

ABSTRAK

Pada penelitian sebelumnya yang berjudul “Simulasi dan Analisis Steganografi Citra Digital Dengan Enkripsi Berdasarkan Prinsip Kubus Rubik”, telah dilakukan pengkombinasian metode steganografi dengan metode enkripsi berdasarkan prinsip kubus rubik. Hasil yang diperoleh adalah pesan hasil enkripsi tidak mudah diserang oleh serangan yang bersifat statistik maupun serangan *Brute-Force*. Akan tetapi sistem tersebut masih memiliki kekurangan, yaitu rusak atau hilangnya pesan rahasia yang disisipkan akibat gangguan selama proses transmisi data. Untuk meningkatkan kualitas dan performansi steganografi, dilakukan penggabungan metode enkripsi dan metode koreksi kesalahan.

Pada tugas akhir ini dilakukan simulasi steganografi data berupa tulisan ke dalam media penyisipan berupa citra digital. Metode enkripsi yang digunakan adalah metode enkripsi berdasarkan prinsip kubus rubik. Metode koreksi kesalahan yang digunakan adalah kode BCH. Sedangkan steganografi menggunakan metode *Least Significant Bit (LSB)*.

Hasil yang diperoleh adalah sistem steganografi dengan menambahkan enkripsi berdasarkan prinsip kubus rubik dan kode BCH menghasilkan nilai akurasi sebesar 100%, nilai PSNR mencapai 78,122 dB dan waktu komputasi minimal 5,45004 detik. Sistem steganografi menggunakan kode BCH lebih tahan terhadap serangan *noise* Gaussian, *noise* Salt and Pepper, *noise* Poisson, *noise* Localvar, *rescale* dan rotasi daripada sistem yang tidak menggunakan kode BCH. Untuk serangan *cropping*, sistem yang menggunakan kode BCH tahan terhadap serangan *cropping* pada rasio 50% saja. Pada rasio 25% dan 12,5%, sistem dengan kode BCH memiliki nilai akurasi yang lebih buruk dibandingkan sistem yang tanpa kode BCH.

Kata kunci : steganografi, citra digital, LSB, kubus rubik, kode BCH