

BAB 1

PENDAHULUAN

1.1. Latar Belakang

Kemajuan pola berpikir manusia menciptakan masyarakat yang sadar bahwa teknologi informasi merupakan salah satu bagian penting pada peradaban. Sejalan dengan perkembangan teknologi informasi, banyak juga pihak-pihak yang tidak bertanggung jawab melakukan tindak kejahatan misalnya pencurian dan pemalsuan informasi dari suatu data. Permasalahan tersebut bisa diatasi menggunakan banyak macam cara dan teknik diantaranya adalah teknik *steganografi*,

Steganografi adalah sebuah teknik menyembunyikan data rahasia di dalam wadah (media) digital sehingga keberadaan data rahasia tersebut sulit diketahui oleh orang atau pihak-pihak yang tidak bertanggung jawab (Aji, 2020), Teknik *steganografi* sendiri memiliki banyak metode yang bisa dipakai sesuai dengan kebutuhan, seperti metode *LSB (Least Significant Bit Mask and Filtering)*, kompresi dan transformasi, *DCT (Discrete Cosine Transform)* dan *DFT (Discrete Fourier Transform)*. Berdasarkan penelitain Novani, Si, Ii, & Maliki, n.d.(2019) yang melakukan kombinasi metode *FFT (Fast Fourier Transform)*, dan *LSB (Least Significant Bit Mask and Filtering)*. Hasil penelitian tersebut file data yang dijadikan wadah dibagi menjadi blok-blok. setelah itu blok data wadah di transform ke domain frekuensi menggunakan metode *FFT (Fast Fourier Transform)* kemudian data atau pesan yang ingin disisipkan kedalam setiap blok data wadah , disisipkan dengan menggunakan metode *LSB (Least Significant Bit)*. Setelah seluruh blok dsisipkan kemudian di invers kembali dengan *FFT*.

Berdasarkan data-data yang sudah dipaparkan diatas, maka pada penelitian ini peneliti akan mencoba mengganti metode *FFT (Fast Fourier Transform)* pada penelitian Novani, Si, Ii, & Maliki, n.d.(2019), dengan metode *DCT (Discrete Cosine Transform)*, dan membandingkan efisensi dan performanya dengan metode *LSB(Least Significant Bit Mask and Filtering)*, metode *DCT* dipakai lantaran penyesuaian frekuensi lebih sederhana daripada metode *FFT* untuk media gambar. Maka judul penelitian ini adalah **“Steganografi pesan teks menggunakan Metode LSB dan DCT”** .

1.2. Identifikasi Masalah

Berdasarkan penjelasan latar belakang diatas, maka rumusan masalah pada penelitian ini adalah Bagaimana mencari perbandingan akan efisiensi kerja, dan kegunaan utama dari Metode *LSB*, dan *DCT*.

1.3. Tujuan dan Manfaat Penelitian

1.3.1 Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Memberikan informasi tingkat efisiensi dan performa dari metode *LSB* dan *DCT* dalam menyembunyikan pesan.
2. Mengubah citra dari file digital dari file awal atau menjadi *file* modifikasi yang mengandung perubahan yang tidak kasat mata.

1.3.2 Manfaat Penelitian

1. Dari penelitian ini diharapkan sanggup memberikan informasi tentang perbandingan antara Metode *LSB*, dan Metode *DCT*.
2. Diharapkan sanggup memberikan pengetahuan bagaimana cara menganalisa citra hasil steganografi.
3. Dari penelitian ini juga diharapkan sanggup membuat program steganografi yang mampu menyembunyikan pesan teks pada citra atau gambar.

1.4. Batasan Masalah

Masalah yang akan dibahas pada penelitian ini mencakup:

1. Penelitian ini menitikberatkan pada pembuatan aplikasi *steganografi* untuk mengamankan pesan teks yang disisipkan pada file digital dengan format *PNG (Portable Network Graphic)*, dan *BMP (BitMap)*.
2. Metode penyisipannya menggunakan *LSB (Least Significant Bit Mask and Filtering)*, *DCT (Discrete Cosine Transform)*.
3. Tipe file yang akan disembunyikan adalah teks.
4. Bagaimana membuat aplikasi steganografi dengan metode *LSB* menggunakan Java Netbeans.
5. Bagaimana membuat aplikasi steganografi dengan metode *DCT* menggunakan Mat Lab.

1.5. Keterbaruan

Berdasarkan penelitian Santiko (2016), pada penelitiannya *Implementasi Model Steganografi Dalam Mengelola Kerahasiaan Info Menggunakan Metode LSB (Least Significant Bit)*. Pada penelitiannya terbagi kedalam 2 proses utama yaitu *hide message* atau penyisipan pesan, dan *extract message* atau membaca kembali pesan yang tersembunyi. Pada hasil percobaan juga dilakukan perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut (PSNR). Hasil dari penelitian ini dapat disimpulkan bahwa aplikasi Steganografi yang telah dihasilkan dari implementasi algoritma *LSB (Least Significant Bit)* dapat dipergunakan dengan baik untuk menyembunyikan pesan pada sebuah image atau file citra digital serta hasil pengujian nilai *PSNR* terhadap image atau file citra digital yang dihasilkan dari aplikasi Steganografi inipun menunjukkan nilai yang relatif baik bergantung pada besar ukuran file citra yang digunakan serta besarnya jumlah karakter yang disisipkan pada file citra tadi

Pada penelitian (Basuki & Maranggani, 2019) Pada penelitiannya yang berjudul *Embedding Pesan Rahasia Di Dalam Suatu Gambar Dengan Metode Least considerable Bit Insertion (LSB)*. Pada penelitiannya, pada berkas image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada information pixel yang menyusun file tersebut. Pada berkas bitmap 24 bit, setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan eight bit (byte) dari zero sampai 255 atau dengan format biner 00000 sampai 11111111. Dengan demikian, pada setiap pixel berkas bitmap 24 bit kita dapat menyisipkan three bit facts. Dan metode berlapis Enkripsi ditambahkan dengan tujuan untuk keamanan berlapis pada informasi yang disisipkan. Dari penelitian ini dapat disimpulkan bahwa Citra digital yang disisipkan dengan metode LSB ditambah dengan enkripsi akan makin sulit untuk dipecahkan oleh orang yang tidak berkepentingan dan dibutuhkan mystery key untuk mendekodekan enkripsi yang digenerate dengan menggunakan scrypt.

Pada penelitian Rekursif, Ardiansyah, Susilo, & Erlansari, 2017 dengan judul *Penerapan Metode Dct (Discrete Cosine Transform) Pada Aplikasi Penyembunyian Pesan*. Pada penelitiannya dia menggunakan metode *DCT (Discrete Cosine Transform)*, file pesan berupa *file* dengan ekstensi **.txt*. isi pesan 100 karakter, 250 karakter dan lebih dari 500 karakter dapat dienkripsi dengan baik, namun disarankan menggunakan *file* citra dengan format *.bmp* sebagai media penyisipan pesan.