dan uji coba dari program aplikasi steganografi metode Least Significant Bit (LSB) ini, maka penulis membuat kesimpulan sebagai berikut:

1. Bahwa keamanan data Steganografi merupakan hal yang sangat penting didalam dunia yang serba modern ini.
2. Algoritma atau metode Least Significant Bit ini dapat meningkatkan keamanan pada sebuah teks atau gambar. Pesan yang bersifat rahasia akan disisipkan kedalam gambar sehingga pesan tersebut tetap aman dari orang-orang yang ingin memanipulasi sebuah pesan tersebut.
3. Hasil dari uji coba untuk menyisipkan pesan rahasia kedalam gambar berjalan dengan baik. Pesan rahasia kembali secara utuh sesuai dengan aslinya sebelum di encode dan saat sesudah decode kembali ke pesan asli tanpa berubah.
4. Output gambar yang sudah tersisipkan sebuah pesan rahasia memiliki perubahan ukuran file gambar (size).

DAFTAR PUSTAKA

- [1] Bachtiar, Adam R. Fakhrol, Firman N. 2018. *Pemrograman Berorientasi Objek Menggunakan Java*. Bandung: Informatika.
- [2] Djuwitaningrum, E.R. dan Apriyani, M. 2016. Teknik Steganografi Pesan Teks Menggunakan Metode Least Significant Bit dan Algoritma Linear Congruential Generator. *Jurnal Informatika*, 4(2): 79-85.
- [3] Iswahyudi, C., Setyaningsih, E., 2012. Pengamanan Kunci Enkripsi Citra Pada Algoritma Super Enkripsi Menggunakan Metode End Of File. *Jurnal Prosiding Nasional Aplikasi Sains & Teknologi (SNAST) Periode III*.
- [4] Munir, Rinaldi. 2004. *Pengolahan Citra Digital dengan Pendekatan Algoritmik*. Bandung: Informatika.
- [1] Permana, A A, 2018, APLIKASI PENYISIPAN TEKS PADA GAMBAR DENGAN ALGORITMA

BLOWFISH DAN LEAST
SIGNIFICANT BIT,

JurnalInformatika Vol 1 No 1
ISSN : 2549 : 0710