BAB I
PENDAHULUAN

1.1 Latar Belakang

Steganografi merupakan cara untuk menyembunyikan informasi atau data dalam bentuk apa pun (teks, gambar, suara, video) ke dalam media yang lebih besar (gambar, suara, video) sedemikian rupa sehingga tidak seorang pun mencurigai adanya keberadaan informasi atau data selain pengirim dan penerima [1]. Penelitian pada steganografi berfokus pada aspek penting seperti *imperceptibility, data payload, security, data integrity, robustness* dengan prioritas utama pada *imperceptibility* [2]. Penelitian dilakukan untuk meningkatkan *data payload* sambil tetap mempertahankan tingkat *imperceptibility* untuk mendapatkan kesimpulan lebih detail mengenai aspek *imperceptibility* dan *data payload*. Beberapa penelitian menggabungkan algoritma kompresi ke dalam teknik steganografi yang digunakan untuk menjaga tingkat *imperceptibility* dan meningkatkan *data payload*. Pengukuran tingkat kualitas *imperceptibility* diukur menggunakan metrik MSE (*Mean Squared Error*), PSNR (*Peak Signal-to-Noise Rasio)*, dan SSIM (*Structural Similarity Indeks)* [3-5].

Beberapa penelitian telah dilakukan untuk mengatasi kelemahan dari teknik LSB, seperti penelitian [6] yang mengusulkan dua modifikasi dari teknik LSB yaitu *Bit Inverse* dan penyisipan berdasarkan panjang pesan. Modifikasi *Bit Inverse* mendapatkan hasil yang cukup baik dengan nilai PSNR = 61.80 dB untuk pesan teks dengan 2110 karakter dan PSNR = 50.01 dB untuk gambar, modifikasi ini memiliki kelemahan yaitu kualitas gambar menurun pada daerah tertentu karena penyisipan beruntun sehingga berisiko untuk dikenali. Sebaliknya, modifikasi penyisipan berdasarkan panjang pesan menunjukkan hasil PSNR yang lebih tinggi dibandingkan dengan modifikasi *Bit Inverse* dengan PSNR = 66.29 dB untuk pesan teks dan PSNR = 54.20 dB untuk gambar. Kemudian pada penelitian [7] yang menggunakan teknik 2 LSB, yang merupakan variasi dari teknik LSB di mana jumlah bit yang disisipkan sebanyak 2 bit sehingga meningkatkan kapasitas dari teknik LSB. Hasil penelitian ini dievaluasi menggunakan metrik MSE dan PSNR, dan mendapatkan nilai masing-masing 0.0012 dan 49.65 dB untuk gambar dengan ukuran 1024 x 1024 *pixel*. Namun, teknik 2 LSB memiliki kelemahan di mana penyisipan pada 2 bit terakhir dapat meningkatkan risiko distorsi visual pada gambar dengan kualitas rendah ataupun gambar

dengan banyak variasi warna sehingga membuat pemilihan gambar menjadi cukup penting agar teknik ini mendapatkan performa yang optimal.

Selanjutnya, penelitian [8] menggunakan konsep *Reversible-Enhanced Stego Block Chaining* (RESBC). Konsep ini mendapatkan hasil yang baik dengan *Hiding Capacity* (HC) hingga 73.74% dengan nilai PSNR sebesar 38.75 dB untuk penyisipan sebanyak 3 *stage* dengan menggunakan algoritma kompresi HE-SFA-LZW pada tiap *stage*. Meskipun konsep ini memiliki hasil yang baik dan lebih aman dibandingkan dengan teknik 4 LSB, namun keamanan metode ini dapat ditingkatkan dengan melakukan pengacakan karena penyisipan masih dilakukan secara berurutan. Lebih lanjut, pada penelitian [9] menggabungkan *Simulated Annealing* (SA), *Linear Congruential Generator* (LCG), dan *Caesar Cipher* dengan teknik LSB dan mendapatkan hasil yang cukup baik dengan nilai PSNR hingga 68.36 dB untuk pesan sebesar 1868 *bytes* dan cover image berukuran 768432 *bytes,* namun metode ini memiliki kelemahan di mana LCG memiliki siklus terbatas, mudah diprediksi serta rentan terhadap serangan *brute force*.

