ABSTRAK

Keamanan sebuah data merupakan hal penting bagi semua pihak. Kebocoran atau kehilangan data dapat berakibat fatal terhadap perusahaan maupun perseorangan. Dalam proses transaksi data perlu diperhatikan tingkat keamanannya, sehingga tidak sembarang orang dapat mengetahui isi dari data tersebut. Teknik anti forensik bertujuan untuk menyulitkan penyidik dalam menemukan sebuah bukti, namun dapat menjadi teknik mengamankan data dari pihak yang tidak memiliki hak akses untuk mendapatkannya. Pada penelitian ini bertujuan untuk membangun sistem yang dapat mengamankan pesan. Terdapat beberapa metode dalam mengamankan data pada teknik anti forensik, yaitu penyandian (Kriptografi) dan penyembunyian (Steganografi). Dalam kriptografi terdapat algoritma *Advanced Encryption Standard* (AES) yang berguna untuk mengenkripsi pesan asli menjadi *ciphertext*. AES merupakan algoritma penyandian *block cipher* yang menggunakan tabel substitusi untuk mentransformasikan *byte* yang ada. Sedangkan dalam Steganografi terdapat metode *Least Significant Bit* (LSB) yang berguna untuk menyembunyikan pesan kedalam citra. LSB merupakan metode penyisipan pesan dengan mengubah bit paling tidak signifikan menjadi pesan. Diketahui berdasarkan hasil pengujian, penyisipan pesan kedalam citra menggunakan bit ke 4 dapat memaksimalkan kapasitas dari citra untuk menyimpan pesan, namun kerusakan yang terjadi akibat penyisipan pesan masih dapat ditoleransi berdasarkan hasil pengujian nilai *Peak Signal to Noise Ratio* (PSNR) dengan nilai 30,52 – 54,72 dB dan pengujian *Visual Attack* dibawah 50% berdasarkan penglihatan manusia yang menandakan sebagian besar responden tidak menyadari adanya pesan didalam citra.

Kata Kunci – *Anti Forensik, AES-256, LSB, PSNR,Visual Attack.*