JTS : Jurnal Teknik
P-ISSN: 2302-8734
E-ISSN: 2581-0006

Vol. 14 No. 01 Th. 2025
Halaman : 39 - 44
26 Februari 2025.

Studi Dan Implementasi Steganografi Pada Citra PNG Dengan Metode Least-Significant Bit (LSB) Mengunakan Java

M. Luthfi Aksani,Lukman Azhari, Fauyhi Eko Nugroho
[1,2,3,] Muhammadiyah Tangerang, Jalan Perintis Kemerdekaan I Babakan No.33, RT.007/03, Cikokol, Kec.Tangerang, Kota Tangerang, Banten 15118, Telp: (021)557 93251
e-mail:luthfi.aksani@ft-umt.ac.id

Receive: 11-01-2025 Accepted: 25-02-2025

ABSTRAK

Informasi adalah sebuah data mentah yang telah dipilah sedemikian rupa sehingga memiliki manfaat informatif bagi sebagian maupun banyak pihak. Dan di era internet ini, transaksi informasi merupakan hal yang lumrah dilakukan di dunia maya. Hal yang sering dilupakan oleh para user internet adalah keamanan data. Dimana informasi di internet sifatnya adalah terbuka, dengan kemungkinan akses oleh user dari seluruh dunia. Dalam kasus yang sensitif, beberapa informasi ditujukan hanya untuk user atau pihak tertentu, dalam hal inilah diperlukan suatu proteksi untuk melindungi informasi dari pihak-pihak yang tidak berhak mengaksesnya. Perkembangan komputer dan perangkat pendukung lainnya yang serba digital, telah membuat data-data digital semakin banyak digunakan. Disisi lain kemudahan tersebut telah memunculkan masalah di sekitar hak cipta dan hak kepemilikan materi digital. Teknik hidden message (steganografi), adalah suatu teknik yang mengijinkan para pengguna untuk menyembunyikan suatu pesan didalam pesan yang lain. Dengan kemampuan tersebut maka informasi hak cipta seperti identitas seorang pengarang, tanggal ciptaan, dan lain-lain dapat disisipkan/disembunyikan kedalam berbagai macam variasi jenis dokumen besar seperti: gambar, audio , video, text atau file biner. Penelitian ini membahas steganografi dengan menggunakan Teknik Dynamic Cell Spreading yang merupakan teknik menyembunyikan/menyisipkan data dengan bantuan buffer memori sebagai media penggabungan.
Kata kunci: Steganografi, citra digital, file gambar bmp, Java, Metode LSB

ABSTRACT

Information is raw data that has been sorted in such a way that it has informative benefits for some or many parties. And in this internet era, information transactions are commonplace in cyberspace. The thing that internet users often forget is data security. Where information on the internet is open, with the possibility of access by users from all over the world. In sensitive cases, some information is intended only for certain users or parties, in this case a protection is needed to protect the information from parties who do not have the right to access it. The development of computers and other supporting devices that are all-digital, has made digital data increasingly used. On the other hand, this convenience has raised problems around copyright and ownership rights of digital materials. Hidden message technique, is a technique that allows users to hide a message from another message. With this ability, copyright information such as the identity of an author, the date of creation, and others can be inserted/hidden into a variety of large document types such as: images, audio, video, text or binary files. This study discusses steganography using the Dynamic Cell Spreading Technique which is a technique of hiding/inserting data with the help of memory buffers as a joining medium.
Keywords: Steganography, digital imagery, bmp image file, Java, LSB Method

PENDAHULUAN

Keamanan suatu informasi pada saat ini tidak akan ada habisnya jika dibahas karena telah menjadi suatu kebutuhan yang sangat penting. Kebutuhan keamanan akan semakin meningkat jika informasi tersebut mengandung nilai – nilai bisnis, privasi, ataupun kepentingan tertentu. Terlebih lagi, aksi penyalahgunaan informasi (hacking) dalam dunia maya semakin marak menyebabkan informasi tersebut harus dilindungi dari gangguan pihak – pihak yang tidak berkepentingan.

