BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era teknologi informasi modern, komunikasi merupakan suatu hal yang penting dan digunakan sebagai sarana untuk saling bertukar dan/atau memberikan informasi-informasi mengenai apapun yang berlangung dalam kehidupan. Informasi yang disampaikan dapat bersifat publik maupun rahasia, namun seringkali informasi yang bersifat rahasia dan hanya dapat dilihat oleh pihak tertentu mengundang pihak-pihak yang tidak berwenang untuk memperoleh informasi tersebut. Hal ini menyebabkan keamanan dan kerahasiaan informasi menjadi aspek krusial dari infrastruktur digital global. Meningkatnya kebutuhan akan perlindungan data sensitif dari akses yang tidak sah atau manipulasi oleh pihak yang tidak berwenang menuntut pendekatan inovatif dalam bidang keamanan informasi.

Kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya (Pakobory *et al*, 2016). Pesan yang dapat diamankan dengan kriptografi ada berbagai jenis, seperti teks, gambar, audio dan lain-lain. Salah satu teknik kriptografi untuk merahasiakan pesan adalah *secret sharing*. *Secret sharing* adalah metode pembagian pesan menjadi beberapa bagian (*shares*) dan diberikan kepada beberapa pihak (*participants*). Pada sebuah skema *(k, n) secret sharing*, dibuat *n shares* sedemikian sehingga pesan hanya dapat diperoleh kembali ketika *k shares* digabungkan (Shamir, 1979).

Untuk pesan berupa citra atau gambar, teknik kriptografi yang digunakan merupakan hasil pengembangan dari teknik *Secret Sharing* yaitu *Visual Secret Sharing* atau kriptografi visual *secret sharing*. Teknik ini diperkenalkan oleh Moni Naor dan Adi Shamir dalam paper "*Visual Cryptography*" pada tahun 1995. Proses enkripsi pada paper tersebut dilakukan dengan membagi suatu citra menjadi *n share* yang di mana setiap *share* tersebut merupakan subset dari citra awal, sedangkan proses dekripsi dilakukan dengan menggabungkan seluruh *n share* sehingga diperoleh kembali citra awal.

Penelitian mengenai kriptografi visual telah dilakukan yaitu oleh Bunga *et al* (2023) yang menggunakan skema *(k, n) secret sharing* untuk melakukan kriptografi pada citra *grayscale*. Pada penelitian tersebut, citra *grayscale* dikonversi ke format biner dan disimpan dalam bentuk matriks kemudian dienkripsi dengan proses permutasi yang menghasilkan *shares* yang sulit dikenali. Pada penelitian berikutnya yang dilakukan oleh Pella *et al* (2021), peneliti menggunakan skema VC*n,k* untuk melakukan kriptografi pada citra keabuan dan citra berwarna. Pada penelitian tersebut, citra asli dilakukan proses dithering dengan algoritma Floyd-Steinberg untuk mengubah 256 warna pada citra asli menjadi 8 warna dasar pada citra *halftone* lalu dienkripsi ke dalam 4 sub-pixel pada citra share. Hasil enkripsi menghasilkan *shares* dengan citra abstrak untuk citra keabuan dan citra abstrak dengan sedikit warna acak untuk citra berwarna.

Kriptografi visual *secret sharing* menghasilkan *shares* dalam bentuk citra abstrak yang sulit dikenali secara langsung. Meskipun hal ini menjamin keamanan citra yang dienkripsi, namun sifat abstrak citra tersebut dapat menimbulkan kecurigaan mengenai keberadaan informasi rahasia di dalamnya. Oleh karena itu, diperlukan adanya perlindungan tambahan terhadap *shares* hasil kriptografi visual, salah satunya adalah menggunakan steganografi untuk menyisipkan *shares* ke dalam citra lain.

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui (Munir, 2019). Salah satu metode untuk penyembunyian pesan dalam steganografi adalah *Least Significant Bit*. *Least Significant Bit* (LSB) adalah metode penyisipan data rahasia ke dalam citra digital dengan memanfaatkan nilai bit yang tidak berarti sehingga tidak mengubah citra digital. Metode LSB merupakan salah satu teknik yang paling umum digunakan dalam steganografi karena sederhana dan efektif (Lutfi & Rosihan, 2018). Teknik LSB bisa digunakan untuk semua citra digital, mulai dari citra biner (1 bit per piksel), citra *grayscale* (8 bit per piksel) dan citra berwarna (24 bit per piksel). Pada umumnya, metode LSB menggunakan bit terakhir dari *Least Significant Bit* sebagai tempat penyisipan pesan, namun terdapat metode lain yang disebut sebagai metode LSB yang ditingkatkan (*Enhanced LSB method*).

Metode LSB yang ditingkatkan (*Enhanced LSB method*) yang disebut juga dengan metode LSB2Z adalah varian dari metode LSB yang memanfaatkan 4-*byte* dari *cover image* sebagai tempat untuk menyisipkan pesan (Alqadi *et al*, 2019). Bit yang digunakan untuk penyisipan pesan dalam metode ini adalah dua bit terakhir LSB *cover image* atau bit ke-7 dan bit ke-8.

