Teknik Steganografi Penyembunyian Pesan Text Rahasia Pada Citra Digital Dengan Metode *Least Significant Bit*

Supardi[1], Ari Amir Alkodri[2], Burham Isnanto[3]
[1]Program Studi Sistem Informasi, ISB Atma Luhur, Bangka Belitung
[2,3]Program Studi Teknik Informatika, ISB Atma Luhur, Bangka Belitung
Email: [1]supardi@atmaluhur.ac.id, [2]arie_a3@atmaluhur.ac.id, [3]burham@atmaluhur.ac.id

Abstrak - Steganografi adalah salah satu teknik yang paling kuat untuk menyembunyikan keberadaan data rahasia tersembunyi di dalam penutup obyek. Gambar adalah objek penutup paling populer untuk Steganografi dan dalam steganografi gambar kerja ini diadopsi. Menanamkan informasi rahasia di dalam gambar membutuhkan perhitungan yang intensif, dan oleh karena itu, merancang Steganography dalam mempercepat kecepatan perangkat Steganografi. Ini diimplementasikan menggunakan prosesor ARM7TDMI dan GSM 900. Ada beberapa teknik untuk menyembunyikan informasi di dalamnya gambar sampul. Teknik domain spasial memanipulasi nilai bit pixel gambar sampul untuk menanamkan informasi rahasia. Bit rahasia ditulis langsung ke sampul image pixel bytes. Akibatnya, teknik domain spasial sederhana dan mudah diterapkan. The Least Significant Bit (LSB) adalah salah satu techniques utama dalam steganografi citra domain spasial. Dalam penelitian ini, teknik baru steganografi LSB telah diusulkan yang merupakan versi improvisasi teknik LSB satu bit. Ada pun tujuan dari penelitian untuk menyembunyikan pesan teks rahasia kedalam file gambar sehingga pesan rahasia menjadi aman karena sudah disimpan didalam file gambar sehingga menjadikan alternatif pengiriman pesan agar terhindar dari pencurian dan sabotase.

Kata Kunci - Steganography, embedded, Cover image, LSB method.

Abstract - Steganography is one of the most powerful techniques for hiding the existence of secret data hidden in the cover of objects. Image is the most popular cover object for Steganography and in steganography this working image is adopted. Embedding classified information in images required intensive computation, and therefore, designed Steganography to accelerate the speed of Steganography tools. It is implemented using an ARM7TDMI and GSM 900 processor. There are several techniques for hiding the information in the cover image. The spatial domain technique manipulates the cover image pixel bit value to embed classified information. The secret bits are written directly to the cover image pixel bytes. As a result, spatial domain techniques are simple and easy to apply. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography. In this study, a new technique of LSB steganography has been proposed which is an improvised version of the one-bit LSB technique. There is also the aim of research to hide secret text messages into image files so that secret messages are safe because they have been stored in image files so that they make an alternative message delivery to avoid theft and sabotage.

Keywords - Steganography, embedded, Cover image, LSB method.

I. PENDAHULUAN

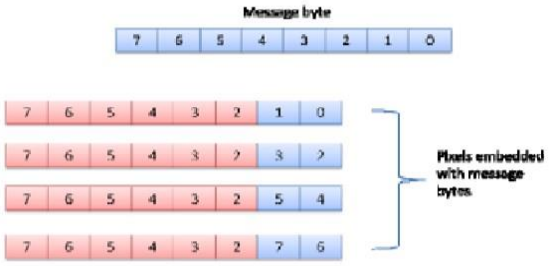
Teknik penyembunyian informasi yang banyak digunakan untuk keamanan data disebut Steganografi. Steganografi juga dapat menyembunyikan informasi rahasia berupa citra atau gambar dalam media digital [1]. Teknik yang digunakan untuk pengamanan informasi pada Steganografi dengan menyembunyikan informasi dengan metode tertentu ke dalam media digital agar perbedaannya tidak kelihatan secara visual antara file asli dengan file yang sudah disisipi informasi (stegoimage) sehingga tidak akan diketahui steganalis (orang yang dapat memecahkan stegoimage tanpa mengetahui kunci yang digunakan) [2]. Metode Least Significant Bit merupakan metode yang menukar bit pixel pada medium penampung dengan setiap bit pesan yang akan disembunyikan [3]. Least Significant Bit (LSB) umum digunakan dalam enkripsi dan dekripsi informasi rahasia. Metode LSB ini bekerja dengan mengubah bit redundan cover image yang tidak berpengaruh signifikan dengan bit dari pesan rahasia [4].

