1. Pendahuluan

1.1 Latar belakang

Hak atas kekayaan intelektual seharusnya menjadi perhatian penting bagi kita. Kreatifitas seseorang akan selalu berkembang jika karyanya dihargai oleh orang lain. Pembajakan karya seseorang oleh orang lain merupakan bentuk tindakan yang tidak menghargai karya orang lain.

Menandai sebuah karya merupakan suatu usaha untuk menjaga keaslian karya tersebut. Sebagai contoh, seseorang membubuhkan tanda tangan kedalam surat yang dibuatnya untuk menandakan bahwa surat itu benar-benar dibuat olehnya. Jika belum puas hanya dengan membubuhkan tanda tangan, bisa ditambahkan stempel untuk memperkuat bukti keasliannya.

Jika permasalahannya ada pada dokumen digital, maka solusi tanda tangan dan stempel dapat kita adaptasi ke bentuk digital. Dalam dunia digital, dikenal teknik kriptografi dengan cara *digital signature*. *Digital signature* fungsinya mirip seperti tanda tangan yaitu sebagai penanda sebuah dokumen. Fungsi stempel dapat diganti dengan teknik steganografi atau *watermarking*. Jika diinginkan dokumen yang memiliki tanda namun tidak dapat terdeteksi oleh orang lain, dapat digunakan teknik steganografi. Sebaliknya, jika tanda yang dibubuhkan ingin ditampilkan bisa digunakan teknik *watermarking*.

Dalam teori *digital signature*, dokumen bersama-sama dengan *signature*-nya dikirimkan ke penerima. Dengan sistem seperti ini, seorang *hacker* masih mempunyai kesempatan untuk memecahkan *digital signature*. Seorang *hacker* dapat dengan mudah mengambil dokumen dan *signature*-nya lalu mencoba melakukan *brute force attack* untuk mengubah *digital signature* dari dokumen tersebut.

Untuk memperkecil kemungkinan pengambilan *digital signature*, maka diperlukan solusi yang lebih efektif. Salah satu caranya yaitu dengan menyisipkan *digital signature* ke dalam dokumen. Proses penyisipan dokumen juga harus menggunakan teknik steganografi, agar seorang hacker tidak menyadari bahwa dalam dokumen tersebut terdapat *signature*.

Dokumen yang akan dijadikan media penyisipan harus mempunyai bit-bit redundan yang dapat dimodifikasi. *Digital signature* disispkan kedalam bit-bit redundan tersebut. Karena sifatnya yang redundan, maka perubahan terhadap bit-bit tersebut diharapkan tidak mengubah kualitas dokumen secara signifikan. Perubahan yang tidak terlalu signifikan ini tidak akan terdeteksi oleh manusia, karena indera visualisasi manusia yang memiliki keterbatasan untuk mendeteksi perubahan dalam skala satuan bit.

Dalam tugas akhir ini akan digunakan algoritma RSA dan SHA-1 sebagai algoritma *digital signature*. Proses penyisipan *digital signature* kedalam dokumen, dalam hal ini citra digital akan dilakukan dengan cara mentransformasikan citra digital. Citra digital yang semula berbentuk domain spasial ditransformasikan kedalam domain skala waktu. Teknik transformasi pada citra digital akan menggunakan DWT (*Discrete Wavelet Transform*), dengan basis *wavelet* Haar.

Latar belakang digunakannya algoritma RSA adalah karena fungsinya yang selain dapat digunakan sebagai algoritma enkripsi, tapi juga untuk autentikasi. Selain itu, keamanan RSA cukup terjamin. Hal ini dikarenakan sulitnya mencari faktor-faktor prima dari bilangan yang besar. Fungsi faktor-faktor prima di sini diperlukan untuk memperoleh kunci *private*.

Fungsi hash SHA-1 digunakan karena dalam penerapan *digital signature*, biasanya algoritma RSA digunakan bersama-sama dengan algoritma *hash function* SHA-1. Selain itu, *Output* yang dihasilkan algoritma SHA-1 adalah 160 bit.

