KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI

INSTITUT TEKNOLOGI DAN BISNIS PALCOMTECH

MAKALAH APLIKASI PENGOLAHAN CITRA DIGITAL TENTANG TEKNIK MENYEMBUNYIKAN DATA / INFORMASI PADA GAMBAR (STEGANOGRAFI)

Disusun Oleh :

ILHAMI PRADINI

011180199

Dosen Pembimbing :

Rendi Almaheri Adi P., S.Kom., M.Kom.

PALEMBANG

2023

DAFTAR ISI

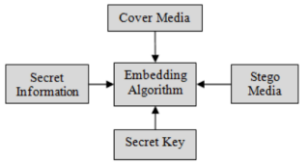
DAFTAR GAMBAR

1. Latar Belakang

Pesatnya pertumbuhan penggunaan internet melalui kapasitas *bandwidth* yang tinggi dan perangkat keras komputer berbiaya rendah telah mendorong pertumbuhan steganografi yang eksplosif (Goel, Rana, & Kaur, 2013). Steganografi adalah teknik yang digunakan untuk menyembunyikan keberadaan data dalam berbagai format seperti teks, gambar, audio, atau video (Siddiqui & Goswami, 2017). Ketika informasi yang dikirimkan dianggap sensitif, sangat penting untuk melindunginya dari pihak yang tidak berwenang. Oleh karena itu, sistem keamanan yang kuat harus dilibatkan. Steganografi adalah salah satu dari sistem keamanan yang dapat digunakan untuk mengamankan transmisi antar pengirim dan penerima (Beroual & Al-Shaikhli, 2018).

Steganografi sering disamakan dengan kriptologi karena keduanya mirip dalam cara keduanya digunakan untuk melindungi informasi penting (Chandramouli & Memon, 2003). Perbedaan keduanya adalah Steganografi melibatkan penyembunyian informasi sehingga nampaknya tidak informasi yang disembunyikan sama sekali. Jika seseorang atau beberapa orang melihat objek yang informasinya disembunyikan di dalamnya, dia tidak akan tahu bahwa ada informasi tersembunyi, oleh karena itu orang tersebut tidak akan berusaha melakukan dekripsi informasi. Steganografi pada dasarnya mengeksploitasi persepsi manusia. Indra manusia tidak terlatih untuk mencari file yang terdapat informasi tersembunyi di dalamnya (Bandyopadhyay, Bhattacharyya, Ganguly, Mukherjee, & Das, 2008).

Teks, gambar digital, audio digital dan video digital telah menjadi objek utama untuk menyembunyikan data. Berikut ini adalah beberapa istilah umum yang perlu untuk diketahui mengenai sistem steganografi yang juga diilustrasikan pada Gambar 1 (Choudry & Wanjari, 2015; Tripathi, Singh, & Singh, 2016).



Gambar 1. Proses Steganografi

- *Cover Media*: Media dimana informasi rahasia ditanam sedemikian rupa sehingga sulit untuk dideteksi keberadaannya.
- *Stego-Media*: Media yang diperoleh setelah menanamkan informasi rahasia.
- *Secret data*: Data atau informasi yang akan disembunyikan di *cover media*.
- *Steganalysis*: Proses mendeteksi keberadaan data rahasia di *cover media*.

Ada banyak teknik steganografi, steganografi gambar adalah teknik yang banyak digunakan dibandingkan dengan yang lain karena kesederhanaannya dan memiliki cara termudah untuk menyembunyikan data dalam gambar (Al-Husainy, 2011). Pendekatan sederhana untuk menanamkan informasi dalam gambar adalah menggunakan metode *Least Significant Bits* (LSB). Kekuatan metode *Least Significant Bits* (LSB) adalah kesederhanaan perhitungan dan sejumlah besar data dapat disembunyikan dalam gambar aslinya dengan tingkat visual yang tinggi (Siddiqui & Goswami, 2017).

Menurut Poornima & Iswarya, metode *Least Significant Bits* (LSB) adalah teknik umum dalam mengenkripsi dan mendekripsi informasi rahasia. Metode LSB didasarkan pada mengubah bit-bit redundan dengan tingkat kepentingan paling rendah dengan bit-bit informasi rahasia. Tujuan LSB adalah untuk mengirimkan informasi rahasia ke penerima tanpa membuat curiga penyusup bahwa pesan sedang disampaikan (Poornima & Iswarya, 2013).

