BAB I

PENDAHULUAN

1.1. Latar Belakang

Masalah keamanan data merupakan isu terpenting di dalam proses pengiriman data. Hal ini disebabkan semakin rentannya data yang beredar karena ancaman *cyber crime* (Landwehr, C., dkk, 2012). Dampak *cyber-crime* mengarah pada faktor ekonomi, psikologi, keamanan negara dan lainnya (Saini, H., dkk, 2012). Salah satu upaya mengatasi masalah ini adalah dengan menyembunyikan data dengan aman ke dalam suatu media penampung berupa teks, gambar, audio dan video. Teknik ini dikenal sebagai teknik steganografi. Pendekatan ini memungkinkan untuk melakukan komunikasi data antara satu pihak dengan pihak lain yang berkepentingan tanpa dicurigai oleh pihak yang tidak berkepentingan.

Steganografi umumnya memiliki dua tipe domain yakni transformasi dan spasial. Steganografi domain transformasi lebih tahan terhadap serangan. dibandingkan dengan domain spasial (Roy, C. Y., & Goel, M. K., 2016). DWT *(Discrete Wavelet Transform)* merupakan salah satu transformasi yang digunakan untuk teknik steganografi domain transformasi. Penggunaan *floating point* pada DWT dapat menyebabkan hilangnya beberapa informasi saat citra direkonstruksi serta menyebabkan waktu komputasi yang lebih besar. IWT *(Integer Wavelet Transform)* ialah perkembangan dari DWT yang bertujuan untuk menghindari kelemahan tersebut (Raftari, N., & Moghadam, A, M. E., 2012). IHWT *(Integer Haar Wavelet Transform)* merupakan IWT yang dikembangkan dari DHWT *(Discrete Haar Wavelet Transform)* dengan tujuan memisahkan data untuk menciptakan nilai transformasi. Salah satu penelitian tentang domain transformasi (Adi, P, W., dkk, 2015), dengan metode pengujian PSNR dan MSE menunjukkan bahwa kualitas citra stego dengan teknik IHWT menggunakan metode steganografi *modulus function* mencapai tingkat *imperceptibility* dan *fidelity* (aspek penyamaran pesan tersisip) lebih tinggi dibandingkan dengan menggunakan metode steganografi CD *(Coefficient Difference)*.

Namun, dengan memanfaatkan kelemahan yang terdapat pada steganografi, para pelaku *cyber crime* dapat dengan mudah mengakses data yang disembunyikan (Ariyus, D., 2009). Sehingga, berbagai pihak mengemukakan bahwa steganografi dianggap tidak mampu lagi memberikan pengamanan terhadap data yang akan dikirimkan (Li, B., dkk, 2011). Oleh sebab itu, diperlukan penerapan teknik kriptografi untuk mengacak isi pesan rahasia sebelum dilakukan teknik steganografi, sehingga pesan rahasia sulit ditemukan keberadaanya dan sekalipun berhasil ditemukan, pesan rahasia tersebut juga masih dalam bentuk acak sehingga tidak terbaca. Salah satu algoritma dari teknik kriptografi adalah NTRU yang merupakan algoritma kriptografi kunci asimetris. Permasalahan kriptografi kunci asimetris adalah penggunaan waktu yang lama pada pembangkitan kuncinya, pada penelitian (Challa, N., dkk, 2007) menunjukkan bahwa algoritma NTRU lebih cepat dalam prosesnya dibandingkan dengan RSA (*Rivest-Shamir-Adleman*) karena operasi bilangan bulat dan pemfaktoran pada RSA menghasilkan nilai yang besar. Dalam prosesnya NTRU memanfaatkan operasi terhadap polinom sehingga pada penerapannya pesan terlebih dahulu diubah ke dalam struktur polinomial untuk dapat dilakukan proses enkripsi dan dekripsi.

Berdasarkan uraian di atas pada penelitian ini dirancang aplikasi pengamanan pesan pada citra warna dengan judul **Pengamanan Data Teks dengan NTRU dan Metode Steganografi Modulus Function pada Koefisien IHWT suatu Citra Warna.**

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, maka yang menjadi permasalahannya adalah penggunaan *floating point* pada *DHWT* menyebabkan hilangnya beberapa informasi saat citra direkonstruksi dan membuat kualitas citra stego rendah sehingga perlu *IHWT* yang menggunakan bilangan bulat untuk mencapai *recovery*. Permasalahan selanjutnya yaitu metode steganografi *modulus function* menggunakan fungsi modulus pada perhitungan pikselnya sehingga dapat memperkecil nilai pada penyisipan dibandingkan dengan metode steganografi *coefficient difference* untuk mencapai tingkat *imperceptibility* yang tinggi serta

algoritma RSA berdasarkan pada operasi bilangan bulat dan pemfaktoran menyebabkan waktu yang lama pada prosesnya sehingga diperlukan NTRU yang berdasarkan operasi polinomial untuk mencapai sebuah sistem kriptografi yang cepat.

