

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Pada perkembangan teknologi yang semakin pesat saat ini menjadikan pertukaran data digital semakin mudah dan cepat, misalnya saja melalui media internet. Dengan adanya kemudahan dalam mendapatkan data digital, seseorang dapat melakukan *interruption*, *interception*, dan *modification* pada data digital tersebut. Oleh karena itu, untuk menjamin keamanan dan kerahasiaan data diperlukan suatu teknik untuk mengamankan data tersebut, salah satunya dengan steganografi. Steganografi adalah suatu cara atau seni menyembunyikan data pada suatu media sehingga hanya pihak pengirim dan penerima saja yang mengetahui data tersebut. Sistem ini dapat mengurangi terjadinya pencurian dan penyalahgunaan data sehingga data yang dikirimkan dapat sampai kepada penerima dengan aman.

Teknik steganografi yang paling sederhana adalah menyisipkan bit pesan secara langsung ke *least significant bit-palne* dari citra *host* dalam urutan deterministik. Modulasi *least significant bit* tidak menghasilkan perbedaan yang dapat dilihat manusia karena amplitudo perubahannya kecil. Kelebihan metode LSB adalah kesederhanaannya dan memiliki *imperceptibility* yang tinggi [1]. Kelebihan lain dari metode LSB adalah memiliki kapasitas penyisipan yang tinggi dan kompleksitas komputasional yang rendah [2]. Untuk mendekomposisi citra, dipilih metode DWT, karena DWT dapat mendekomposisi sinyal menjadi komponen terpisah dengan skala yang berbeda. Hal ini dianggap sebagai metode analisis multi-resolusi. Jadi, citra *host* bisa dipecah menjadi rangkaian komponen frekuensi rendah dan tinggi dengan transformasi wavelet. Berdasarkan efek visual manusia, penyisipan informasi pesan rahasia digital ke area frekuensi rendah tidak mudah untuk diketahui [3].

Salah satu kelebihan dari matriks R yang digunakan dalam skema ini adalah nilai absolut elemen dari matriks R lebih besar daripada nilai absolut dari matriks

Q . Selain itu, QR menguraikan daerah citra yang homogen (seragam) dimana kolom dengan 8×8 blok adalah sama, hanya matriks R yang memiliki nilai dan yang lainnya nol. Jadi, dalam skema ini untuk menyisipkan pesan rahasia digunakan matriks R agar tidak menimbulkan persepsi visual yang signifikan pada citra-stego. Selain itu, konsep deret Fibonacci dipilih karena suatu hal yang menarik, yaitu rasio antara semua angka Fibonacci ini setelah beberapa kombinasi pertama semakin mendekati 1,618. Rasio ini (1,618) dianggap oleh orang Yunani dan Romawi sebagai "*Golden Section*" atau "*divine proportion*". Apa yang dihasilkan adalah sederet angka yang menunjukkan "*Golden Ratio*" dan hubungan yang terbukti berlaku untuk alam, simetri dan secara umum untuk hubungan yang selaras dan indah antara banyak hal. Baik berhubungan dengan seni, arsitektur, alam, hewan, bahkan bagian tubuh manusia dan seberapa sering bisa melihatnya dalam kehidupan sehari-hari [4]. Pada steganografi citra, deret Fibonacci ini dapat meningkatkan *security* terhadap pesan rahasia yang disisipkan.

1.2 Penelitian Terkait

Sebelumnya sudah banyak dilakukan penelitian tentang steganografi atau watermarking dengan menggunakan metode *Discrete Wavelet Transform* (DWT), *QR decomposition*, *Least Significant Bit* (LSB) dan deret Fibonacci. Pada [5], Fallahpour menggunakan deret Fibonacci pada watermarking audio untuk membagi spektrum FFT kedalam *frames* yang lebih pendek dan untuk mengubah *magnitude* FFT yang terpilih. Hasil penelitian menunjukkan bahwa metode ini memberikan kapasitas penyisipan yang tinggi tanpa merusak citra *cover*. Pada [3], Xu menggunakan DWT berdasarkan *SIFT features transform* pada watermarking citra. Hasil penelitian menunjukkan bahwa bekerja pada domain wavelet frekuensi rendah memberikan kualitas *imperceptible* dan *robustness* yang baik. Pada [6], Binny menunjukkan metode LSB pada steganografi audio memberikan kapasitas penyisipan yang besar dengan tetap memberikan kualitas *imperceptible* yang baik. Pada [7], Jiancheng mengkombinasikan metode *phase watermark* dan transformasi Fibonacci. Hasil penelitian menunjukkan bahwa kombinasi dari kedua algoritma ini memberikan kualitas *robustness* yang lebih baik dibandingkan dengan algoritma *traditional phase watermark*. Pada [8], Zou memperkenalkan metode *digital image*

