

## BAB I PENDAHULUAN

### 1.1 LATAR BELAKANG MASALAH

Perkembangan teknologi digital semakin meningkat, ini mengakibatkan mudahnya *user* dalam melakukan proses penggandaan dan pertukaran data seperti pada *text*, citra, audio maupun video. Pada sistem digital, penggandaan data dapat menghasilkan data baru yang hampir menyerupai data asli, untuk itu di perlukan suatu sistem perlindungan terhadap data tersebut. Selain itu, diperlukan juga sistem perlindungan dalam pengiriman data.

Perlindungan data pada sistem digital dapat berupa metoda *criptography* yaitu metoda pengacakan data menggunakan suatu kunci *criptography*, dalam hal ini *criptography* memusatkan kepada keamanan data, dimana jika seorang *user* yang tidak dikehendaki ingin mendapatkan data maka *user* tersebut akan terhalang oleh kunci *criptography*-nya, atau perlindungan data menggunakan metode *steganography* yang menyisipkan data dengan suatu data.

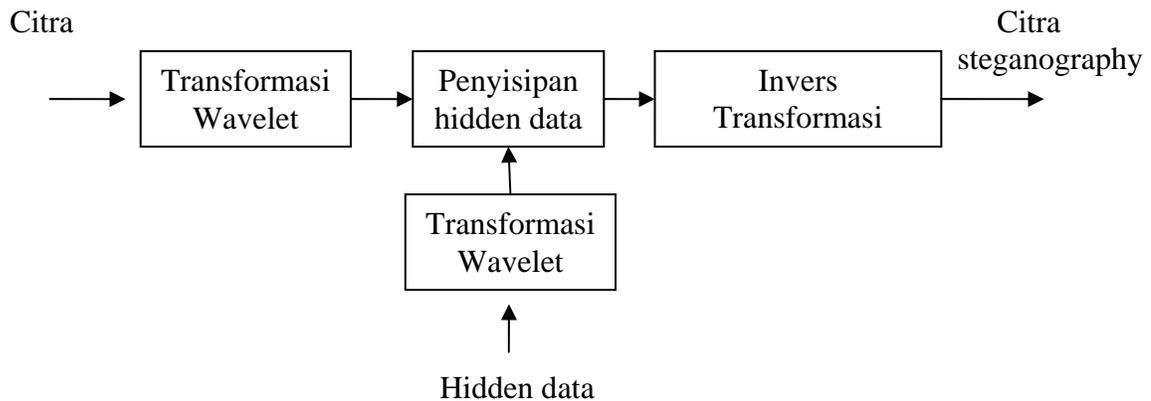
*Steganography* merupakan ilmu yang mempelajari bagaimana menyembunyikan suatu data pada data yang lain dengan suatu metode penyisipan data informasi melalui media yang disembunyikan (*hidden data*) berupa *text*, suara, *image*, dan video. Pada sistem *steganography*, *hidden data* adalah data yang akan disembunyikan baik itu berfungsi sebagai penanda ataupun sebagai data yang akan dikirimkan

Ada berbagai teknik transformasi pada *steganography*, seperti FFT (*Fast Fourier Transform*), DCT (*Discrete Cosine Transform*), *Wavelet Transform*, dsb. Penerapan pada berbagai jenis data digital dengan berbagai transformasi turut mempengaruhi beberapa parameter penting dalam *steganography* (*bitrate*, *invisible*, dan *robustness*). Dalam tugas akhir ini akan digunakan transformasi *wavelet* sebagai alat bantu matematis untuk melakukan dekomposisi suatu sinyal, seperti audio dan citra, menjadi komponen-komponen frekuensi yang berbeda, sehingga masing-masing komponen tersebut dapat dipelajari.

