# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Sekarang dengan berkembangnya teknologi munculah sebuah kata yang disebut dengan internet. Dengan adanya internet ini, penyebaran informasi sangat mudah dan cepat. Internet berperan penting dalam transmisi data yang memberikan kemudahan dalam pengiriman data. Pertumbuhan yang cepat dalam konsumsi informasi digital dalam decade terakhir telah menyerukan perhatian serius terhadap isu-isu keamanan seperti managemen hak digital, keaslian dan keamanan konten[5].

Berbagai kejahatan di dunia maya seperti pemalsuan, modifikasi, duplikasi dan intersepsi telah mencapai tingkat yang mengkhawatirkan[16]. Tidak semua pengiriman data akan sampai pada penerima dengan benar, sering kali ada kesalahan dalam pengiriman data ataupun ada gangguan dalam bentuk kejahatan dengan tujuan mencuri informasi-informasi yang ada dalam data tersebut.

Jejaring sosial merupakan layanan dalam sebuah jaringan yang bertujuan untuk memberikan fasilitas pada masyarakat umum untuk saling berhubungan dalam dunia maya layaknya dalam dunia nyata di kehidupan sehari-hari.Salah satu contoh, *Facebook* adalah kata yang sudah tidak asing lagi bagi masyarakat umum. Banyak hal yang bisa dilakukan dalam jejaring sosial satu ini. Mulai dari berteman, bermain, berbisnis, bahkan untuk urusan pekerjan lainnya dalam kegiatan saling tukar informasi lewat file atau dokumen. Didalam social media tersebut kita dapat menampilkan banyak percakapan yang bisa dilihat secara langsung oleh pengguna social media yang lainnya. Sehingga untuk system keamanan infirmasi pada social media sangat kurang.

Namun, kita tidak tahu seberapa aman data tersebut dapat terkirim sampai ke tujuan tanpa ada system keamanan data pada da tersebut untuk melindungi informasi-informasi penting dalam data. Metode untuk melindungi atau mengamankan data dari gangguan-gangguan pihak yang tidak berkepentingan yakni menggunakan kriptografi dan steganografi.

Kriptografi berfungsi untuk menyembunyikan (mengenkripsi) dan menampilkan kembali (mendeskripsi) data sehingga informasi dalam data tidak dapat dibaca (di lihat) oleh pihak lain yang tidak berkepentingan. Salah satu cabang dari informasi persembunyian yang berfokus pada komunikasi rahasia steganografi. Steganografi menyembunyikan keberadaan pesan yang menghindari perhatian penyadap. Hal ini membuat steganografi dengan cara yang baik untuk menyampaikan informasi rahasia melalui media digital [11].

Steganografi telah diterapkan di berbagai media digital, seperti audio, gambar, video dan teks biasa. Di antara mereka berbagai media, gambar adalah media yang paling popular untuk menanamkan pesan rahasia[7]. Gambar adalah media yang menarik untuk steganografi sejak Human Visual System (HVS) tidak sensitive terhadap perubahan kecil dalam gambar terutama diwilayah perubahan yang signifikan [8].

Salah satu aspek terpenting dalam steganografi adalah berfokus pada tingkat keamanan agar informasi-informasi penting yang kita tanamkan sulit untuk diketahui ataupun di sadap oleh pihak-pihak yang tidak berwenang. Steganografi itu tidak merubah informasi atau data yang kita miliki untuk dikirim ke penerima melainkan menyisipkan pesannya ke media lain seperti halnya pada gambar sehingga pada proses pengiriman data pesan-pesan yang kita kirim lebih aman.

Salah satu metode steganografi yang paling awal di domain spasial diusulkan oleh [9], yang disebut "*Least Significant Bit* (LSB) Pergantian". LSB itu hanya mengganti *image-cover* dengan aliran bit rahasia. Data yang disembunyikan dalam bit signifikan setidaknya dapat diketahui, maka metode ini rentan terhadap ekstraksi oleh pihak lain [10]. Umumnya, metode domain spasial ini rentan terhadap serangan visual dan perubahan pixel[4]. Disisi lain mengubah metode domain yang lebih kuat terhadap operasi pengolahan citra karena skema persembunyiannya di daerah yang signifikan dari gambar sampul[7] [12]. Dalam mengubah metode domain, *Discrete Cisine transform* (DCT) secara luas digunakan untuk mengubah gambar ke domain frekuensi [13].

Di beberapa media digital, media yang paling sering digunakan pada staganografi adalah gambar digital. Dan salah satu teknik yang terkenal di *steganography image digital* yaitu *Cosine Transform Discrete* (DCT). Dalam blok kecil penggunaan DCT dapat mengakibatkan efek memblokir dan menimbulkan artefak yang tidak diinginkan secara keseluruhan pada sebuah *image.* Dari kelemehan DCT tersebut dapat diatasi dengan menggunakan *Discrete Wavelet Transform* (DWT) yang lebih kompatibel dengan *Human Visual System* (HVS). Hasil DWT pada koefisien titik ambang, meskipun input sebagai representasi piksel nilai dari *image* adalah bilangan bulat dan koefisian wavelet tidak lagi menggunakan integer [15].