scrambling berdasarkan transformasi Fibonacci. Pada penelitian [7] menunjukkan bahwa metode transformasi Fibonacci mempunyai kelebihan (1) proses *encoding* dan *decoding* yang mudah dan dapat diaplikasikan secara *realtime*; (2) *scrambling effect* yang bagus; (3) metode ini dapat menahan berbagai macam serangan, seperti kompresi, noise dan *packet loss*.

Pada [9], Chandran menjelaskan secara rinci tentang LSB, DCT dan DWT pada steganografi citra. Hasil penelitian menunjukkan bahwa parameter *imperceptible* dan *robustness* pada DWT mempunyai kualitas yang lebih baik dibandingkan dengan LSB dan DCT. Pada [10], Lalitha menyatakan bahwa watermarking audio dengan skema DWT-Arnold *transform* lebih baik dibandingkan dengan skema DCT-Arnold *transform*. Hasil penelitian menunjukkan bahwa skema ini mempunyai kualitas *robustness* yang baik dalam menahan berbagai macam serangan seperti *re-quantization*, *filtering*, *re-sampling* dan *cropping*. Namun sayangnya, skema DWT-Arnold *transform* tidak dibandingkan dengan skema DWT-Fibonacci. Pada [11], Kaur mendeskripsikan perbandingan antara beberapa model watermarking citra digital dalam metode DWT-SVD, DCT-SVD dan DWT-DCT-SVD, dan menyatakan bahwa masih terdapat banyak kombinasi metode yang dapat digunakan dan dieksplorasi untuk meningkatkan performansi.

Beberapa penelitian [12][13][14][15][16], mengusulkan metode baru untuk watermarking atau steganografi citra, yaitu Fibonacci-Haar wavelet *transform* untuk meningkatkan ketahanan dan keamanan. Dekomposisi sub-band bergantung pada nilai Fibonacci *p-sequence* dan proses penyisipan menggunakan SVD. Hasil penelitian menunjukkan keefektifan dari metode yang digunakan, mempunyai kualitas *imperceptible* dan *robustness* yang baik serta dapat menahan berbagai macam serangan.

Pada [17], Sun menunjukkan skema watermarking citra digital menggunakan metode *chaotic system* dan QR *decomposition*. QR *decomposition* digunakan untuk menyisipkan dan mengekstrak watermark untuk performansi yang lebih baik, *Logistic Mapping* (LM) dan *pseudorandom circular chain* (PCC) digunakan untuk meningkatkan keamanan. Hasil penelitian menunjukkan citra watermarking

memiliki kualitas visual yang baik, terutama bila citra diserang oleh *noise pollution* dan *cropping*. Pada [18], Singh menunjukkan skema watermarking citra, untuk menyisipkan citra warna sebagai watermark kedalam citra warna sebagai *host*, dengan menggunakan metode DCT pada masing-masing blok citra watermark dan citra *host*, QR *factorization* diaplikasikan pada blok citra watermark, dan *Logistic and Lorentz chaotic maps* digunakan untuk memperkuat proses penyisipan dan menentukan lokasi. Hasil penelitian menunjukkan bahwa watermarking citra pada skema ini memiliki ketahanan terhadap berbagai macam serangan citra, seperti *cropping*, perubahan tingkat kecerahan (*contrast adjustment*) dan perubahan warna (*coloring*).