Salah satu cara yang paling sering digunakan adalah dengan mengenkripsi informasi – informasi tersebut, yang disebut dengan kriptogrfi. Metode lainnya yaitu dengan menyembunyikan data rahasia tersebut di dalam data yang lain. Teknik ini disebut dengan steganografi. Berbeda dengan teknik kriptografi yang dengan mudah dideteksi keberadaanya (walaupun sulit untuk dimengerti), steganografi

menyamarkan keberadaan dari informasi (data) yang ingin disampaikan ke dalam media penyamar, misalnya media yang berbentuk berkas multimedia.

Masalah yang dapat dirumuskan dari latar belakang di atas adalah bagaimana membangun suatu aplikasi steganografi pada citra digital file gambar bitmap yang efisien, bagaimana mengeksploitasi keterbatasan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada file gambar yang belum disisipi pesan rahasia, sehingga dengan keterbatasan tersebut manusia sulit menemukan gradasi penurunan kualitas warna file gambar yang telah disisipi pesan rahasia.Tujuan yang di harapkan antara lain menganalisa teknik steganografi pada citra digital file gambar bitmap untuk menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi dan menghasilkan file gambar yang mempunyai kualitas tidak jauh berbeda dengan citra digital file gambar aslinya, sehingga pesan terlihat hanya seperti pesan biasa saja.

METODE PENELITIAN

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan.

Kata "steganografi" berasal dari bahasa Yunani steganos, yang artinya “tersembunyi atau terselubung”, dan graphein, “menulis”. Kini, istilah steganografi termasuk penyembunyian data digital dalam berkas-berkas (file) komputer. Contohnya, si pengirim mulai dengan berkas gambar biasa, lalu mengatur warna setiap pixel ke-100 untuk menyesuaikan suatu huruf dalam alphabet (perubahannya begitu halus sehingga tidak ada seorangpun yang menyadarinya jika ia tidak benar-benar memperhatikannya).Pada umumnya, pesan steganografi muncul dengan rupa lain seperti gambar, artikel, daftar belanjaan, atau pesan-pesan lainnya.

Pesan yang tertulis ini merupakan tulisan yang menyelubungi atau menutupi. Contohnya, suatu pesan bisa disembunyikan dengan menggunakan tinta yang tidak terlihat di antara garis-garis yang kelihatan.Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia (teks atau gambar) di dalam berkas-berkas lain yang mengandung teks, image, bahkan audio tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari berkas semula. **Metode Steganography**[4] Sudah banyak metode yang digunakan untuk menyembunyikan pesan di dalam sebuah image tanpa mengubah tampilan image, sehingga pesan yang disembunyikan tidak akan terlihat. Berikut akan dibahas beberapa metode umum yang digunakan pada image steganography. Kata steganografi berasal dari bahasa Yunani steganos (στεγανός) yang berarti "ditutupi atau dilindungi", dan graphein (γράυειν) yang berarti "menulis". Dari asal katanya steganografi berarti "tulisan tersembunyi". Steganografi adalah seni dan ilmu menulis informasi tersembunyi sedemikian rupa sehingga tak seorang pun, selain pengirim dan penerima yang dituju, mengetahui keberadaan informasi tersebut. Secara umum, informasi akan muncul dalam bentuk yang lain: foto, artikel, daftar belanja, atau beberapa *covertext* lain. Secara klasik, informasi disembunyikan menggunakan tinta tak terlihat diantara garis-garis yang tampak dalam sepucuk surat pribadi.

