BAB 2

TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Penelitian yang dilakukan berpedoman dari hasil penelitian-penelitian terdahulu yang pernah dilakukan sebelumnya sebagai bahan kajian dan perbandingan yang dinilai baik. Beberapa hasil penelitian yang dilakukan oleh peneliti terdahulu yang telah dilakukan perbandingan oleh penulis tidak lepas dari dari topik peneliti yaitu, tentang teknik steganografi menggunakan metode *least significant bit* dan *discreate wavelet transform.*

Penelitian yang telah dilakukan (Malo, Santoso, & Pranowo, 2017), perancangan aplikasi ini menggunakan metode *least significant bit* dan *end of file*, dimana dalam prosesnya menggunakan system encode dan decode untuk memasukan dan melihat isi dari pesan didalam gambar. Pada penelitian ini algoritma yang digunakan meletakan data/pesan yang dimasukan kedalam gambar dengan format RGB (*Red, Green, Blue*). Metode *least significant bit* dapat dilakukan dari pixel berapapun pada format RGBnya.

Penelitian yang dilakukan (Amin, 2016), menyembunyikan pesan berupa teks rahasia kedalam citra digital true colour 24 *bit* dalam format RGB. Algoritma yang digunakan untuk menyisipkan pesan rahasia menggunakan algoritma LSB (*Least Significant Bit*) dengan *bit* atau bit ke-8 dalam setiap komponen warna RGB. Pilihan jenis file citra RGB dengan pertimbangan kapasitas pesan yang dapat disisipkan lebih besar dibandingkan jika menggunakan citra grayscale, hal

ini dikarenakan dalam 1 pixel dapat disisipkan 3 buah bit pesan. Ujicoba yang dilakukan memberikan hasil bahwa pesan yang disembunyikan ke dalam citra digital tidak mengurangi kualitas citra digital secara signifikan, dan pesan yang telah disembunyikan dapat diekstrak kembali, sehingga pesan yang dikirimkan dapat sampai dengan aman kepada penerima.

(Liu et al., 2008) Rasio penyembunyian informasi adalah metrik yang terkenal untuk mengevaluasi kinerja steganalisis. Dalam makalah ini, kami memperkenalkan metrik baru kompleksitas gambar untuk meningkatkan evaluasi kinerja steganalisis. Selain itu, kami juga menyajikan skema steganalisis steganografi pencocokan bit paling signifikan (LSB), berdasarkan pada penambangan fitur dan teknik pengenalan pola. Dibandingkan dengan metode steganalisis terkenal lainnya dari steganografi pencocokan LSB, metode kami melakukan yang terbaik. Hasil juga menunjukkan bahwa signifikansi fitur dan kinerja deteksi tidak hanya bergantung pada rasio penyembunyian informasi, tetapi juga pada kompleksitas gambar.

Untuk meningkatkan keamanan pesan yang dikirim melalui steganografi internet digunakan (Verma, Poonam, & Chawla, 2014). Berbagai teknik steganografi telah diusulkan sejauh ini. Steganografi Bit Least Significant Bit adalah salah satu teknik di mana bit piksel paling signifikan dari gambar diganti dengan bit data. Pendekatan ini memiliki keuntungan yang paling sederhana untuk dipahami, mudah diimplementasikan dan menghasilkan stego-gambar yang mengandung data tertanam sebagai tersembunyi. Kerugian dari Least Significant Bit adalah ia rentan terhadap steganalisis dan tidak aman sama sekali. Jadi untuk

membuatnya lebih aman, algoritma bit paling tidak penting dimodifikasi untuk bekerja dengan cara yang berbeda. Pendekatan yang diusulkan ini sama sekali tidak mengambil bit paling sedikit piksel secara berurutan tetapi dikombinasikan dengan pendekatan titik tengah untuk memilih piksel yang digunakan untuk menyembunyikan pesan. Tujuan dari makalah ini adalah untuk menyajikan analisis teoritis pendekatan Least Significant Bit dan untuk mengusulkan skema penyematan LSB canggih yang tidak hanya menunjukkan keunggulan LSB tetapi juga memberikan tingkat keamanan tambahan. Skema ini mematahkan pola reguler LSB, mengakibatkan peningkatan kesulitan steganalisis dan dengan demikian meningkatkan tingkat keamanan.

