NAMA : M.ILHAM RIZKI AL-FARIZ

NPM :011200035

PROJECT MANDIRI PENGOLAHAN CITRA DIGITAL

PENGANTAR :

Menyembunyikan data atau informasi dalam gambar umumnya melibatkan teknik steganografi. Steganografi adalah ilmu tentang cara menyembunyikan pesan atau data dalam suatu media, seperti gambar, tanpa menarik perhatian orang lain.

STEGANOGRAFI:

Steganografi adalah ilmu atau seni menyembunyikan pesan, data, atau informasi rahasia dalam suatu media (seperti gambar, audio, video, atau teks) tanpa menarik perhatian orang lain yang melihat atau mendengarkan media tersebut. Konsep steganografi telah digunakan sejak ribuan tahun yang lalu sebagai cara untuk mengamankan komunikasi rahasia dalam bentuk tulisan di benda-benda yang tampak umum, seperti pada gulungan papirus di era Mesir kuno.

Tujuan utama dari steganografi adalah membuat pesan tersembunyi tetap tidak terdeteksi oleh mata atau alat analisis biasa, sehingga hanya penerima yang dituju yang dapat menemukan dan membaca pesan tersebut. Perbedaan utama antara steganografi dan kriptografi adalah bahwa kriptografi berfokus pada enkripsi pesan untuk membuatnya tidak dapat dibaca tanpa kunci, sementara steganografi berfokus pada menyembunyikan pesan sehingga tidak dapat ditemukan.

Penerapan Steganografi pada Gambar:

Steganografi pada gambar adalah salah satu bentuk yang paling umum dan populer. Hal ini terutama karena gambar sering digunakan untuk berbagai tujuan, seperti media penyimpanan dan berbagi informasi. Teknik yang paling sederhana dalam steganografi gambar adalah menggunakan metode LSB (Least Significant Bit), seperti yang telah dijelaskan sebelumnya. Dengan menyisipkan data dalam bit paling tidak signifikan dari setiap piksel gambar, kita dapat menyembunyikan pesan atau informasi secara tidak terlihat.Meskipun steganografi dapat digunakan secara etis untuk tujuan seperti keamanan data, karya seni, atau watermarking, tetapi ada juga potensi penyalahgunaan, seperti dalam kasus menyembunyikan pesan teroris atau untuk tujuan ilegal lainnya. Oleh karena itu, beberapa negara memiliki undang-undang yang mengatur penggunaan dan penelitian tentang steganografi.

Tujuan Steganografi dalam Pengolahan Citra:

Keamanan Informasi: Tujuan utama steganografi dalam pengolahan citra adalah untuk menyembunyikan pesan atau informasi rahasia dalam citra, sehingga hanya penerima yang memiliki kunci atau algoritma dekripsi yang tepat yang dapat mengakses dan membaca pesan tersembunyi. Ini dapat digunakan untuk mengamankan komunikasi dan menyimpan informasi sensitif.Perlindungan Hak Cipta: Steganografi juga dapat digunakan untuk melindungi hak cipta dan mencegah penggunaan atau penyebaran tidak sah dari gambar atau konten digital lainnya. Dengan menyematkan watermark digital atau informasi hak cipta dalam gambar, pencipta dapat melacak penggunaan dan sumber gambar.

Aplikasi Steganografi dalam Pengolahan Citra:

Keamanan dan Intelijen: Steganografi dalam citra digunakan dalam aplikasi militer dan intelijen untuk menyembunyikan informasi rahasia dalam gambar yang hanya dapat diakses oleh pihak berwenang. Ini dapat digunakan dalam pertukaran informasi militer, penyebaran intelijen, dan komunikasi rahasia antara agen-agen pemerintah.

Watermarking Digital: Steganografi digunakan untuk menyematkan watermark digital dalam gambar untuk melindungi hak cipta, mengidentifikasi sumber, atau memberikan informasi tambahan tentang gambar tersebut. Watermarking juga digunakan dalam industri hiburan untuk melindungi hak cipta pada gambar, video, atau musik yang dipublikasikan secara daring.

Riset Medis: Steganografi dapat digunakan dalam bidang medis untuk menyembunyikan informasi penting dalam gambar medis seperti MRI atau CT scan. Ini membantu dalam penelitian medis, pertukaran data sensitif, dan peningkatan keamanan data medis.

Pengamanan Data: Steganografi dalam citra juga dapat digunakan untuk menyembunyikan informasi rahasia dalam file citra seperti kartu identitas, dokumen, atau data pribadi. Ini dapat membantu dalam pengamanan data dan mencegah akses tidak sah.

Rahasia Bisnis: Perusahaan dapat menggunakan steganografi untuk menyembunyikan informasi rahasia dalam gambar yang berkaitan dengan proyek, strategi bisnis, atau rencana pengembangan produk agar tetap aman dari mata-mata kompetitor.