Steganografi juga meliputi penyisipan informasi dalam *file* komputer. Dalam steganografi digital, komunikasi elektronik dapat mencakup pengkodean *steganographic* dalam lapisan transportasi, seperti *file* dokumen, *file* gambar, program atau protokol. *File* media sangat ideal untuk transmisi *steganographic* karena ukurannya yang besar. Sebagai contoh sederhana, pengirim mungkin mulai dengan *file* gambar yang tidak terlalu kompleks dan menyesuaikan warna setiap piksel 100 dengan huruf dalam alfabet. Karena perubahannya begitu halus, maka seseorang yang tidak secara khusus mencarinya tidak dapat melihat informasi yang disisipkan. Teknik steganografi yang digunakan pada proyek akhir ini adalah variasi *least significant bit substitution*, karena meskipun tergolong sederhana, namun dengan perpaduan algoritma yang tepat dapat menjadi teknik yang dapat diandalkan.

a. Penyisipan Least Significant Bit[2]

Cara paling umum untuk menyembunyikan pesan adalah dengan memanfaatkan Least-Significant Bit (LSB). Walaupun banyak kekurangan pada metode ini, tetapi kemudahan implementasinya membuat metode ini tetap digunakan sampai sekarang. Metode ini membutuhkan syarat, yaitu jika dilakukan kompresi pada stego, harus digunakan format lossless compression, karena metode ini menggunakan bit-bit pada setiap pikses pada image.

Jika digunakan format lossy compression, pesan rahasia yang disembunyikan dapat hilang. Jika digunakan image 24 bit color sebagai cover, sebuah bit dari masing-masing komponen Red, Green, dan Blue, dapat digunakan sehingga 3 bit dapat disimpan pada setiap piksel. Sebuah image 800 x 600 piksel dapat digunakan untuk menyembunyikan 1.440.000 bit (180.000 bytes) data rahasia. Misalnya, di bawah ini terdapat 3 piksel dari image 24 bit color :

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Jika diinginkan untuk menyembunyikan karakter A (10000001) dihasilkan :

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100110 11101001)

Dapat dilihat bahwa hanya 3 bit saja yang perlu diubah untuk menyembunyikan karakter A ini. Perubahan pada LSB ini akan terlalu kecil untuk terdeteksi oleh mata manusia sehingga pesan dapat disembunyikan secara efektif. Jika digunakan image 8 bit color sebagai cover, hanya 1 bit saja dari setiap piksel warna yang dapat dimodifikasi sehingga pemilihan image harus dilakukan dengan sangat hati-hati, karena perubahan LSB dapat menyebabkan terjadinya perubahan warna yang ditampilkan pada citra. Akan lebih baik jika image berupa image grayscale karena perubahan warnanya akan lebih sulit dideteksi oleh mata manusia.

b. Format *Portable Network Graphics* (.PNG)

PNG (*Portable Network Graphics*) adalah salah satu format penyimpanan citra yang menggunakan metode pemadatan yang tidak menghilangkan bagian dari citra tersebut (Inggris *lossless compression*).Untuk keperluan pengolahan citra, meskipun format PNG bisa dijadikan alternatif selama proses pengolahan citra - karena format ini selain tidak menghilangkan bagian dari citra yang sedang diolah (sehingga penyimpanan berulang ulang dari citra tidak akan menurunkan kualitas citra) PNG (Format berkas grafik yang didukung oleh beberapa web browser. PNG mendukung transparansi gambar seperti GIF, berkas PNG bebas paten dan merupakan gambar bitmap yang terkompresi.