Pada [19], Naderahmadian memaparkan teknik *blind watermarking* untuk menyisipkan citra biner sebagai watermark kedalam citra *grayscale*. Skema ini didasarkan pada QR *decomposition* pada domain wavelet (DWT) dan menggunakan matriks R untuk menyisipkan watermark. QR-DWT memiliki kompleksitas komputasional yang rendah namun tetap mempertahankan ketahanan terhadap serangan pengolahan citra yang berbeda, terutama terhadap rotasi, median filtering, average filtering dan noise *Salt and Pepper*. Skema watermarking menunjukkan hasil yang baik dibandingkan dengan metode SVD dan DCT. QR juga memiliki kapasitas watermarking yang lebih besar dibandingkan dengan SVD. Pada [20], Guo mengusulkan metode watermarking citra yang optimal berdasarkan algoritma Firefly di dalam domain DWT-QR. Kekuatan penyisipan watermark yang optimal diperoleh dengan algoritma Firefly. Analisis hasil eksperimen ini menunjukkan bahwa metode watermarking citra yang diusulkan tidak hanya memiliki *imperceptibility* yang baik, namun juga tahan terhadap beberapa serangan pengolahan citra dan serangan geometrik. Pada [21], Jia mengusulkan skema watermarking citra warna berdasarkan DWT dan QR *decomposition* untuk menyisipkan watermark citra warna kedalam *host* citra warna. Dengan menggunakan teknik kuantisasi, informasi watermark citra warna dimasukkan kedalam semua elemen pada baris pertama matriks R . Hasil penelitian menunjukkan bahwa algoritma yang diusulkan ini tidak hanya memiliki

imperceptibility watermarking yang lebih tinggi, namun juga memiliki ketahanan yang lebih kuat terhadap beberapa serangan pengolahan citra dan serangan geometrik. Jia juga menyebutkan bahwa QR *decomposition* memiliki kompleksitas komputasi yang lebih rendah daripada SVD.

Dalam tugas akhir ini, skema steganografi citra berdasarkan DWT dan QR *decomposition* diusulkan untuk menyisipkan pesan rahasia kedalam citra *host* berwarna pada *color space* dan *layer* tertentu. Pertama, citra *host* RGB dikonversi ke *color space* tertentu. *Color space* yang tersedia dan dapat dipilih adalah RGB, YCbCr atau NTSC. *Layer* dimana pesan rahasia disisipkan juga bisa dipilih. Pilihan yang tersedia adalah *layer 1*, *layer 2*, *layer 3*, *layer 1 & 2*, *layer 2 & 3*, *layer 1 & 3* dan semua *layer 1, 2 & 3*. Setelah *layer* citra yang dipilih pada *color space* tertentu ditransformasikan oleh DWT, selanjutnya dibagi menjadi blok *pixel* 8×8 yang tidak tumpang tindih. Kemudian, setiap blok *pixel* yang dipilih didekomposisi dengan QR *decomposition* dan elemen pada matriks *R* dihitung untuk disisipi informasi pesan rahasia. Pesan rahasia disisipkan ke dalam matriks *R* dari QR *decomposition* pada citra *host* dengan menggunakan metode LSB, dimana posisi yang dipilih ditentukan sesuai dengan angka Fibonacci yang digunakan untuk memperkuat dan menentukan lokasi penyisipan. Penelitian serupa tentang steganografi citra yang menggunakan metode DWT dan QR *decomposition* telah dipaparkan oleh [17][18][19][20][21]. Perbedaan antara penelitian [17][18][19][20][21] dengan tugas akhir ini adalah penelitian tersebut tidak menggunakan deret Fibonacci dan metode LSB sebagai skema penyisipan untuk menyembunyikan data. Selain itu, pada penelitian tugas akhir ini yang diproses adalah penyisipan teks ke citra, bukan citra ke citra.

1.3 Rumusan Masalah

Berdasarkan deskripsi latar belakang dan penelitian terkait, maka dapat dirumuskan beberapa masalah di tugas akhir ini yaitu sebagai berikut.

1. Dikarenakan adanya berbagai macam serangan seperti *interruption*, *interception*, dan *modification* yang dapat dilakukan oleh “*man in the middle attack*” ketika berlangsungnya pertukaran informasi melalui

media digital, maka dibutuhkan sistem steganografi berkualitas tinggi dengan metode DWT, QR, LSB dan deret Fibonacci.

- a. Bagaimana proses penyisipan dan ekstraksi menggunakan DWT, QR, LSB dan deret Fibonacci?
2. Sistem steganografi yang dibuat pada penelitian ini adalah steganografi citra, yang berarti memanfaatkan visual manusia. Oleh karena itu, citra stego yang dihasilkan harus mempunyai performansi *imperceptibility*, *fidelity*, *recovery* dan *robustness* yang baik.
 - a. Bagaimana performansi citra *host* sebelum dan setelah disisipi pesan rahasia?
 - b. Bagaimana performansi citra-stego sebelum dan setelah diberikan berbagai macam serangan?
3. Pesan rahasia (teks) yang disisipkan kedalam citra *cover* harus tetap utuh dan benar.
 - a. Bagaimana performansi pesan rahasia (teks) setelah diekstrak/diambil dari citra-stego?