Telah ada beberapa penelitian dalam menyembunyikan data di dalam gambar menggunakan teknik steganografi. Penelitian Hermansa, dkk. yaitu Implementasi Algoritma

Playfair Cipher dan Least Significant Bit pada Citra Digital. Untuk metode steganografi Least Significant Bit (LSB) dalam menyisipkan pesan rahasia atau embedded sulit untuk ditebak secara kasat mata melihat perubahan yang terjadi tidak terlalu signifikan antara sebelum dan sesudah gambar disisipkan [5]. Perbandingan Hasil Impelementasi steganografi Dan Kriptografi Menggunakan LSB (Least Significant Bit) dengan EOF (End Of File), penelitian Santoso dan AlHadi disimpulkan bahwa dengan metode LSB (Least Significant Bit) dan EOF (End Of File) ini, image yang disisipkan pesan, file dan dokumen dari segi tampilan tidak terlihat perbedaan dengan image aslinya [6]. Kemudian pada penelitian Fikhri dan Hendrawaty dengan judul Implementasi Steganografi Text To Image Menggunakan Metode One Bit Least Significant Bit Berbasis Android. Penyisipan berbagai macam pesan teks ke dalam 5 buah cover image dengan normalisasi 900x900 pixel semuanya berhasil dilakukan, sehingga tingkat keberhasilan proses penyisipan pesan teks dari sampel yang dilakukan adalah 100 %, dengan rata-rata waktu penyisipan 0,009 detik [7]. Penelitian Mulyanto, dkk. dengan judul Penyisipan Pesan Teks pada Citra Menggunakan Metode LSB dan 2-Wrap Length. Hasil penelitian menunjukkan semakin besar citra cover, nilai MSE yang dihasilkan cenderung lebih kecil, dan nilai PSNR cenderung lebih besar. Kualitas citra hasil penyisipan lebih bagus pada citra yang berukuran lebih besar dibandingkan pada citra yang berukuran lebih kecil. Semakin besar dimensi citra yang digunakan sebagai media cover akan dapat menampung banyak pesan yang dapat disisipkan. Semakin sedikit karakter yang disisipkan maka semakin tinggi tingkat keberhasilan kembalinya pesan [8]. Selanjutnya penelitian darwis dan kisworo dengan judul Teknik Steganografi Untuk Penyembunyian Pesan Teks Menggunakan Algoritma End Of File. Pengujian imperectibility memberikan hasil steganografi pada gambar, dengan metode kuesioner yang menghasilkan 70% mahasiswa dibidang komputer tidak mengetahui tentang Steganografi dan 100% menyatakan gambar hasil steganografi tidak dapat terlihat oleh indra mata manusia secara kasat mata. Pada proses pengujian tahap fidelity tidak nampak nilai MSE yang hanya menghasilkan nilai "0" dan PSNR menghasilkan nilai "∞" (tak hingga) dikarenakan metode yang digunakan menyisipkan pesan di akhir file tanpa merubah nilai intensitas warna pikselnya [9]. Penelitian Kamali, dkk. dengan judul Steganografi Ganda pada Citra Berbasiskan Metode LSB Dan DCT Dengan Menggunakan Deret Fibonacci. Hasil citra stego jika dilihat secara kasat mata tidak terlihat perbedaan. Begitu juga jika dibandingkan dengan perhitungan PSNR. Pada penyisipan level pertama rata – rata nilai PSNR adalah 52,279 dB dan rata – rata PSNR pada penyisipan level kedua adalah 56,342 dB. Keduanya menunjukan nilai PSNR di atas 40 dB, menunjukan bahwa citra hasil stego memiliki perbedaan yang sedikit dibandingkan dengan citra asli [10].

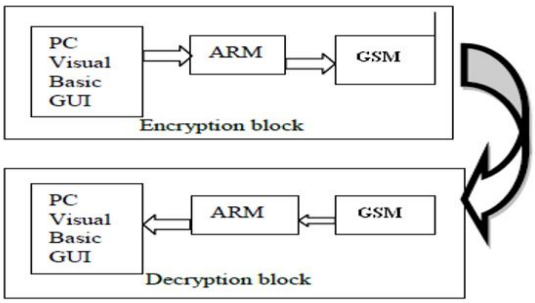
II. METODE PENELITIAN

LSB adalah bit signifikan terendah dalam nilai byte dari piksel gambar. Steganografi gambar berbasis LSB menyematkan rahasia dalam bit terkecil dari nilai-nilai pixel dari gambar sampul.



