

Bab 1

Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi digital dan internet telah memberikan kemudahan dalam mendapatkan akses, dan menyebarkan informasi multimedia dalam bentuk digital seperti teks, gambar, audio, dan video [1]. Kemudahan bertukar informasi pada bentuk digital, menyebabkan informasi dapat diperoleh dan dimanipulasi oleh siapa saja. Sebagai contoh, saat ini data pasien di rumah sakit dapat disimpan dalam media elektronik. Data seperti citra medis digital, X-ray, dan mammogram dapat dimanipulasi dengan mudah oleh perkembangan pesat dari teknologi informasi saat ini [1]. Untuk contoh informasi sensitif yang disebutkan sebelumnya, diperlukan sebuah skema agar informasi dapat dengan aman disimpan atau dikirim melalui internet. Salah satu skema yang dapat digunakan adalah steganografi.

Steganografi adalah ilmu menyembunyikan pesan ke dalam sebuah media yang disebut *carrier* atau *cover object*. *Carrier* dapat berupa gambar digital, berkas audio, atau berkas video. Pesan tersembunyi atau disebut *payload* dapat berupa teks, gambar, berkas audio, atau berkas video. Pengimplementasian steganografi pada media digital umumnya diklasifikasikan pada dua domain yaitu domain spasial serta domain frekuensi [2]. Steganografi pada domain spasial biasa menggunakan algoritma *least significant bit* (LSB), algoritma ini bekerja dengan menggantikan lang-

sung bit- bit kurang signifikan pada *cover object* dengan bit- bit data pesan, algoritma ini menjadi sangat populer karena algoritmanya yang sederhana dengan kompleksitas komputasi yang rendah, namun algoritma ini sangat rentan untuk terdeteksi [2]. Pada perkembangan skema steganografi, algoritma LSB dapat digunakan pada domain frekuensi, keuntungan skema steganografi pada domain frekuensi adalah untuk meningkatkan keamanan dan menjadi sulit untuk terdeteksi [3]. Untuk merubah suatu data dari domain spasial menuju domain frekuensi, algoritma yang populer digunakan adalah *discrete cosine transformation* (DCT).

Akhir- akhir ini telah banyak ditemukan skema steganografi yang menggunakan algoritma LSB pada domain frekuensi menggunakan transformasi DCT. Skema ini menawarkan beberapa keunggulan diantaranya kapasitas penyimpanan yang tinggi, sambil tetap mempertahankan karakteristik dari *cover- image* [2]. Skema yang sudah ada diantaranya adalah algoritma *J- steg*, *F5*, dan *Outguess* [2].

Tugas akhir ini menggunakan skema steganografi yang hampir sama. Pertama- tama citra digital yang ditanami pesan terlebih dahulu dirubah ke dalam domain frekuensi menggunakan persamaan DCT. Setelah itu pesan terlebih dahulu diacak menggunakan pemetaan logistik. Nilai awal pada pemetaan logistik dioptimasi menggunakan *particle swarm optimization* berdasarkan fungsi PSNR, sedangkan pada jurnal acuan [2] optimasi pemetaan logistik menggunakan *genetic algorithm* (GA). Selanjutnya bit- bit pesan diacak menggunakan pemetaan logistik yang telah dioptimasi. Lalu bit- bit pesan disisipkan menggunakan algoritma LSB. Terakhir, citra yang telah disisipi pesan dirubah kembali kedalam domain spasial menggunakan persamaan *inverse discrete cosine transformation* (IDCT) untuk memperoleh citra stego. PSO dipilih berdasarkan beberapa keuntungan yang dimilikinya. PSO merupakan algoritma optimasi yang sederhana dan mudah diimplementasikan. Algoritma PSO dapat digunakan dalam berbagai macam bidang studi diantaranya optimisasi fungsi, klasifikasi model, *machine learning*, *neural network training*, pemrosesan sinyal, *vague system control*, *automatic adaptation control* [4]. PSO juga terbukti

lebih efisien secara komputasi dibandingkan dengan algoritma optimasi lain seperti GA [5].

1.2 Perumusan Masalah

Berdasarkan uraian pada latar belakang, berikut adalah rumusan masalah yang diperoleh:

1. Bagaimana menerapkan algoritma *particles swarm optimization* dan metode *chaos* pada steganografi citra digital berbasis *least significant bit* untuk meningkatkan keamanan steganografi tanpa mengurangi kemampuan penyisipan?
2. Bagaimana performansi algoritma *particle swarm optimization* dan metode *chaos* pada steganografi citra digital berbasis *least significant bit* terhadap algoritma LSB sederhana?

1.3 Tujuan

Untuk menjawab perumusan masalah yang ada, maka tujuan dari tugas akhir ini yaitu:

1. Menerapkan algoritma *particle swarm optimization* dan metode *chaos* pada steganografi citra digital berbasis *least significant bit*.
2. Mengetahui performansi algoritma *particle swarm optimization* dan metode *chaos* pada steganografi citra digital berbasis *least significant bit*.

1.4 Batasan Masalah

Batasan- batasan masalah yang digunakan pada tugas akhir ini adalah:

1. *Carrier* atau media yang digunakan untuk menyimpan pesan tersembunyi adalah citra berformat *bitmap*.

2. Pesan yang disisipkan berupa teks.

1.5 Metodologi Penyelesaian Masalah

Metode yang dilakukan untuk menyelesaikan tugas akhir adalah:

1. Studi literatur, mempelajari referensi- referensi yang berhubungan dengan steganografi, algoritma *particle swarm optimization*, *chaostic map* dan *discrete cosine transformation*. Referensi dapat berupa jurnal atau buku.
2. Penelitian, dilakukan dengan merancang sistem dan melakukan pengujian sistem.
3. Analisis, menganalisis pengaruh algoritma *particle Swarm optimization* yang digunakan untuk meminimalisir degradasi terhadap *cover-image*.
4. Pembuatan laporan, berdasarkan analisis dan kesimpulan yang didapatkan, yang selanjutnya dibuat dalam bentuk laporan tugas akhir.

1.6 Jadwal Kegiatan

Rancangan jadwal kegiatan pengerjaan tugas akhir:

Tabel 1.1: Jadwal kegiatan

No	Kegiatan	Bulan Ke					
		1	2	3	4	5	6
1	Studi Literatur	■	■	■	■	■	■
2	Penelitian	■	■	■	■	■	■
3	Analisis	■	■	■	■	■	■
4	Pembuatan Laporan	■	■	■	■	■	■