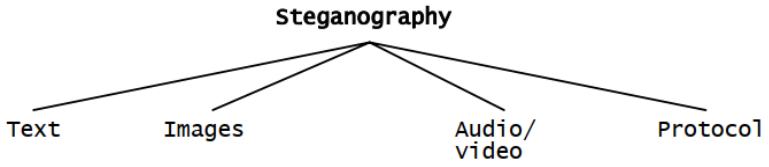
LSB menggunakan format file BMP 24-bit cocok dan efisien karena gambar BMP sudah memiliki kualitas yang bagus dan resolusi tinggi sehingga informasi yang disembunyikan tidak dapat dideteksi mata manusia.

Berdasarkan uraian diatas, maka penelitian ini bertujuan untuk membuat suatu aplikasi steganografi pada citra digital menggunakan metode metode *Least Significant Bits* (LSB) yang dapat diterapkan untuk kebutuhan keamanan data.

2. Tinjauan Pustaka

Hampir semua format file digital dapat digunakan untuk steganografi, tetapi format yang lebih cocok adalah format dengan tingkat redundansi yang tinggi.

Gambar 2 menunjukkan empat kategori utama format file yang dapat digunakan untuk steganografi (Morkel, Eloff, & Olivier, 2005).



Gambar 2. Kategori Steganografi

Steganografi teks menggunakan file digital tidak sering digunakan karena file teks memiliki jumlah redundan yang sangat kecil. Gambar adalah objek paling populer yang digunakan untuk steganografi. Di domain digital, terdapat banyak format file gambar yang berbeda, sebagian besar untuk aplikasi tertentu. Untuk format file gambar yang berbeda ini, terdapat berbagai algoritma steganografi.

Untuk menyembunyikan informasi dalam file audio, dapat menggunakan teknik serupa untuk file gambar. Satu teknik berbeda untuk audio steganografi adalah masking, yang mengeksploitasi sifat-sifat telinga manusia untuk menyembunyikan informasi tanpa disadari.

Istilah protokol steganografi mengacu pada teknik menanamkan (*embedding*) informasi dalam pesan dan protokol kendali jaringan yang digunakan dalam transmisi jaringan (Ahsan & Kundur, 2002).

Mengingat semakin banyaknya gambar digital, terutama di internet dengan tingkat redundansi yang berlebihan dalam representasi digital dari suatu gambar, maka penelitian ini akan fokus dalam menyembunyikan informasi pada gambar (citra digital) dengan referensi dari beberapa penelitian sebelumnya mengenai steganografi pada gambar (citra digital).

Prabowo, Hidayatno, & Christiyono menerapkan *discrete cosine transform* dan *chaos theory* untuk membuat suatu sistem berbasis pengolahan citra yang dapat digunakan untuk melakukan steganografi data rahasia digital (citra, teks, atau suara) pada media penampung citra digital, serta untuk mengetahui kinerja program tersebut dan keandalannya terhadap berbagai operasi manipulasi data. (Prabowo, Hidayatno, & Christiyono, 2012).

Edisuryana, Isnanto, & Somantri dalam penelitiannya mengimplementasikan teknik kriptografi dan steganografi pada citra berformat bitmap dengan menggunakan metode *end of file* (EOF). Metode kriptografi yang digunakan adalah *caesar cipher* dan *zig-zag cipher*. Berdasarkan penggunaan aplikasi, didapatkan hasil bahwa pada tahap enkripsi dengan metode *caesar chiper* perlu diperhatikan karakter pesan dan karakter pengganti spasi agar tidak saling tumpang tindih. Steganografi dengan menggunakan metode *end of file* (EOF) tidak merusak kualitas dari citra asli/citra cover, sehingga citra asli dengan citra stego nampak mirip dan sulit dibedakan secara kasat mata. Steganografi dengan menggunakan metode *end of file* (EOF) mengakibatkan ukuran citra yang disisipi pesan mengalami penambahan ukuran tinggi (Height) dan ukuran berkasnya (Edisuryana, Isnanto, & Somantri, 2013).

Marhaeni merancang aplikasi steganografi pada media citra digital terkompresi *joint photographic experts group* (jpeg) menggunakan aplikasi *stephy*. Dari hasil penelitian menunjukan bahwa menyembunyikan file di dalam gambar dapat membantu meningkatkan keamanan data (Marhaeni, 2017).

Siregar, Ramadhani, & Siregar mengimplementasikan steganografi pada citra digital menggunakan algoritma *diversity*. Dari hasil uji coba, diketahui bahwa dengan algoritma *diversity*, penyisipan dan ekstraksi pesan dapat dilakukan dengan baik (Siregar, Ramadhani, & Siregar, 2018).

