ABSTRAK

Kemajuan teknologi pada saat ini mempengaruhi banyaknya masyarakat yang bisa mengakses berbagai bentuk informasi dalam bentuk, data, dan dokumen, serta kemudahan bertukar informasi dan pengiriman pesan melalui *e-mail* (*publik dan privat*). Tetapi belakangan ini, sering terjadi masalah, antara lain pemalsuan *e-mail (spoofing),* penyalahgunaan *e-mail* (spam), peretas menggunakannya sebagai media penyebaran malware, kebocoran *e-mail* (*man-in-the-middle attack*), dan beberapa lainnya.

Penelitian ini menggunakan kombinasi steganografi LSB dan kriptografi AES. Algoritma AES (*Advanced Encryption Standard*) dipilih karena dirancang khusus untuk keamanan tingkat lanjut dan ketahanan terhadap berbagai jenis serangan, kesederhanaan desain, kekompakan kode dan kecepatan enkripsi, serta deskripsi setiap file atau data. Metode yang digunakan dalam steganografi adalah *Least Significant Bit* (LSB), merupakan metode yang tidak terlalu kompleks dan penyimpanan pesan pada *cover object* juga cukup besar, sehingga data dapat disisipkan. Dasar metode ini adalah berdasarkan bilangan biner yaitu 0 dan 1, sehingga proses aplikasinya menjadi lebih mudah.

Berdasarkan hasil pengujian yang telah dilakukan didapatkan bahwa nilai rata-rata untuk kecepatan enkripsi AES adalah 0,2811 pada pengujian steganografi menghitung nilai MSE dan PSNR dengan rata-rata MSE adalah 0,04008 dan nilai rata-rata pada PSNR adalah 132,2448. Berdasarkan pengujian MSE dan PNSR didapatkan bahwa nilai MSE yang dihasilkan kurang dari 1 db dan PNSR di atas 40, berarti perubahan kualitas warna antara citra asli dengan stego image tidak mengalami perubahan yang signifikan, sehingga keberadaan dari file yang tersembunyi tidak mudah di deteksi oleh indra penglihatan manusia.

Kata Kunci : ***e-mail, Advanced Encryption standard, Least Significant Bit, steganografi dan kriptografi.***