DWT dipilih karena transformasi *wavelet* merupakan perbaikan dari teknik transformasi Fourier. Transformasi *wavelet* dapat memberikan informasi tentang kombinasi skala dan frekuensi, berbeda dengan transformasi Fourier yang hanya memberikan informasi tentang frekuensi. Selain itu transformasi Fourier berbasis pada fungsi *sinus* dan *cosinus* yang bersifat periodik dan kontinu. Hal ini akan berakibat jika akan melakukan perubahan pada suatu posisi, maka akan mempengaruhi posisi-posisi lainnya.

Basis *wavelet* Haar dipilih karena proses komputasinya yang tidak terlalu rumit, mengingat fokus aplikasi yang akan dibuat adalah pada cara pembentukan dan penyisipan *digital signature*. *Wavele*t Haar menggunakan *window rectangular* untuk mengambil sample deretan waktu, sehingga resolusi untuk perubahan pengambilan sample cenderung kasar.

1.2 Perumusan masalah

Dalam tugas akhir ini, terdapat beberapa permasalahan yang timbul yaitu :

1. Bagaimana menjamin suatu informasi adalah milik kita (kebutuhan *identity*).
2. Bagaimana menyimpan informasi (untuk menyisipkan *digital signature* pada citra digital) untuk menjamin bahwa citra digital yang dihasilkan proses invers *Discrete Wavelet Transform* sama dengan citra digital asal.
3. Bagaimana mengekstrak kembali *digital signature* yang telah disisipkan sehingga dapat dilakukan proses verifikasi.

1.3 Tujuan

Tujuan dari Tugas Akhir ini adalah :

1. Mengimplementasikan salah satu teknik kriptografi, yaitu *digital signature* dengan menggunakan fungsi hash SHA-1 dan algoritma RSA.
2. Mengimplementasikan teknik steganografi dengan menggunakan *Discrete Wavelet Transform* basis *wavelet Haar*.
3. Membuat aplikasi untuk proses steganografi antara citra digital dan *digital signature*.
4. Membuat aplikasi untuk verifikasi data hasil pemisahan antara citra steganografi dan *digital signature* untuk menjamin identitas kepemilikan data..

1.4 Metodologi penyelesaian masalah

Metode yang digunakan dalam penyelesaian tugas akhir ini adalah sebagai berikut :

1. Studi Literatur
   Mempelajari konsep kriptografi, steganografi, *digital signature*, algoritma RSA, fungsi hash satu arah SHA1, dan *Discrete Wavelet Transform*.
2. Analisis Sistem
   Mempelajari dan Menganalisis kebutuhan pada implementasi penyisipan *digital signature* pada citra digital. Analisa yang dilakukan meliputi :
   a. algoritma yang digunakan untuk implementasi *digital signature*
   b. metode transformasi yang digunakan untuk implementasi steganografi
   c. cara yang digunakan untuk menjamin citra yang dihasilkan proses invers *Discrete Wavelet Transform* sama dengan citra asal
   d. pemilihan basis *wavelet* untuk *Discrete Wavelet Transform*.
3. Perancangan dan Implementasi
   Melakukan perancangan dan mengimplementasikan implementasi penyisipan *digital signature* pada citra digital dengan metode *Discrete Wavelet Transform*. Perancangan dan Implementasi yang dilakukan terbagi dalam 4 tahap, yaitu :
   a. Mengimplementasikan *digital signature* dengan menggunakan algoritma RSA dan fungsi Hash satu arah SHA1.
   b. Mengimplementasikan steganografi dengan metode *Discrete Wavelet Transform* dengan basis *wavelet* Haar.
   c. Menyimpan informasi untuk menyisipkan *digital signature* pada citra digital.
   d. Melakukan analisa pengaruh beberapa pengolahan citra terhadap ketahanan citra hasil steganografi.
4. Pengambilan Kesimpulan dan Penyusunan Laporan Tugas Akhir