Nurfauzan, Hidayat, & Saida menganalisis steganografi ganda pada citra digital menggunakan metode *discrete wavelet transform* dan *singular value decomposition* dengan penyisipan *spread spectrum image steganography*. Metode *spread spectrum image steganography* digunakan untuk metode penyisipan pertama pada domain spasial, sedangkan pada penyisipan kedua digunakan metode *discrete wavelet transform* untuk mentransformasi cover citra kedua ke domain frekuensi dan pesan disisipkan dengan memodifikasi singular value dengan menggunakan metode *singular value decomposition*. Hasil penelitian menunjukan stego-file yang dihasilkan memiliki *imperceptibility* dan *robustness* yang cukup baik. Hal ini diukur berdasarkan nilai PSNR dan SNR

pada kedua proses penyisipan, SSIM pada penyisipan kedua dan BER pada saat proses ekstraksi (Nurfauzan, Hidayat, & Saida, 2018).

Menyembunyikan informasi di dalam gambar adalah teknik yang populer saat ini. Pendekatan sederhana untuk menanamkan (*embedding*) informasi dalam gambar *cover* adalah dengan menggunakan metode *Least Significant Bits* (LSB) (Nosrati, Karimi, & Hariri, 2011).

Selain sederhana, metode *Least Significant Bits* (LSB) juga mudah diimplementasikan. Media penampungnya berupa gambar digital karena jumlahnya yang besar di internet. Kehandalan penggunaan citra dibandingkan dengan media lain adalah kualitas citra yang telah disisipi pesan rahasia tidak berbeda jauh dengan kualitas citra aslinya (Yenni, 2012).

Metode *Least Significant Bits* (LSB) bekerja pada bit yang terendah dari suatu deretan bit data. Penggunaan metode *Least Significant Bits* (LSB) ini dengan menyisipkannya pada bit rendah atau bit yang paling kanan pada data pixel yang menyusun gambar tersebut. Seperti di ketahui untuk file bitmap 24 bit di setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (*byte*) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111 (Mesran, 2012).

Dalam penelitian ini akan dibangun aplikasi steganografi pada media citra digital menggunakan metode *Least Significant Bits* (LSB), gambar berformat BMP (*bitmap*) 24-bit digunakan sebagai media untuk penyembunyian pesan, serta file pesan yang akan disembunyikan berupa teks ataupun dokumen (pdf, *word, excel, txt*) dalam betuk *file* rar sehingga informasi yang akan disampaikan terhadap orang lain tidak mudah diketahui oleh orang-orang yang tidak mempunyai hak untuk mengaksesnya, serta tanpa menimbulkan rasa keingintahuan seseorang terhadap informasi tersebut.

3. Teori Dasar Pengolahan Citra Digital

3.1. Konsep Dasar Pengolahan Citra

Pengolahan citra digital melibatkan serangkaian operasi dan teknik untuk memanipulasi citra digital, seperti filtering, segmentasi, dan ekstraksi fitur. Citra digital direpresentasikan dalam bentuk matriks piksel, di mana setiap elemen matriks mewakili intensitas cahaya pada lokasi piksel tertentu.

3.2. Representasi Citra Digital

Representasi citra digital melibatkan beberapa format seperti grayscale (hitam putih), RGB (warna), dan CMYK (untuk pencetakan). Dalam aplikasi ini, kami akan menggunakan format RGB yang paling umum, di mana setiap piksel direpresentasikan dengan tiga komponen warna: merah (R), hijau (G), dan biru (B).

3.3. Transformasi Citra Digital

Transformasi citra melibatkan perubahan citra dari domain spasial ke domain frekuensi, atau sebaliknya. Transformasi frekuensi umumnya digunakan untuk menganalisis spektrum frekuensi citra, sementara transformasi spasial digunakan untuk memodifikasi citra secara langsung.

4. Fungsi dan Operasi Dasar pada Citra Digital

Fungsi dan operasi dasar pada citra meliputi operasi aritmatika, operasi logika, operasi geometri, dan operasi statistik. Misalnya, operasi aritmatika dapat digunakan untuk menggabungkan dua citra, operasi logika untuk membandingkan atau memanipulasi piksel, operasi geometri untuk mengubah ukuran atau memutar citra, dan operasi statistik untuk menghitung statistik piksel.

5. Metode Penyembunyian Data dalam Citra Digital

5.1. Pengenalan Teknik Penyembunyian Data

Teknik penyembunyian data dalam citra bertujuan untuk menyembunyikan pesan atau data rahasia dalam citra digital secara tidak

terlihat bagi mata manusia. Dalam konteks ini, kita akan fokus pada teknik steganografi, yang mengenkripsi dan menyembunyikan pesan dalam citra dengan cara yang tidak dapat dideteksi secara visual.

