Abstrak

Pertukaran informasi yang bersifat rahasia melalui media yang umum digunakan seperti internet riskan dilakukan. Salah satu solusi untuk menangani permasalahan tersebut adalah steganografi, yaitu penyisipan pesan pada media digital seperti citra, *audio*, ataupun *video* sehingga pesan yang dipertukarkan tidak mencurigakan. Salah satu metode steganografi yang baik dan berkapasitas besar adalah *Bit-Plane Complexity Segmentation* (BPCS). Steganografi akan lebih baik bila dikombinasikan dengan teknik enkripsi, salah satunya *Advance Encryption Standard* (AES).

Hasil penelitian menunjukkan bahwa metode steganografi BPCS memiliki kapasitas penyisipan pesan yang besar, mencapai 47% dari ukuran *vessel image.* Hasil *stego image* berkualitas baik dengan nilai PSNR di atas 30 dB, walaupun ada beberapa *stego image* yang memiliki nilai PSNR di bawah 30 dB karena memakai 87-99% dari kapasitas maksimal. Nilai MOS *stego image* yang diuji seluruhnya di atas 4,12 yang menunjukkan kualitas baik. Namun metode ini tidak tahan terhadap perubahan, sehingga bila *stego image* ditambahkan *Gaussian Noise,* pesan yang didekode mengalami perubahan. Hal tersebut memberikan keuntungan bagi pengirim dan penerima pesan untuk menghilangkan bukti. Penggunaan enkripsi AES mengurangi jumlah blok yang terkonjugasi pada proses steganografi BPCS. Walaupun memerlukan sedikit waktu tambahan, namun penggunaan enkripsi AES pada metode steganografi BPCS tentu akan mempersulit *eavesdropper* dalam mendeteksi dan mengambil pesan rahasia.

Kata kunci: steganografi, BPCS, *vessel image*, *stego image*, enkripsi, AES.