Tabel 1. Perbandingan *JPEG*, *GIF* dan *PNG*

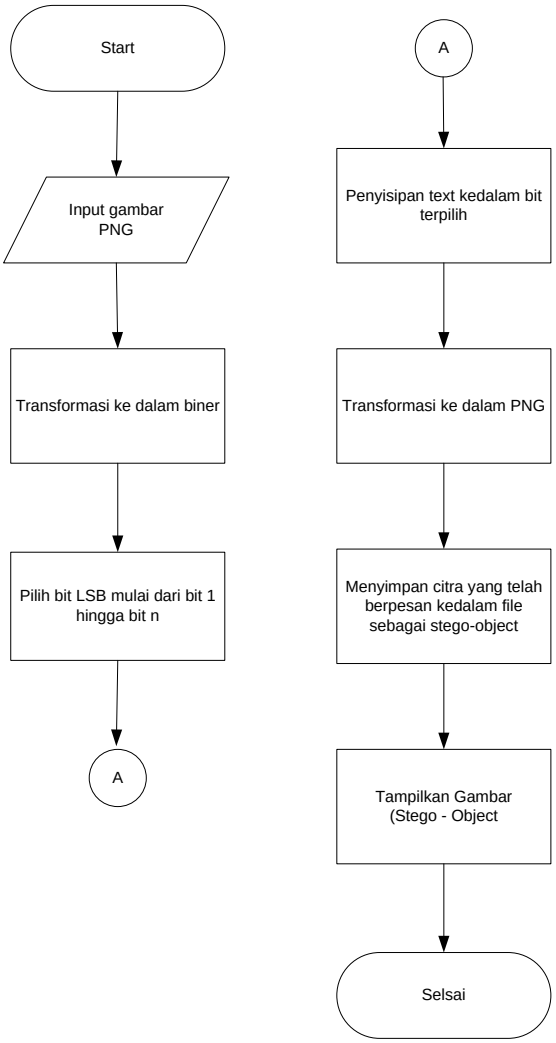
	JPEG	*GIF*	*PNG*
Teknik Kompresi	*Huffman, DCT*	*LZW*	*Deflate*
Lossy* atau *Lossless	*Lossy*	*Lossless*	*Lossless*
Warna	RGB, *grayscale*	*Indexed color*	*Indexed color, grayscale,* RGB
Warna Transparan	Tidak	Ya	Ya

JTS : Jurnal Teknik
P-ISSN: 2302-8734
E-ISSN: 2581-0006

Vol. 14 No. 01 Th. 2025
Halaman : 39 - 44
26 Februari 2025.

ANALIS DAN PEMBAHASAN DAN PERANCANGAN

Sistem steganografi yang dibahas akan di fokuskan kepada bagaimana cara membangun suatu sistem steganografi pada citra digital file gambar yang efisien dan untuk mengeksploitasi keterbatasan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada file gambar yang belum disisipi pesan rahasia. Sehingga dengan keterbatasan tersebut manusia sulit menemukan gradasi penurunan kualitas warna file gambar yang telah disisipi pesan rahasia. Sistem ini terdiri dari dua buah sub sistem yaitu : sistem penyisipan dan sistem pengekstrakkan. Sistem penyisipan berfungsi untuk melakukan proses penyembunyian pesan ke file citra digital gambar. Komponen dari sistem penyisipan ini yaitu terdapat komponen untuk menuliskan pesan yang dipakai untuk menempatkan penulisan pesan rahasia. Sistem pengekstrakkan berfungsi untuk melakukan pengekstrakkan file untuk memeperoleh pesan yang telah disisipkan ke dalam file gambar tersebut. Komponen pada sistem pengekstrakkan ini terdapat komponen untuk membaca baca pesan yang digunakan untuk menempatkan pesan rahasia yang akan dibaca, sehingga keluarannya akan memulai proses pemisahan pesan rahasia dari file gambar.



Gambar Diagram alir proses penyisipan pesan

KESIMPULAN

Beberapa kesimpulan yang dapat diambil adalah sebagai telah berhasil dikembangkannya perangkat lunak yang dapat melakukan steganografi pada citra terkompresi JPEG. Kebutuhan fungsional dari perangkat lunak, seperti proses penyisipan dan ekstraksi pesan, serta penggunaan kunci sudah dapat dilakukan dengan benar. Metode Spread Spectrum sebagai metode penyisipan pesan sudah dapat dilakukan dengan benar, yaitu melakukan proses spreading terhadap pesan, modulasi pesan dengan kunci, dan penyisipan pesan dalam matriks frekuensi yang terdapat pada citra terkompresi JPEG. Kualitas citra terkompresi JPEG yang dihasilkan bergantung dari besarnya ukuran pesan. Berdasarkan pengamatan yang dilakukan saat pengujian, citra JPEG yang disisipkan lebih banyak akan mengalami perubahan yang lebih besar.