5.2. Metode Steganografi

Steganografi memiliki beberapa metode yang dapat digunakan untuk menyembunyikan data dalam citra. Beberapa metode yang umum digunakan meliputi:

- Least Significant Bit (LSB): Teknik ini menggantikan bit terakhir dalam nilai piksel dengan bit pesan yang akan disembunyikan. Metode ini efektif pada citra dengan kualitas tinggi.
- Transformasi Domain: Metode ini melibatkan transformasi citra ke domain frekuensi, seperti transformasi Fourier atau transformasi kosinus diskrit, dan menyembunyikan pesan dalam koefisien frekuensi rendah.
- Metode Komplemen: Metode ini memanfaatkan perbedaan antara gambar asli dan gambar yang diubah untuk menyimpan pesan.

5.3. Metode Steganalisis

Steganalisis adalah teknik yang digunakan untuk mendeteksi keberadaan data tersembunyi dalam citra. Beberapa metode steganalisis umum meliputi analisis statistik, analisis frekuensi, dan penggunaan model prediktif untuk mengidentifikasi perubahan yang tidak wajar dalam citra.

5.4. Algoritma dan Protokol yang Digunakan

Algoritma steganografi LSB untuk menyembunyikan data dalam citra. Algoritma ini melibatkan penggantian bit terakhir dalam nilai piksel dengan bit pesan yang akan disembunyikan. Untuk ekstraksi data, algoritma akan membaca bit terakhir dari setiap piksel dalam citra untuk mendapatkan pesan yang disembunyikan.

6. Implementasi Aplikasi Pengolahan Citra Digital

6.1. Desain Aplikasi

Aplikasi akan memiliki antarmuka pengguna sederhana yang memungkinkan pengguna untuk memilih citra yang akan digunakan sebagai media untuk menyembunyikan data. Aplikasi akan memberikan pilihan untuk menyembunyikan pesan teks atau file dalam citra, dan juga untuk mengekstraksi kembali pesan dari citra.

6.2 Implementasi Algoritma Penyembunyian Data

Algoritma penyembunyian data akan mengambil citra dan pesan sebagai input. Citra akan dimodifikasi dengan mengganti bit terakhir setiap piksel sesuai dengan bit pesan yang akan disembunyikan. Hasilnya adalah citra yang telah mengandung pesan yang disembunyikan.

6.3 Implementasi Algoritma Ekstraksi Data

Algoritma ekstraksi data akan mengambil citra yang telah mengandung pesan sebagai input. Algoritma ini akan membaca bit terakhir setiap piksel dalam citra untuk mengembalikan pesan yang disembunyikan.

6.4 Uji Coba dan Evaluasi Kinerja Aplikasi

Aplikasi akan diuji dengan menggunakan berbagai citra dan pesan. Kinerja aplikasi akan dievaluasi berdasarkan waktu eksekusi dan keberhasilan dalam menyembunyikan dan mengekstraksi kembali pesan tanpa mengurangi kualitas visual citra.

7. Studi Kasus

7.1 Contoh Penggunaan Aplikasi dalam Kehidupan Sehari-hari

Aplikasi ini dapat digunakan dalam berbagai konteks, seperti menyembunyikan pesan rahasia dalam gambar profil media sosial, menyembunyikan informasi penting dalam gambar dokumen, atau mengamankan data rahasia dalam gambar yang dikirim melalui email.

7.2 Analisis dan Interpretasi Hasil

Hasil dari pengujian dan evaluasi kinerja aplikasi akan dianalisis untuk mengevaluasi efektivitas teknik penyembunyian data yang digunakan. Kelebihan, kelemahan, dan potensi pengembangan lebih lanjut akan dibahas.

8. Kesimpulan

8.1 Ringkasan Proyek

Proyek ini berhasil mengembangkan aplikasi pengolahan citra digital dengan teknik penyembunyian data. Aplikasi ini memungkinkan pengguna untuk menyembunyikan pesan dalam citra menggunakan algoritma steganografi LSB, serta mengekstraksi kembali pesan dari citra.

8.2 Hasil yang Dicapai

Hasil proyek ini adalah aplikasi yang dapat digunakan untuk menyembunyikan dan mengekstraksi data dalam citra digital dengan menggunakan teknik steganografi.

8.3 Saran

Pengembangan lebih lanjut dapat dilakukan untuk meningkatkan kinerja aplikasi, seperti mengimplementasikan teknik steganografi yang lebih canggih, meningkatkan antarmuka pengguna, atau mendukung format citra yang lebih luas.