1.4 Asumsi dan Batasan Masalah

1.4.1 Asumsi

Asumsi dalam penelitian ini adalah citra-stego tahan terhadap berbagai macam serangan dan citra-stego yang dihasilkan mempunyai performansi *imperceptibility*, *fidelity*, *recovery* dan *robustness* yang baik berdasarkan parameter PSNR, BER, CER dan MOS. Metode yang digunakan adalah DWT, QR, LSB dan deret Fibonacci pada citra warna (RGB) sebagai *host/cover*, pesan rahasia yang disisipkan berupa teks.

1.4.2 Batasan Masalah

Adapun batasan masalah dalam tugas akhir ini adalah sebagai berikut:

1. Perancangan sistem dilakukan dengan menggunakan aplikasi Matlab versi 2016a;
2. Informasi yang disisipkan berupa teks dengan jumlah karakter pesan rahasia sebanyak 17, 31, 41 dan 70 karakter;

3. Steganografi citra dilakukan dengan menggunakan metode DWT, QR *decomposition*, LSB dan deret Fibonacci;
4. Penyisipan file teks ke dalam citra *host* menggunakan metode LSB;
5. Jumlah file citra *host* yang digunakan dalam tugas akhir ini sebanyak lima file citra *host* format .bmp berdimensi 1024x1024 dan merupakan file .bmp asli bukan hasil konversi dari file yang telah terkompresi;
6. Metode yang digunakan untuk mengubah domain waktu ke domain frekuensi yaitu dengan teknik transformasi DWT;
7. Parameter yang dianalisis adalah parameter *robustness* atau ketahanan data pesan rahasia yang direpresentasikan dengan BER, parameter kualitas citra secara objektif yang direpresentasikan dengan parameter PSNR, parameter kualitas citra secara subjektif yang direpresentasikan dengan MOS.
8. Serangan yang dilakukan sebanyak sembilan jenis serangan yaitu kompresi JPG, LPF, *median filter*, *histogram*, *Gaussian*, *salt and pepper*, *resize*, *rotate* dan *cropping*.

1.5 Tujuan dan Manfaat Penelitian

1.5.1 Tujuan

Tujuan dari penelitian ini adalah ingin mendapatkan citra-stego dengan performansi *imperceptibility*, *fidelity*, *recovery* dan *robustness* yang baik. Diterapkannya metode DWT, QR, LSB dan deret Fibonacci adalah untuk mendapatkan performansi citra-stego yang lebih baik dari penelitian-penelitian terkait.

1.5.2 Manfaat

Manfaat yang dapat diberikan kepada pengguna atau kepada pihak yang berkepentingan adalah tidak adanya rasa khawatir ketika mengirimkan pesan rahasia melalui media digital, seperti internet, karena pesan rahasia yang dikirimkan telah diamankan dan disembunyikan dengan baik, sehingga kasus "*man in the middle attack*" yang dapat melakukan *interruption*, *interception*, dan *modification*, tidak akan mendapatkan pesan rahasia tersebut.

1.6 Hipotesis

Berdasarkan uraian latar belakang dan rumusan masalah, maka dapat dibuat hipotesis bahwa citra-stego yang dihasilkan mempunyai performansi *imperceptibility*, *fidelity*, *recovery* dan *robustness* yang baik berdasarkan parameter PSNR, BER, CER dan MOS.

1.7 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam pembuatan tugas akhir ini adalah sebagai berikut:

1. Studi Literatur

Studi literatur ini dimaksudkan untuk mempelajari konsep dan teori-teori yang berkaitan dengan tugas akhir ini, baik berupa buku, jurnal ilmiah, paper maupun berkonsultasi dengan dosen pembimbing tugas akhir.

2. Analisis dan Desain

Pada tahap ini dilakukan perancangan untuk proses penyisipan dan ekstraksi pesan rahasia (teks) ke dalam citra menggunakan metode DWT, QR, LSB dan deret Fibonacci.