Gambar 1. *Proposed LSB Algorithm*

Pada gambar 1 Konsep LSB Embedding sederhana. Ini mengeksploitasi fakta bahwa tingkat ketepatan dalam banyak format gambar jauh lebih besar daripada yang dapat dipahami oleh visi manusia rata-rata. Oleh karena itu, gambar yang diubah dengan sedikit variasi pada kolomnya tidak dapat dibedakan dari aslinya oleh manusia, hanya dengan melihatnya. Dalam teknik LSB konvensional, yang membutuhkan delapan byte piksel untuk menyimpan 1 byte data rahasia tetapi dalam teknik LSB yang diusulkan, hanya empat byte piksel yang cukup untuk menampung satu byte pesan. Sisa bit dalam piksel tetap sama. Untuk keamanan, hanya enkripsi yang mungkin tidak cukup, maka pro-posed project termasuk Steganography dimana data yang dienkripsi disembunyikan ke dalam gambar dan kemudian gambar ditransmisikan dalam jaringan.

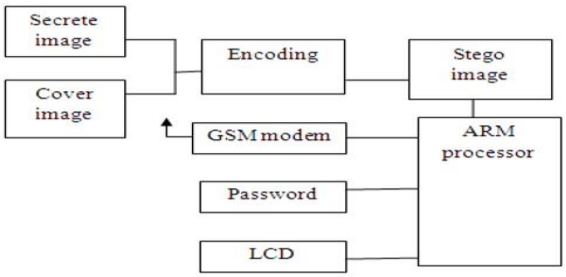


Gambar 2. *Experimental block diagram*

Pada gambar 2, Algoritma Least Significant Bit untuk steganografi gambar. Diagram blok seperti yang ditunjukkan terutama berisi mengikuti blok.

1. Komputer pribadi (PC)
2. ARM7TDMI

3. GSM 900

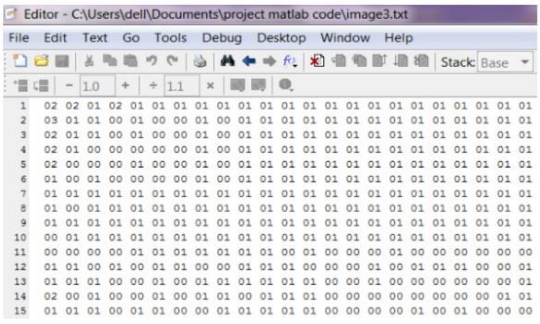


Gambar 3 : *Block diagram of Encryption*

Proses enkripsi pada gambar 3 yaitu baca gambar rahasia dan cover dan ubah menjadi gambar skala abu-abu, kemudian periksa ukuran gambar rahasia dengan gambar penutup sehingga ukuran gambar rahasia harus kurang dari gambar sampul. Mengkodekan gambar rahasia ke dalam biner menggunakan perintah bit gate dan membaginya menjadi bagian-bagian RGB kemudian mengganti bit-bit MSB dari gambar rahasia menjadi bit-bit LSB dari gambar cover. Sembunyikan kata sandi dengan gambar Stego dan kirim menggunakan modem GSM. Proses dekripsi: Proses sebaliknya terjadi di bagian penerima, gambar Stego dapat didekripsi menggunakan kata sandi.

MATLAB adalah bahasa berkinerja tinggi untuk komputasi teknis. Fungsi Matlab adalah mudah digunakan, fungsi antarmuka pengguna yang memandu pengguna melalui proses baik en-coding & decoding pesan ke atau dari gambar masing-masing. Dalam karya ini, Matlab diimplementasikan untuk memproses teknik steganografi LSB dengan ukuran frame yang berbeda 256 * 256, 128 * 128, 64 * 64 dan hasil simulasi ditampilkan. Ada tiga langkah utama yang terlibat dalam menerapkan steganografi LSB seperti berikut ini.