1.3. Tujuan

Tujuan yang akan dicapai dalam penelitian tugas akhir ini adalah mengimplementasikan NTRU dan metode steganografi *modulus function* pada koefisien IHWT pada suatu citra warna untuk menghasilkan sistem pengamanan data teks yang bersifat rahasia.

1.4. Manfaat

Manfaat dari penyusunan tugas akhir ini, yaitu sistem yang dibuat dapat digunakan sebagai alternatif pengamanan data teks dan juga penelitian ini dapat dikembangkan ataupun dijadikan referensi untuk penelitian selanjutnya.

1.5. Ruang Lingkup

Dalam upaya mencapai visi dalam penelitian tugas akhir ini, maka batasan masalah pembahasan mencakup :

1. Citra yang digunakan untuk menampung pesan adalah citra RGB 24 bit dengan format *.bmp*
2. Perkiraan kapasitas tampung sebuah citra sampul dihitung dengan rumus

$$Kapasitas\_tampung = \frac{\left(Jumlah\ piksel * \frac{3}{4}\right)}{2} * saluran * Threshold.$$

   Dimana: Jumlah piksel = Panjang piksel * lebar piksel dari citra sampul
   Saluran = 3 Komponen dari citra sampul yaitu R, G dan B.
   Threshold = Panjang bit sisip yang bernilai 1, 2 dan 3..
3. Tingkat transformasi IHWT adalah 1 kali.
4. Nilai parameter w*eighting factor (α)* = 2 yang digunakan untuk mendapatkan nilai pada baris dan kolom dari *citra* stego.

5. Nilai parameter NTRU telah ditetapkan terlebih dahulu sesuai standar *security level* yang di rekomendasi oleh *IEEE P1363.1*^{TM}*/D10* untuk menghindari kesalahan pada saat enkripsi dan dekripsi.
6. Pengujian ketahanan citra stego terhadap *noise salt and pepper* dan kontras.
7. Persentase *noise* pada pengujian terhadap *noise* adalah 0,005% yang akan dilakukan berulang-ulang sebanyak 10 kali pada masing-masing parameter set dan bit sisip.

1.6. Metodologi Penelitian

Langkah-langkah yang ditempuh dalam pengerjaan tugas akhir ini adalah menggunakan metodologi *waterfall* sebagai berikut:

1. Studi Literatur

   Pada tahap ini dilakukan studi literatur yang diantaranya mencari, memahami dan mempelajari dengan seksama berbagai macam artikel berkaitan dengan steganografi, citra warna, *data hiding*, *modulus function*, pembentukan kunci, enkripsi, dekripsi, metode *IHWT, NTRU* dan *PSNR, noise salt and pepper* yang berkaitan dengan hasil tugas akhir ini.
2. Pengembangan Aplikasi
   a. Analisis Sistem

      Pada tahap ini dilakukan analisis terhadap cara kerja sistem yang akan dibangun, dengan memakai model analisis sistem *flowchart.*
   b. Perancangan Sistem

      Pada tahap ini dilakukan perancangan dari aplikasi yang akan dibangun, seperti perancangan *interface* dengan *Balsamiq Mockups* dan sebagainya.
   c. Implementasi

      Pengembangan aplikasi yang akan dibangun dibuat dengan menggunakan software bahasa pemrograman *C#.NET*, *Visual Studio 2013*.

3. Pengujian Sistem

   a. Melakukan pengujian oleh sistem dengan mengubah parameter steganografi dan kriptografi untuk mendapatkan hasil *imperceptibility* menggunakan *MSE* dan *PSNR*.

   b. Melakukan perbandingan pada *citra stego* dengan *citra asli* untuk mendapatkan hasil *imperceptibility* menggunakan *MSE* dan *PSNR* dengan merubah citra (sebaran warna) yang berbeda dengan ukuran yang sama serta mengubah parameter kriptografi.

   c. Melakukan pengujian *robustness* pada citra stego yang menggunakan teknik IHWT melalui nilai persentase pesan yang kembali dalam mencapai *recovery* terhadap *noise salt and pepper* dan kontras.

4. Kesimpulan

   Penarikan kesimpulan akan dilakukan setelah pengujian hasil pada tahap sebelumnya.