3. Simulasi Sistem

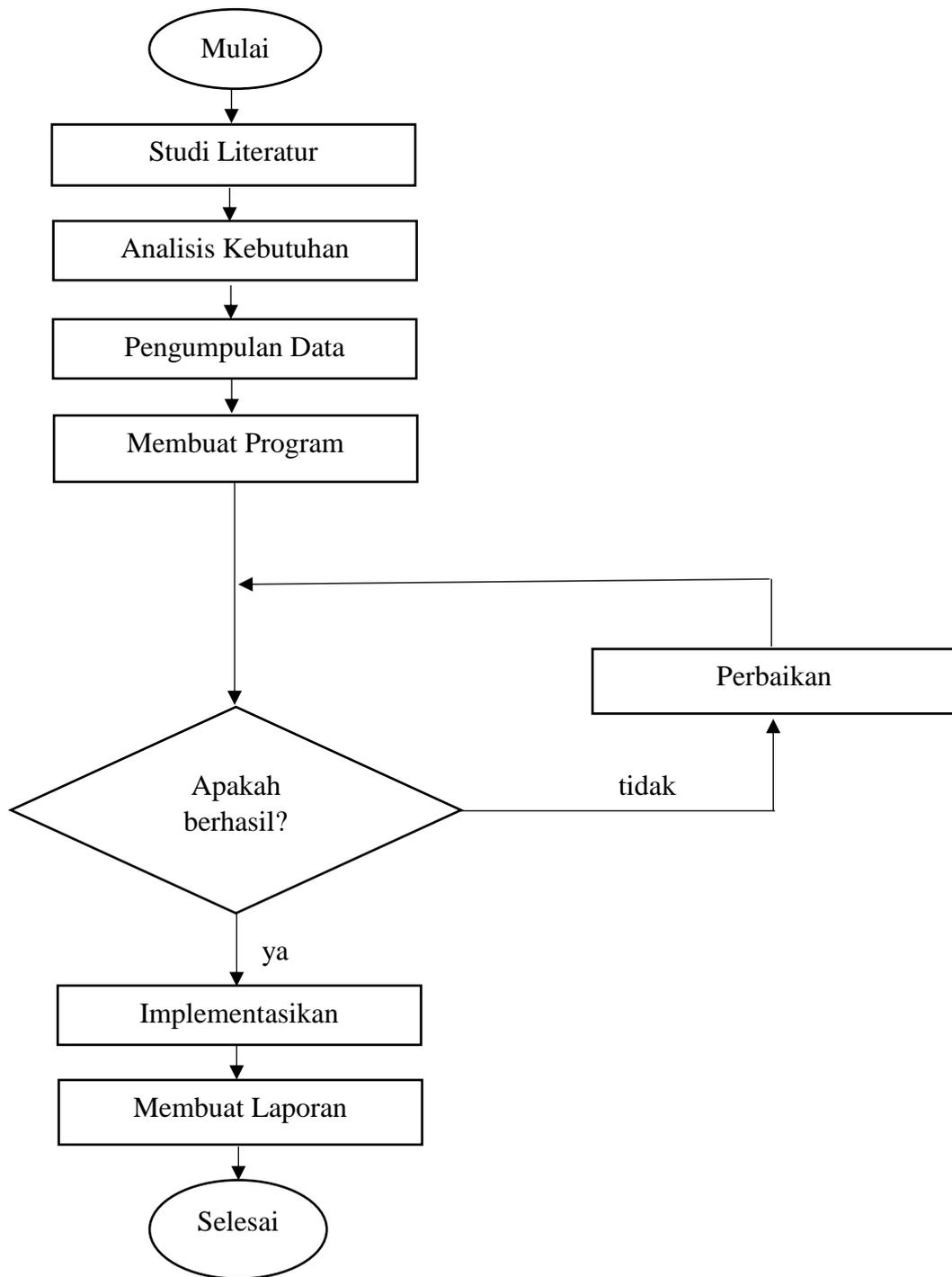
Tahapan simulasi sistem meliputi penerapan hasil analisis dan desain yang telah dilakukan pada tahapan sebelumnya.

4. Pengujian dan Analisis Hasil

Pada tahap ini dilakukan pengujian dan analisis dari hasil simulasi sistem untuk mengetahui kualitas citra setelah disisipi pesan rahasia dan mengetahui kualitas dari pesan rahasia setelah proses ekstraksi.

5. Penyusunan Laporan Penelitian

Pada tahap akhir ini hasil yang didapat dari tahapan-tahapan sebelumnya disusun dalam bentuk tulisan dengan format penulisan tugas akhir. Gambaran umum prosesnya ditunjukkan oleh Gambar 1.1.



Gambar 1.1 Metodologi Penelitian