Selama ini *hidden steganography* memiliki *robust* yang rendah, dengan kata lain tidak tahan terhadap derau. Dan sebaliknya, *robust steganography* memiliki *hidden* yang rendah karena data yang disembunyikan (*hidden data*) tampak pada data citra *host*. Studi terdahulu menunjukkan bahwa teknik *steganography* dengan metode ICA-Wavelet memiliki sifat *robust* yang tinggi tetapi *hidden* yang tidak terlalu baik. Dengan tetap mempertahankan sifat *robust* ICA-Wavelet yang tinggi tetapi memiliki *hidden* yang tinggi juga, penulis selaku peneliti mencoba untuk mengambil dua metode dalam *steganography* sebagai perbandingan, yaitu *steganography* berbasis *spread spectrum bit random* terdistribusi *uniform* yang untuk seterusnya akan menggunakan istilah *spreader uniform* dan *steganography* berbasis *Chaotic Random Number* yang seterusnya akan menggunakan istilah *spreader chaotic*.

*Chaotic* merupakan suatu sistem yang dinamis yang mempunyai perilaku terbatas. Dua karakteristik yang dimiliki sinyal *chaotic* adalah *spectrum* daya yang kontinu pada suatu pita frekuensi tertentu, dari ciri ini menunjukkan bahwa sinyal *chaotic* merupakan sinyal yang nonlinier sekaligus sering dikatakan sinyal *noise*, dan mempunyai kepekaan yang tinggi terhadap kondisi awal [17]. Pada aplikasinya sinyal *chaotic* dapat berfungsi sebagai algoritma pemetaan dan sebagai pembangkit kode-kode *random* yang tidak mempunyai pola.

Sedangkan *spread spectrum* dalam dunia komunikasi merupakan proses dimana sinyal pita sempit dimodulasi oleh sinyal pita lebar yang akan menyebar sinyal pita sempit tersebut [10]. Dalam *steganography*, sinyal pita sempit dianalogikan dengan *hidden data* yang akan disisipkan dan sinyal pita lebar dianalogikan sebagai citra digital yang telah didekomposisi *wavelet* atau media digital yang akan disisipi *hidden data*. Gambaran umum proses *steganography* dapat dilihat pada Gambar 1.1 dibawah ini.



**Gambar 1.1** Gambaran *steganography* secara umum dengan Transformasi *wavelet* [1].

## 1.2 PERUMUSAN MASALAH

Berdasarkan latar belakang yang dikemukakan diatas, maka masalah yang akan diteliti adalah :

1. Bagaimana menyisipkan *hidden data* kedalam informasi citra pembawa dengan menggunakan *spreader* (*spreader chaotic* ataupun *spreader uniform*) pada *hidden data*.
2. Bagaimana kualitas citra *steganography* yang dihasilkan setelah disisipkan informasi berupa citra atau *text*.
3. Bagaimana proses penyisipan *hidden data* ini harus memiliki ketahanan terhadap pemrosesan sinyal secara digital yang terjadi pada citra hasil *steganography*, baik menggunakan *spreader chaotic* ataupun *spreader uniform*.

## 1.3 BATASAN MASALAH

Pada penelitian tugas akhir ini akan dibatasi pada beberapa batasan masalah, yaitu:

1. Citra *host* merupakan citra warna dalam format *Bitmap* dengan skema warna *Grayscale* 8 bit dengan ukuran 512 x 256.

2. Nilai *Spreading* dihasilkan oleh *spreader chaotic* atau *spreader uniform*.
3. Metode *Spreader Chaotic* dan *Spreader uniform* dipakai pada *hidden data* dalam bentuk citra ataupun *text*.
4. Masalah teknik transmisi seperti *interleaving* dan *gain* tidak dibahas tugas akhir ini.
5. Citra digital yang digunakan sebagai *hidden data* merupakan citra berformat *bitmap* dengan skema warna *grayscale* 8 bit dan *text* 8 bit.
6. Pengujian kehandalan citra digital hasil *steganography* dilakukan pada proses *decoding* setelah citra terkena derau dan juga kompresi JPEG. Derau yang ditambahkan adalah derau *uniform*.
7. Teknik *steganography* diimplementasikan menggunakan bahasa pemrograman MATLAB 7.01

#### 1.4 TUJUAN PENELITIAN

Secara umum tujuan penulisan yang ingin dicapai dalam tugas akhir ini adalah:

1. Menguji dan membandingkan kualitas *image* hasil kedua metode *steganography* dan *hidden data* secara objektif dengan menggunakan nilai SNR (*Signal to Noise Ratio*). Semakin kecil nilai SNR-nya, maka semakin buruk kualitas *image* hasil *steganography*-nya. Dan BER (*Bit Error Rate*) jika menggunakan *hidden data* berupa *text*. Semakin besar nilai BER-nya, maka *text* yang dihasilkan semakin tidak sesuai dengan yang asli.
2. Menguji dan membandingkan kualitas *image* hasil *steganography* dengan kedua metode *spreader* dan *hidden data* berupa citra secara subjektif berdasarkan *Mean Opinion Score* (MOS) sebanyak 30 orang sampling, semakin besar nilai MOS-nya maka semakin bagus kualitas citra jika dilihat langsung (mendekati citra asli).
3. Menguji dan membandingkan kualitas sistem *image steganography* dengan berbasis *Chaotic Random Number* (*spreader chaotic*) dan *Spread Spectrum Bit Random* terdistribusi *uniform* (*spreader uniform*) terhadap

*noise* dan kompresi JPEG untuk mengetahui tingkat kehandalan dari masing-masing metode.

4. Merancang dan mengimplementasikan *Image steganography* menggunakan perangkat lunak yang dapat menyisipkan *hidden data* dengan *spreader chaotic* dan dengan *spreader uniform*.

## 1.5 METODE PENELITIAN

Metodologi yang dilakukan dalam tugas akhir ini mencakup hal-hal sebagai berikut:

1. Mengumpulkan bahan-bahan referensi yang akan menunjang proses penelitian, seperti buku tentang *wavelet*, *Chaotic Random Number*, *Spread Spectrum Bit Random*, dan semua yang berkaitan dengan *steganography*. Selain dari buku-buku tersebut, penulis juga mengumpulkan bahan dari TA terdahulu yang membahas *steganography*, *wavelet*, dan *Spread Spectrum Bit Random*.
2. Studi literatur tentang *steganography*, *wavelet*, metode *Chaotic Random Number*, ICA, metode *Spread Spectrum Bit Random*, DWT (*Discrete Wavelet Transform*) yang merupakan tahap pendalaman materi.
3. Identifikasi permasalahan yang akan muncul pada saat melakukan penelitian ini, seperti mengalami *error* dalam pemrograman dan kesulitan menerapkan teori-teori dalam proses penelitian nantinya. Selanjutnya penulis memperdalam teori yang berkaitan dalam permasalahan dalam penelitian tersebut.
4. Menentukan sepuluh citra *host* yang berbeda berdasarkan *region* warnanya.
5. Menentukan dua *hidden data* berupa citra dengan ukuran yang berbeda yaitu 512 x 256 dan 64 x 32.
6. Menentukan teks yang akan digunakan sebagai *hidden data*.
7. Membuat rancangan sistem untuk melakukan proses *steganography* dengan *spreader chaotic* dan *spreader uniform*.

8. Menyusun algoritma program yang digunakan pada proses penyisipan *hidden data* yang berupa citra dengan *spreader chaotic* dan *spreader uniform*, kemudian mendeteksi kembali *hidden data* berupa citra atau *text*.
9. Merancang program berdasarkan algoritma yang telah dibuat dan mengimplementasikannya kedalam bahasa pemrograman MATLAB versi 7.01.
10. Melakukan analisa hasil implementasi *steganography* dengan *spreader chaotic* dan *spreader uniform*, untuk mengetahui metode *spreader* yang memiliki tingkat *hidden* dan *robust* yang lebih baik.
11. Membuat kesimpulan dari hasil penelitian *spreader chaotic* dan *spreader uniform*.