Dalam tulisan ini, kami mengusulkan metode hybrid baru untuk steganografi (Mostafa, Ali, & El Taweal, 2016) gambar dengan menggunakan transformasi curvelet diskrit dan bit paling signifikan (LSB). Metode yang diusulkan disebut Hybrid Curvelet Transform dan Least Significant Bit (HCTLSB). Dalam HCTLSB, curvelet de noising diterapkan sebagai langkah preprocessing untuk menghilangkan noise dari gambar sampul. Gambar sampul ditransformasikan dengan menerapkan transformasi curvelet diam-diam sebelum menanamkan data rahasia dengan menggunakan teknik LSB. Invok? ing transformasi curvelet dalam metode yang diusulkan dapat menangani diskontinuitas kurva pada gambar sampul untuk mendapatkan kualitas dan ketahanan gambar yang lebih baik. Teknik LSB diterapkan pada gambar koefisien curvelet diskrit yang diperoleh untuk menanamkan data rahasia tanpa membuat perubahan nyata pada gambar sampul. Kinerja umum dari metode yang diusulkan

diuji pada 10 sampul dan gambar rahasia dan dibandingkan dengan dua metode benchmark. Hasil percobaan menunjukkan bahwa metode yang diusulkan adalah metode yang menjanjikan dan dapat memperoleh hasil yang lebih baik daripada metode yang dibandingkan lainnya. Indeks Syarat-transformasi urvelet, bit yang paling tidak signifikan, transformasi steganografi gambar, bit yang paling signifikan, steganografi gambar.

Steganografi adalah teknik penyembunyian data banyak digunakan dalam berbagai aplikasi pengamanan informasi (Baby, Thomas, Augustine, George, & Michael, 2015). Steganografi mentransmisikan data dengan menyembunyikan keberadaan pesan sehingga pemirsa tidak dapat mengidentifikasi pengiriman pesan dan karenanya tidak dapat mendekripsi itu. Karya ini mengusulkan teknik pengamanan data yang digunakan untuk menyembunyikan beberapa gambar warna menjadi gambar warna tunggal menggunakan Transformasi Wavelet Diskrit. Gambar sampul dibagi menjadi bidang R, G dan B. Gambar rahasia tertanam ke dalam pesawat ini. Dekomposisi N-level dari gambar sampul dan gambar rahasia dilakukan dan beberapa komponen frekuensi yang sama digabungkan. Gambar rahasia kemudian diekstraksi dari gambar stego. Di sini, gambar stego yang diperoleh memiliki perubahan yang kurang jelas dibandingkan dengan gambar asli dengan keamanan keseluruhan yang tinggi.

(Nikhil Simha, Prakash, Kashyap, & Sarkar, 2017) Keamanan menempatkan peran penting dalam suatu aplikasi komunikasi untuk transfer data yang aman. Image Steganography adalah salah satu teknik yang paling dapat diandalkan dalam enkripsi dan dekripsi suatu gambar (tersembunyi) di dalam

gambar lain (penutup) sedemikian rupa sehingga hanya gambar sampul yang terlihat. Dalam makalah ini frekuensi domain Steganografi Gambar menggunakan DWT dan teknik LSB Dimodifikasi diusulkan. Pendekatan yang diusulkan menggunakan DWT untuk mengubah informasi domain spasial ke domain frekuensi informasi. Pita LL digunakan untuk Gambar lebih lanjut Proses steganografi. Gambar diterjemahkan menggunakan LSB terbalik. Karena pita LL digunakan untuk tujuan encoding dan decoding, kebutuhan memori desain kurang untuk perangkat keras pelaksanaan. Ini juga akan meningkatkan frekuensi operasi arsitektur. Teknik yang diusulkan memperoleh PSNR tinggi untuk stegano dan memulihkan gambar tersembunyi.