DAFTAR REFERENSI

Cole, Eric. 2003. Hiding in Plainsight : Steganography and the Art of Covert Communication. Wiley Publishing,Inc.

Destriana, R., & Taufiq, R. (2023). TEORI SISTEM INDUSTRI.

Destriana, R., Husain, S. M., & Handayani, N. (2021). DIAGRAM UML DALAM MEMBUAT APLIKASI ANDROID FIREBASE" STUDI KASUS APLIKASI BANK SAMPAH".

Destriana, R., Kom, M., Husain, S. M., Kom, S., Handayani, N., Kom, M., ... & Kom, S. (2021). Diagram UML Dalam Membuat Aplikasi Android Firebase" Studi Kasus Aplikasi Bank Sampah". Deepublish.

Destriana, R. (2022). Enterprise Resource Planning Bagi Pemula (Teori dan Konseptual).

Destriana, R., Handayani, N., Husain, S. M., & Siswanto, A. T. P. (2021, March). A Research to Design, Develop and Implementation of Android Application System for Waste Bank Sharia Community at Kampung Hijau Kemuning. In IOP Conference Series: Materials Science and Engineering (Vol. 1115, No. 1, p. 012042). IOP Publishing.

Kirovski, D., Malvar, H.S. , “Microsoft Audio Watermarking Tool”, IEEE, 2003.

Kustiawan, D., Cholifah, W. N., Destriana, R., & Heriyani, N. (2022). Rancang Bangun Sistem Informasi Akuntansi Pengelolaan Koperasi Menggunakan Metode Extreme Programming. Jurnal Teknologi Dan Informasi, 12(1), 78-92.

Liesnaningsih, L., Taufiq, R., Destriana, R., & Suyitno, A. P. (2020). Sistem Pendukung Keputusan Penerima Beasiswa Berbasis WEB Menggunakan Metode Simple Additive Weighting (SAW) pada Pondok Pesantren Daarul Ahsan. Jurnal Informatika Universitas Pamulang, 5(1), 54-60.

Maulana, Ahmad Mansur, "Data Hiding Steganograph Pada File Image Menggunakan Metode Least Significant Bit", PENS-ITS, Surabaya, 2009

Fitriawati, N., Herdiansah, A., Taufiq, R., & Destriana, R. (2022). It Disaster Recovery Plan Dalam Mendukung Business Continuity Plan Saat Terjadi Force Majeure. JIKA (Jurnal Informatika), 6(3), 249-255.

Permana, A. A., Perdana, A. T., Handayani, N., & Destriana, R. (2021, March). A stunting prevention application "Nutrimo"(nutrition monitoring). In Journal of Physics: Conference Series (Vol. 1844, No. 1, p. 012023). IOP Publishing.

Nuraini, R., Destriana, R., Nurnaningsih, D., Daniarti, Y., & Alexander, A. D. (2023). Sunflower image classification using multiclass support vector machine based on histogram characteristics. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 7(1), 146-152.

Romdhoni, Muhamad Arif, "Kriptografi Visual Pada Citra Biner Dan Berwarna Serta Pengembangannya Dengan Steganografi Dan Fungsi Xor", Teknik Informatika ITB, Bandung,2008 .

Yanuardi, Y., & Destriana, R. (2020). Perancangan Sistem Informasi Penjualan Online Gas dalam Strategi E-business Menggunakan Analisis Swot. JIKA (Jurnal Informatika), 4(1), 1-6.