## 1.6 SISTEMATIKA PENULISAN LAPORAN

Tugas Akhir ini disusun dengan sistematika pembahasan sebagai berikut :

### BAB I           Pendahuluan

Bab ini berisi tentang latar belakang dilakukannya penelitian *steganography* dengan *spreader chaotic* dan *spreader uniform*, perumusan masalah yang akan dianalisa, pembatasan masalah selama melakukan penelitian, tujuan yang ingin dicapai dalam melakukan penelitian ini, metodologi pemecahan masalah dan sistematika penulisan laporan.

### BAB II          Dasar Teori

Bab ini memuat penjelasan mengenai digital *steganography*, metode yang dapat digunakan untuk penyisipan *hidden data* seperti *Discrete Wavelet Transform* (DWT), metode *spreader* pada *hidden data* dengan menggunakan *spreader chaotic* dan *spreader uniform*, dan proses ekstraksi *hidden data* serta metode yang digunakan seperti *Independent Component Analysis* (ICA).

**BAB III** Perancangan dan Implementasi

Bab ini menjelaskan mengenai proses perancangan penyisipan *hidden data* dalam bentuk citra ataupun *text* dengan *spreader chaotic* dan *spreader uniform* terhadap data citra dan proses ekstraksi *image steganography*.

**BAB IV** Analisa

Pada bab ini memuat tentang analisa terhadap kualitas citra hasil *steganography* secara objektif dengan menghitung *Signal to Noise Ratio* (SNR), dan juga secara subjektif dengan menggunakan *Mean Opinion Score* (MOS).

**BAB V** Penutup

Bagian ini menguraikan kesimpulan dari hasil penelitian tugas akhir ini, yaitu analisa perbandingan performansi *spreader chaotic* (*spreader* berbasis *chaotic random number*) dengan *spreader uniform* (*spreader* berbasis *spread spectrum bit random* terdistribusi *uniform*) pada *steganography* dengan acuan *steganography* yang hanya menggunakan *ICA-wavelet*. Selain itu, terdapat saran-saran untuk pengembangan lebih lanjut dari *steganography* dengan metode-metode perbaikan lainnya.

# BAB I

## PENDAHULUAN

### 1.1 LATAR BELAKANG MASALAH

Perkembangan teknologi digital semakin meningkat, ini mengakibatkan mudahnya *user* dalam melakukan proses penggandaan dan pertukaran data seperti pada *text*, citra, audio maupun video. Pada sistem digital, penggandaan data dapat menghasilkan data baru yang hampir menyerupai data asli, untuk itu di perlukan suatu sistem perlindungan terhadap data tersebut. Selain itu, diperlukan juga sistem perlindungan dalam pengiriman data.

Perlindungan data pada sistem digital dapat berupa metoda *criptography* yaitu metoda pengacakan data menggunakan suatu kunci *criptography*, dalam hal ini *criptography* memusatkan kepada keamanan data, dimana jika seorang *user* yang tidak dikehendaki ingin mendapatkan data maka *user* tersebut akan terhalang oleh kunci *criptography*-nya, atau perlindungan data menggunakan metode *steganography* yang menyisipkan data dengan suatu data.

*Steganography* merupakan ilmu yang mempelajari bagaimana menyembunyikan suatu data pada data yang lain dengan suatu metode penyisipan data informasi melalui media yang disembunyikan (*hidden data*) berupa *text*, suara, *image*, dan video. Pada sistem *steganography*, *hidden data* adalah data yang akan disembunyikan baik itu berfungsi sebagai penanda ataupun sebagai data yang akan dikirimkan

Ada berbagai teknik transformasi pada *steganography*, seperti FFT (*Fast Fourier Transform*), DCT (*Discrete Cosine Transform*), *Wavelet Transform*, dsb. Penerapan pada berbagai jenis data digital dengan berbagai transformasi turut mempengaruhi beberapa parameter penting dalam *steganography* (*bitrate*, *invisible*, dan *robustness*). Dalam tugas akhir ini akan digunakan transformasi *wavelet* sebagai alat bantu matematis untuk melakukan dekomposisi suatu sinyal, seperti audio dan citra, menjadi komponen-komponen frekuensi yang berbeda, sehingga masing-masing komponen tersebut dapat dipelajari.