Teknik LSB dipilih karena merupakan teknik yang paling mudah untuk diterapkan [2], namun teknik LSB memiliki kelemahan karena kapasitas yang kecil dan penyisipan dilakukan secara berurutan. Untuk mengatasi hal tersebut RESBC dipilih karena kapasitasnya yang besar dan konsep *stage* dapat meningkatkan keamanan [8]. Akan tetapi konsep RESBC memiliki kelemahan karena penyisipannya yang masih dilakukan secara berurutan. Untuk mengatasi kelemahan itu, Generator Modulo digunakan untuk menghasilkan nilai yang terlihat acak namun sebenarnya mengikuti aturan tertentu [10]. Namun, generator modulo seperti LCG umumnya menggunakan nilai awal 1 sehingga menjadikannya mudah diprediksi dan sifat deterministik sehingga algoritma *Diffie-Hellman* diterapkan untuk meningkatkan nilai kerahasiaan, karena nilai dari k dihasilkan melalui mekanisme pertukaran kunci sehingga sulit untuk ditebak.

Berdasarkan uraian di atas, maka dilakukan penulisan tugas akhir dengan judul "**PENGAMANAN CITRA WARNA MENGGUNAKAN *MODIFIED REVERSIBLE-ENHANCED STEGO BLOCK CHAINING* DAN GENERATOR MODULO".**

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, rumusan masalah pada tugas akhir ini adalah:

1. Metode RESBC yang ada masih melakukan penyisipan bit secara berurutan, sehingga dapat membahayakan pesan rahasia yang disisipkan.

2. Belum diketahui sejauh mana tingkat *imperceptibility* dari metode RESBC yang telah dimodifikasi, terutama setelah penambahan variasi bit penyisipan dan pengacakan posisi penyisipan.

1.3 Tujuan

Tujuan dari tugas akhir ini adalah:

1. Membangun aplikasi pengamanan citra warna menggunakan *Modified Reversible-Enhanced Stego Block Chaining* (MRESBC) dan Generator Modulo untuk memberikan keamanan pada citra warna.
2. Menerapkan konsep RESBC, generator modulo, variasi bit penyisipan, dan algoritma *Diffie-Hellman* untuk meningkatkan keamanan pada aplikasi yang dibangun.
3. Mengetahui tingkat *imperceptibility* dari *stego-image* setelah penyisipan pesan rahasia.

1.4 Manfaat

Manfaat yang diharapkan dari tugas akhir ini adalah:

1. Aplikasi yang dibangun dapat digunakan sebagai alternatif dalam pengamanan citra warna.
2. Laporan tugas akhir dapat digunakan sebagai referensi untuk penelitian pengamanan citra di kemudian hari.

1.5 Ruang Lingkup

Agar pembahasan dalam tugas akhir ini lebih terarah dan mencegah adanya perluasan masalah dan pembahasan yang terlalu kompleks, maka diperlukan ruang lingkup terhadap tugas akhir ini, yaitu sebagai berikut:

1. Citra sampul adalah gambar persegi RGB 24 bit dengan format .bmp berukuran sebagai berikut:

$$Total\ pixel\ (R) = \left\lceil \sqrt{\frac{(13 + Total\ Byte\ Kompresi)\ x\ 8}{Jumlah\ bit\ sisip\ x\ 3}} \right\rceil$$

Di mana:

$$Total\ Byte\ Kompresi\ \leq\ (2^{32}) - 1$$

$$pesan \leq\ prime \leq cover\ image$$

2. Citra pesan adalah gambar persegiformat .bmp, berupa RGB 24 bit atau *Grayscale* 8 bit, dengan ukuran minimal 200 x 200 *pixel* dan maksimal 500 x 500 *pixel.*
3. *Staging* yang digunakan pada *Modified Reversible-Enhanced Stego Block Chaining* (MRESBC) berada pada rentang 1 sampai 3.
4. Algoritma kompresi dan dekompresi citra pesan yang digunakan adalah *Lempel-Ziv-Welch* (LZW) dengan maksimal kamus 2 *bytes*.
5. Pesan bit hasil kompresi memiliki tambahan data *header* 13 *bytes* nilai tetap untuk informasi citra pesan, yaitu 1 *byte* untuk jumlah *channel* pesan (*decimal* = "1" menandakan citra pesan adalah *grayscale* dan "3" adalah citra RGB), 2 *bytes* untuk tinggi. 2 *bytes* untuk lebar, 4 *bytes* untuk kunci DHKE dan 4 *bytes* untuk ukuran kompresi dalam jumlah *bytes*.
6. Jumlah bit sisip adalah 1, 2, 3 dan 4 bit dengan jumlah bit sisip yang dipilih akan digunakan untuk tiap *stage* penyisipan.
7. Kunci dari *Diffie-Hellman Key Exchange* merupakan titik awal dari pangkat yang digunakan oleh Generator Modulo.
8. Pengujian hanya dilakukan pada gambar dengan format RGB 24 bit menggunakan jumlah bit sisip dan jumlah *stage*.