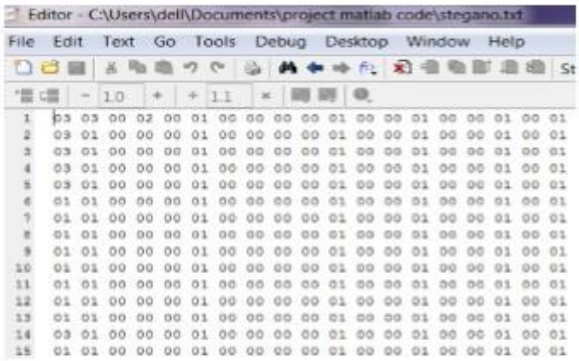
1. Conversion of image to matrix



Gambar 4. *Intensity values of cover image*

Pada gambar 4, nilai intensitas gambar penutup yang diperoleh selama konversi gambar ke matriks diwakili. Dalam proses konversi gambar ke matriks, kita mengonversi gambar penutup input ke nilai matriks yang disimpan dalam file teks. Pertama-tama gambar dibaca dari komputer, gambar aslinya dalam bentuk RGB yang diubah menjadi gambar abu-abu. Gambar abu-abu diubah ukurannya menjadi ukuran tertentu 256 * 256. Setiap gambar memiliki nilai intensitas untuk setiap piksel, di sini nilai intensitas ini disimpan ke dalam file teks.

2. Embedding process



Gambar 5. *Intensity values of stegano-image*

Pada gambar 5 ditunjukkan nilai intensitas gambar em-bedded. Setelah selesai gambar ke matriks langkah selanjutnya adalah menanamkan pesan ke dalam gambar. Gambar yang diperoleh selama proses ini disebut sebagai gambar stegano-embed. Pesan tertanam ke dalam nilai intensitas gambar yang diperoleh selama gambar ke konversi matriks.

3. Conversion of matrix to image

Pada tahap ini nilai intensitas diubah kembali ke gambar. Citra yang didapat memiliki pesan yang tertanam di dalamnya. Citra cov-er dan gambar yang diperoleh di sini harus identik. Oleh karena itu tujuan Steganografi terpenuhi.

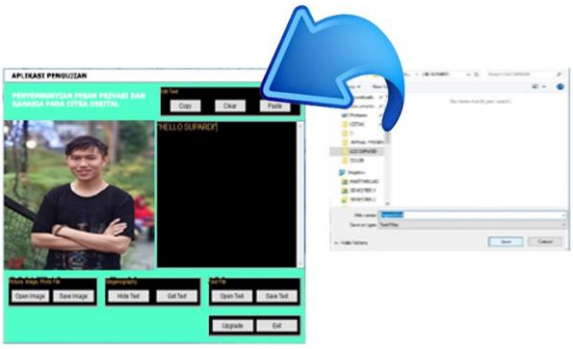
III. HASIL DAN PEMBAHASAN

Penyertaan Least Significant Bit (LSB) adalah strategi sederhana untuk menerapkan steganografi. Seperti semua metode steganografi, ia menyematkan data ke dalam sampul sehingga tidak dapat dideteksi oleh pengamat biasa. Teknik ini bekerja dengan mengganti beberapa informasi dalam piksel yang diberikan dengan informasi dari data dalam gambar. Meskipun dimungkinkan untuk menanamkan data ke dalam gambar pada setiap bit-plane, embedding LSB

dilakukan pada bit yang paling tidak signifikan. Ini meminimalkan variasi warna yang diciptakan oleh embedding. Langkah-langkah berikut menggambarkan bagaimana metode LSB ini digunakan untuk menyembunyikan pesan "HALLO SUPARDI" dalam gambar "Supardi.bmp" dengan menggunakan software dan ketentuan cara proses penginstalan [11].

Gambar 6. Tampilan memasukkan text pesan

Pada gambar 6 menampilkan menu mempersiapkan foto/gambar dimana proses yang dilakukan adalah memasukkan text menyesuaikan kebutuhan dan kepentingan yang akan disisipkan pada foto dengan ketentuan *Image* (*.bmp) secara defaultnya.



Gambar 7. Tampilan proses penyimpanan gambar

Gambar 7 menjelaskan proses yang dilakukan untuk tempat penyimpanan file yang akan di *save* dengan memberikan nama file.txt, dan dipastikan proses dapat dilakukan sampai berhasil.

