

ABSTRAK

Keamanan informasi menjadi bagian yang tidak terpisahkan dari komunikasi data. Steganografi adalah praktik menyembunyikan informasi dengan cara meyisipkan pesan rahasia kedalam media lain atau dikenal sebagai *carrier-file* seperti citra digital, audio, video ataupun IP *header*. Pengawasan steganografi sulit untuk dilakukan sehingga dapat disalahgunakan oleh pihak kriminal dalam menyembunyikan jejaknya, pernah ada dugaan bahwa teroris menerapkan steganografi dalam berkomunikasi. Oleh sebab itu, perlu adanya sistem yang dapat mengatasi hal tersebut.

IDIH merupakan salah satu metode steganalisis yang digunakan untuk mengidentifikasi steganografi dengan *carrier file* berupa citra digital. IDIH merupakan improvisasi dari metode sebelumnya yaitu DIH yang pertama kali diperkenalkan oleh T. Zhang et al. Pada metode DIH, histogram LSB plane sebelum dan setelah diubah menjadi nol dibuat dari file citra yang diindikasikan memiliki pesan rahasia untuk mendapatkan estimasi panjang pesan. Kemudian ditambahkan skema baru metode IDIH dalam mencari nilai error untuk menghitung rasio *embedding* pesan termodifikasi yang menghasilkan estimasi panjang pesan rahasia yang lebih akurat.

Pada tugas akhir ini, hasil yang dicapai adalah performa steganalisis yang ditunjukkan dari akurasi sistem dalam membedakan citra yang memiliki pesan rahasia dan tidak. Akurasi IDIH untuk citra *grayscale* yaitu 87,4% dan 75,4% untuk citra RGB sedangkan DIH menghasilkan akurasi untuk citra *grayscale* yaitu 75,3% dan untuk citra RGB yaitu 70,9%.

Kata kunci : *Steganography, Steganalysis, Histogram Analysis, Steganalysis IDIH*