

## BAB V

### KESIMPULAN DAN SARAN

Berdasarkan rumusan masalah dan hasil pembahasan penelitian yang telah diuraikan maka diperoleh kesimpulan dan saran dari hasil penelitian tersebut.

#### 5.1 Kesimpulan

Berdasarkan hasil dan pembahasan yang telah diuraikan pada bab sebelumnya, didapat kesimpulan sebagai berikut:

1. Implementasi kriptografi visual *Secret Sharing* dan steganografi *Enhanced Least Significant Bit* terdiri dari dua tahap. Tahap pertama yaitu pengirim pesan melakukan enkripsi citra pesan menggunakan kriptografi visual *Secret Sharing* dengan membagi citra menjadi beberapa *share* kemudian menyembunyikan *share* ke dalam citra lain menggunakan steganografi *Enhanced Least Significant Bit* untuk menghasilkan *stego image*. Tahap kedua yaitu penerima pesan mengekstraksi *stego image* menggunakan steganografi *Enhanced Least Significant Bit* untuk memperoleh semua *share* kemudian didekripsi dengan kriptografi visual *Secret Sharing* untuk mendapatkan citra pesan. Pengamanan citra *grayscale* dengan kriptografi visual *Secret Sharing* dan steganografi *Enhanced Least Significant Bit* dapat meningkatkan keamanan pesan serta mengurangi kecurigaan karena pesan disembunyikan ke dalam citra lain.
2. Konstruksi program aplikasi kriptografi visual *Secret Sharing* dan steganografi *Enhanced Least Significant Bit* untuk meningkatkan keamanan data pada citra *grayscale* dapat dilakukan dengan bahasa pemrograman *Python* dan *package Tkinter dan PIL (Pillow)*. *Package Tkinter* digunakan untuk membuat *user interface* (tampilan antarmuka) sehingga memudahkan *user* dalam menggunakan program dan *package PIL* digunakan dalam pemrosesan citra.
3. Steganografi *Enhanced Least Significant Bit* dapat menghasilkan *stego image* yang memiliki nilai *Peak Signal-to-Noise Ratio (PSNR)* lebih dari 30 dB saat dibandingkan dengan *cover image*. Hal ini berarti *stego image* yang dihasilkan memiliki kualitas yang baik.

4. Penggabungan kriptografi visual *Secret Sharing* dan steganografi *Enhanced Least Significant Bit* dapat menghasilkan citra hasil dekripsi yang memiliki nilai *Normalized Cross-Correlation* (NCC) yang lebih mendekati nilai satu ketika menggunakan tiga *n\_bit* saat dibandingkan dengan citra pesan. Hal ini berarti citra hasil dekripsi yang dihasilkan dengan menggunakan tiga *n\_bit* lebih identik dengan citra pesan.

## 5.2 Saran

Terdapat beberapa saran dari penulis untuk dikembangkan dan diperbaiki untuk penelitian selanjutnya, yaitu:

1. Menggunakan teknik kriptografi visual yang berbeda seperti teknik *Random Grids* dalam mengenkripsi citra menjadi *share*.
2. Mengembangkan program aplikasi sehingga dapat digunakan untuk citra berwarna (RGB).
3. Menggunakan metode steganografi yang berbeda dalam menyisipkan citra ke dalam citra lain seperti *Spread Spectrum* untuk meningkatkan keamanan serta mendapatkan nilai NCC yang lebih baik.