

ABSTRAK

Perkembangan teknologi khususnya di bidang internet menyebabkan mudahnya pertukaran data dalam bentuk softfile baik itu berbentuk media *audio*, *image*, atau *video*. Kemudahan pertukaran data ini menyebabkan banyak kejahatan digital seperti pembajakan atau pengambilan data. Hal tersebut dapat diatasi dengan salah satunya menggunakan *watermark*. Namun, *watermark* saja masih kurang dalam hal keamanan apalagi untuk *watermark* yang dinilai butuh privasi lebih.

Teknik yang digunakan dalam tugas akhir ini adalah kombinasi algoritma *advanced encryption standard* (AES) dan *discrete wavelet transform* (DWT) dimana pertama *plaintext* dilakukan enkripsi menggunakan algoritma AES dan hasilnya disisipkan pada media citra menggunakan DWT. Nantinya citra hasil penyisipan akan dicari PSNR enkripsinya dan *plaintext* hasil ekstraksi akan dibandingkan dengan *plaintext* asliya untuk dicari nilai BER. Percobaan ini dilakukan pada tiap *subband* baik pada DWT level satu atau dua dan menggunakan variasi input 32 dan 64 karakter.

Pada hasil uji coba PSNR didapat bahwa nilai PSNR pada semua uji coba memiliki nilai yang baik yaitu berkisar >50 dB sedangkan untuk BER dari uji coba didapat untuk tanpa serangan tidak ada BER sedangkan pada serangan rotasi berkisar 0.5 karena dipengaruhi *avalanche effect* AES. Uji coba terbaik didapat pada 32 karakter pada DWT level satu dimana BER tidak ditemukan. Sedangkan media citra terbaik pada citra berjenis homogen dan terburuk pada citra berjenis CGI.

Kata kunci : *Kriptografi, watermarking, AES, DWT*