Dalam titik pengembangan DWT ini memiliki beberapa kelemahan yang salah satunya adalah kehilangan informasi. Dari kelemehan itu, *Integer Wavelet Transform* (IWT) memberikan solusi untuk DWT. IWT merupakan wavelet generasi ke-2 yang mampu memberikan definisi secara wafelet pada sebuah jaringan interval atau jaringan yang tidak teratur [7]. IWT dengan presisi yang terbatas dapat menghindari masalah kehilangan informasi atau floting point presisi di DWT.

Melihat keuntungan dari transformasi wavelet, khususnya pada bilangan bulat transformasi wavelet melalui skema angkat yang telah digunakan oleh [16] maka penelitian ini mengusulkan untuk menggunakan *Integer Haar Wavelet Transform* (IHWT) untuk berkerja pada domain frekuensi gambar. IHWT merupakan perkembangan dari *Discrete Haar Wavelet Transform* melelui skema angkat yang mengubah bilangan bulat dari nilai-nilai piksel suatu image ke dalam keofisien bulat wavelet dan juga sebaliknya.

*Coefficient Difference* merupaka sebuah metode baru hasil adopsi dari metode *Pixel Value Differencing* (PVD). Perbedaan nilai antara dua koefisien wavelet tetangga pada setiap subband merupakan sarana sebagai penyembunyian pesan. Metode *Coefficient Difference* ini menanamkan dan menyembunyikan pesan rahasia dengan nilai-nilai yang berbeda dalam jumlah presisi yang terbatas yang cocok dalam *Integer Wavelet Ttransform*.

Pesan yang tertanam pada 1-tingkat *Integer Haar Wavelet Transform* (IHWT) menggunakan *Coeffcient Difference* yang di adopsi dari *Pixel Value Differencing* (PVD) [2]. Pesan akan ditanam pada selisih dari nilai-nilai dua koefisien wavelet yang saling berdekatan. Dari metode di atas hasilnya menunjukan bahwa IHWT dan *Coefficient Difference* dapat dengan mudah mengungguli metode yang mengimplementasikan IHWT dan *Pixel Metode Mapping* (PMM) dalam hal kapasitas maksimum serta imperceptibility [2].

Berdasarkan analisa masalah diatas, maka pada penelitian ini akan membahas tentang Steganografi untuk Citra Digital dengan *Coefficient Difference* dalam *Integer Haar Wavelet Transform* (IHWT). Sebagai bahan pertimbangan untuk pengamanan data sehingga tidak terjadi pencurian ataupun penyadapan informasi dalam data tersebut. Dengan dilakukannya penelitian ini, diharapkan dapat dikembangkan lagi metode yang di usulkan untuk di uji cobakan pada system keamanan data. Sehingga penelitian ini dapat membatu pengamanan data dalam jejaring social.

## 1.2 Rumusan Masalah

Titik utama pembahasan masalah dalam penelitian ini, diantaranya adalah sebagai berikut:

1. Bagaimana mengimplementasikan Algoritma *Coefisien Difference* dan *Integer Haar Wavelet Transform* (IHWT) untuk Media Digital pada Steganografi?
2. Bagaimana tingkat kualitas citra dan perbedaan citra saat sebelum dan sesudah disisipi oleh teks maupun citra lain?

## 1.3 Ruang Lingkup dan Batasan Masalah

Dalam analisis permasalahan yang telah dipaparkan pada latar belakang di atas. Perlu ada batasan-batasan ruang lingkup guna memberikan kemudahan sebuah praktek. Beberapa batasan masalah dalam penelitian ini:

1. Metode steganografi dapat di terapkan pada image. Dalam penelitian ini hanya menyisipkan pesan rahasia citra digital.
2. Citra yang digunakan untuk menyisipkan pesan rahasia berukuran 512 x 512.
3. Format citra yang digunakan berukuran 8 bit dengan format *.jpg, *.bmp, dan *.tif.
4. Tools yang digunakan yakni Matlab R2012a.
5. Untuk mengukur kualitas citra digital menggunakan PNSR dan SSIM.

## 1.4 Tujuan Penelitian

Berdasarkan batasan-batasan dan perumusan masalah, maka tujuan dari penelitian tugas akhir ini adalah sebagai berikut:

1. Dapat menunjukan hasil implementasi Algoritma *Coefisien Difference* dan *Integer Haar Wavelet Transform* (IHWT) untuk Media Digital pada Steganografi
2. Dapat mengukur tingkat kualitas citra dan perbedaan citra setelah dan sebelum disisipi oleh teks maupun citra lain (pesan).

## 1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan beberapa manfaat sebagai berikut:

1. Bagi Peneliti:
   a. Meningkatkat kreatifitas dan keahlian (skill) peneliti.
   b. Menunjukan kemampuan penulis untuk melakukan analisis dan mencari solusi untuk permasalahan yang ada.
   c. Mengimplementasikan hasil belajar dalam bangku perkuliahan kedalam kehidupan luar khususnya di bidang steganografi.
2. Bagi Universitas Dian Nuswantoro:
   a. Sebagai tolok ukur keberhasilan pemberian materi kuliah yang dapat dipahami dan diserap oleh mahasiswa selama waktu perkuliahan.
   b. Sebagai bahan referensi bagi mereka yang mau melakukan dan mengadakan penelitian untuk dikembangkan lebih lanjut dengan permasalahan, batasan masalah dan bidang permasalahan yang berbeda.
   c. Sebagai bahan evaluasi akademik guna peningkatan mutu dan kualitas pendidikan.