Pada pesan berupa citra atau gambar, metode LSB yang ditingkatkan bergantung pada *Most Significant Bit* (MSB) untuk men-*embed* citra rahasia ke *Least Significant Bit* (LSB) dari *cover image*. Untuk citra berwarna 24-bit, terdapat dua skema. Pada skema pertama, dua bit terakhir *Least Significant Bit* dari setiap piksel (*red, green, blue*) pada *cover image* diganti dengan dua bit pertama *Most Significant Bit* (MSB) citra rahasia. Pada skema kedua, bit terakhir *Least Significant Bit* (LSB) dari setiap piksel merah diganti dengan bit pertama *Most Significant Bit* (MSB) citra rahasia kemudian dua bit terakhir *Least Significant Bit* (LSB) dari setiap piksel hijau dengan dua bit *Most Significant Bit* (MSB) selanjutnya dari citra rahasia dan tiga bit terakhir *Least Significant Bit* (LSB) dari setiap piksel biru diganti dengan tiga bit *Most Significant Bit* (MSB) selanjutnya dari citra rahasia (Rawat, 2013).

Beberapa penelitian mengenai varian dari metode LSB telah dilakukan yaitu oleh Kurniasih (2023) yang menggunakan metode LSB-2 untuk menyisipkan pesan rahasia berupa teks ke dalam citra. Proses *embedding* dilakukan dengan menggunakan metode LSB-2, di mana pesan disisipkan ke bit ke-6 dari *cover image*. Nilai PSNR yang diperoleh dari *stego image* hasil proses *embedding* adalah 73,40 dB. Penelitian selanjutnya dilakukan oleh Alqadi *et al* (2019) yang menggunakan metode LSB2Z untuk menyisipkan pesan rahasia berupa teks ke dalam citra. Proses *embedding* dilakukan dengan menyisipkan pesan ke dua bit terakhir (bit ke-7 dan bit ke-8) dari *cover image*. Nilai PSNR yang diperoleh dari *stego image* adalah 129,46 dB.

Penelitian lainnya dilakukan oleh Rawat *et al* (2013) yang menggunakan metode *Enhanced* LSB untuk menyisipkan citra berwarna ke dalam citra berwarna lain. Proses *embedding* dilakukan menggunakan dua skema metode *Enhanced* LSB, di mana skema pertama mengganti dua bit *Least Significant Bit* (LSB) *cover image* dengan dua bit *Most Significant Bit* (MSB) citra rahasia yang me nghasilkan *stego*

image dengan nilai PSNR yang diperoleh adalah 41,58 dB. Proses *embedding* selanjutnya dilakukan dengan menggunakan skema kedua yang menghasilkan *stego image* dengan nilai PSNR yang diperoleh adalah 42,69 dB.

Berdasarkan uraian di atas, dalam penelitian ini akan dikaji penggabungan antara kriptografi visual menggunakan skema *Secret Sharing* dengan steganografi metode *Enhanced Least Significant Bit* (LSB) untuk meningkatkan keamanan data pada citra *grayscale.*

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dirumuskan masalah sebagai berikut:

1. Bagaimana cara mengamankan citra *grayscale* menggunakan kriptografi *Visual Secret Sharing* dan metode *Enhanced Least Significant Bit*?
2. Bagaimana konstruksi program aplikasi penggabungan kriptografi *Visual Secret Sharing* dan metode *Enhanced Least Significant Bit*?
3. Bagaimana perbandingan nilai *Peak Signal-to-Noise Ratio* antara *stego image* dan *cover image* dalam mengetahui kualitas *stego image*?
4. Bagaimana perbandingan nilai *Normalized Cross-Correlaiion* antara citra pesan dan citra hasil dekripsi yang sebelumnya diperoleh dari proses *extracting* dalam mengetahui keidentikan citra hasil dekripsi?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang diuraikan, maka tujuan dari penelitian ini adalah:

1. Mengetahui cara mengamankan citra *grayscale* menggunakan kriptografi *Visual Secret Sharing* dan metode *Enhanced Least Significant Bit*.
2. Mengonstruksi program aplikasi komputer mengenai penggabungan kriptografi *Visual Secret Sharing* dan metode *Enhanced Least Significant Bit.*
3. Mengetahui kualitas *stego image* berdasarkan hasil nilai *Peak Signal-to-Noise Ratio* antara *stego image* dan *cover image*.

4. Mengetahui keidentikan citra hasil dekripsi berdasarkan hasil nilai *Normalized Cross-Correlat ion* antara citra pesan dan citra hasil dekripsi.

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini adalah:

1. Citra yang digunakan sebagai pesan rahasia merupakan citra *grayscale*.
2. Ukuran citra yang digunakan sebagai pesan dan citra yang digunakan sebagai *cover image* harus sama.
3. File citra yang digunakan memiliki format *.png.
4. Banyak n *share* yang dihasilkan terbatas dengan $2 \leq n \leq 4$.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Memberikan kontribusi pada bidang matematika terapan melalui pengembangan kriptografi *Visual Secret Sharing* dan metode *Enhanced Least Significant Bit* dalam mengamankan citra *grayscale*.
2. Menghasilkan sebuah program aplikasi untuk mengamankan citra *grayscale* dengan penggabungan kriptografi *Visual Secret Sharing* dan metode *Enhanced Least Significant Bit*.