Gambar 8. Tampilan Proses Hide Text

Selanjutnya pada gambar 8 dilakukan proses menyembunyikan text yang sudah disiapkan kemudian akan muncul pesan artinya pesan teks sekarang tersembunyi di dalam gambar.

IV. KESIMPULAN DAN SARAN

Berdasarkan hasil dari penelitian maka dapat dihasilkan simpulan bahwa steganografi dengan menggunakan metode LSB dapat menyisipkan informasi kedalam media citra digital pada bagian akhir file gambar. Dengan teknik penyembunyian pesan teks rahasia kedalam file gambar sehingga pesan rahasia menjadi aman karena sudah disimpan didalam file gambar terbukti dapat menjadikan alternatif pengiriman pesan agar terhindar dari pencurian dan sabotase.

Berdasarkan simpulan dari hasil penelitian yang telah diuraikan, maka saran yang dapat diberikan untuk pengembangan lebih lanjut dari penelitian ini adalah teknik steganografi dapat dibangun dengan berbagai macam media penyisipan seperti audio maupun video untuk penelitian selanjutnya. Aplikasi ini diharapkan dapat diterapkan dengan format citra lainnya seperti PNG, GIF, dll sehingga menjadikan lebih dinamis.

DAFTAR PUSTAKA

[1] S. Lutfi and R. Rosihan, "Perbandingan Metode Steganografi LSB (Least Significant Bit) Dan MSB (Most Significant Bit) Untuk Menyembunyikan Informasi Rahasia Kedalam Citra Digital," *JIKO (Jurnal Inform. dan Komputer)*, vol. 2, no. 1, pp. 34–42, 2018, doi: 10.33387/jiko.v1i1.1169.

[2] M. Sri Pebriyani Manurung, "Penerapan Algoritma Advanced Encryption Standard dalam Mengamankan File pada Citra dengan Metode Least Significant Bit," *J. Tek. Inform. Unika St. Thomas*, vol. 04, no. 01, pp. 62–69, 2019.

[3] Hermansa, R. Umar, and A. Yudhana, "Analisis Sistem Keamanan Teknik Kriptografi dan Steganografi Pada Citra Digital (BITMAP)," *Semin. Nas. Teknol. Fak. Tek. Univ. Krisnadwipayana*, pp. 520–528, 2019.

[4] I. W. Ardiyasa, "Implementasi Teknik Data Hidding Untuk Pengamanan Pesan Rahasia Pada Media Digital," in *Seminar Nasional Sistem Informasi dan Teknologi Informasi 2018*, 2018, pp. 601–605.

[5] Hermansa, R. Umar, and A. Yudhana, "Implementasi Algoritma Playfair Cipher dan Least Significant Bit pada Citra Digital," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 3, pp. 454–461, 2020.

[6] B. Widia Santoso and F. Reza AlHadi, "Perbandingan Hasil Impelementasi Steganografi dan Kriptografi Menggunakan LSB (Least Significant Bit) dengan EOF (End Of File)," *J. ICT Learn.*, vol. 3, no. 1, pp. 81–97, 2017.

[7] A. A. Fikhri and Hendrawaty, "Implementasi Steganografi Text To Image Menggunakan Metode One Bit Least Significant Bit Berbasis Android," *J. Infomedia*, vol. 3, no. 1, pp. 10–17, 2018.

[8] Mulyanto, R. Vincentius Febriyana, and A. Bramanto Wicaksono Putra, "Penyisipan Pesan Teks pada Citra Menggunakan Metode LSB dan 2-Wrap Length," in *Seminar Nasional APTIKOM (SEMNASTIK) 2019*, 2019, pp. 536–543.

[9] D. Darwis and Kisworo, "Teknik Steganografi Untuk Penyembunyian Pesan Teks Menggunakan Algoritma End Of File," *J. Sist. Inf. dan Telemat.*, vol. 8, no. 2, pp. 98–108, 2017.

[10] M. H. Al Kamali, B. Hidayat, and N. Andini, "Steganografi Ganda pada Citra Berbasiskan Metode LSB Dan DCT Dengan Menggunakan Deret Fibonacci," in *Seminar Nasional Teknologi Informasi dan Multimedia 2018*, 2018, pp. 37–42.

[11] A. Amir Alkodri and B. Isnanto, *Buku Ajar Pengelolaan Instalasi Komputer*. Yogyakarta: Graha Ilmu, 2019.