Ada beberapa metode dalam steganografi, yaitu:

Metode Substitusi Least Significant Bit (LSB):

Metode Substitusi Least Significant Bit (LSB) adalah salah satu teknik steganografi yang paling sederhana dan umum digunakan untuk menyembunyikan pesan atau informasi rahasia dalam citra digital. Teknik ini bekerja dengan menyisipkan data atau pesan tersembunyi dalam bit paling tidak signifikan (LSB) dari setiap komponen warna (misalnya, merah, hijau, dan biru) dari piksel dalam gambar. LSB merupakan bit terakhir dari setiap komponen warna dalam representasi biner dari nilai piksel.

Berikut adalah penjelasan rinci tentang cara kerja metode Substitusi LSB:

Representasi Binier dalam Citra Digital:

Citra digital terdiri dari piksel-piksel yang memiliki nilai-nilai warna. Di dalam komputer, nilai warna piksel direpresentasikan dalam bentuk bilangan biner. Misalnya, dalam format gambar RGB (Red, Green, Blue), setiap komponen warna (R, G, B) dari setiap piksel direpresentasikan oleh 8 bit. Dengan demikian, setiap komponen warna memiliki nilai biner antara 00000000 hingga 11111111 (0 hingga 255 dalam desimal).

Data Tersembunyi:

Data yang ingin disembunyikan harus diubah menjadi bentuk biner sebelum disisipkan dalam gambar. Misalnya, jika kita ingin menyembunyikan pesan teks, setiap karakter dalam pesan harus diubah menjadi biner menggunakan kode ASCII.

Sisipkan Data:

Proses penyisipan dimulai dengan mengambil piksel pertama dalam gambar. Kemudian, bit paling tidak signifikan dari setiap komponen warna piksel (R, G, B) diganti dengan bit dari data yang akan disembunyikan. Misalnya, jika kita ingin menyisipkan bit data pertama ke dalam komponen warna merah, maka kita akan mengganti bit terakhir dari komponen warna merah dengan bit data pertama. Langkah ini diulang untuk setiap piksel dalam gambar hingga seluruh data tersembunyi disisipkan.

Pemulihan Data:

Untuk mendekripsi data yang tersembunyi, penerima yang berwenang akan mengekstraksi bit paling tidak signifikan dari setiap komponen warna (R, G, B) dalam gambar. Bit-bit ini kemudian digabungkan untuk membentuk data yang tersembunyi.

Kelebihan dan Kekurangan Metode Substitusi LSB:

Kelebihan:

Sederhana: Metode ini sangat sederhana dan mudah diimplementasikan.

Tidak mempengaruhi tampilan visual: Karena hanya bit paling tidak signifikan yang digunakan, perubahan pada gambar tidak terlihat secara visual.

Kecepatan: Proses penyisipan dan ekstraksi data cukup cepat, terutama pada gambar dengan ukuran kecil.

Kekurangan:

Rentan terhadap serangan: Metode LSB rentan terhadap serangan steganalisis, di mana pihak yang tidak berwenang dapat mencoba menganalisis gambar untuk mendeteksi perubahan pada bit paling tidak signifikan.

Kapasitas terbatas: Karena hanya bit paling tidak signifikan yang digunakan, kapasitas penyimpanan data tersembunyi terbatas dan tergantung pada ukuran gambar.

Pengubahan yang tidak diinginkan: Jika data tersembunyi mengalami kerusakan, mungkin saja gambar mengalami distorsi atau degradasi.

Metode Transformasi:

Metode ini melibatkan transformasi data yang akan disembunyikan ke dalam domain lain (seperti domain frekuensi) menggunakan transformasi matematis, seperti Transformasi Fourier atau Transformasi Kosinus Diskrit. Setelah itu, data yang sudah diubah ini dapat disematkan ke dalam koefisien transformasi dari gambar tersebut.

Prosesnya adalah sebagai berikut:

a. Terapkan transformasi matematis pada data yang akan disembunyikan.

b. Sisipkan koefisien transformasi tersebut pada gambar.

c. Untuk mendekripsi, lakukan langkah-langkah sebaliknya.

Kesimpulan:

Steganografi adalah metode rahasia untuk menyembunyikan pesan atau data dalam media tanpa menarik perhatian pihak lain. Penerapan paling umum adalah steganografi pada gambar, menggunakan teknik seperti LSB untuk menyembunyikan data dalam bit paling tidak signifikan dari piksel gambar. Bagian penting dari menggunakan steganografi adalah memastikan bahwa pesan tersembunyi tidak mengubah tampilan media secara mencolok sehingga tetap aman dan tidak terdeteksi oleh pihak yang tidak berwenang.