BAB I

PENDAHULUAN

1.1. Latar Belakang

Dalam Perkembangan teknologi informasi, keamanan data adalah hal yang sangat penting, apalagi data yang dikirimkan adalah pesan yang sangat rahasia. Berbagai usaha dilakukan untuk menjamin agar pesan rahasia yang dikirimkan tersebut tidak bisa diakses oleh pihak lain (Hanafi, 2003). Dewasa ini penyembunyian pesan rahasia tidak hanya dapat dilakukan dengan menyamarkan pesan tersebut, melainkan dapat pula menyisipkan pesan tersebut dalam media lain. Dengan demikian orang lain tidak akan curiga terhadap pesan rahasia yang dikirim, karena pesan tersebut tidak terlihat, yang terlihat hanyalah media penampung pesan tersebut (E.T. Sobirina, 2009). Hal ini akan lebih aman dibandingkan dengan mengirimkan pesan dalam bentuk berkas terenkripsi yang akan membuat orang lain curiga dan berusaha untuk mengetahui isi pesan yang dikirim.

Dalam dunia keamanan data, istilah steganografi sangat dikenal. Steganografi adalah teknik menyembunyikan atau menyamarkan keberadaan pesan rahasia dalam suatu media penampungnya. Steganografi pada media digital digunakan untuk mengeksploitasi keterbatasan kekuatan sistem indera penglihatan dan pendengaran manusia, sehingga dengan keterbatasan tersebut sulit menemukan perubahan pada berkas yang telah disisipi pesan rahasia (E.T. Sobirina, 2009).

Secara teori, semua berkas yang ada di dalam komputer dapat digunakan sebagai media penampung pesan, seperti berkas citra berformat JPG, GIF, BMP, berkas *audio* berformat MP3, WAV, bahkan di dalam sebuah *video* dengan format AVI, atau dalam format lainnya seperti TXT, HTML, PDF. Semua berkas dapat dijadikan tempat bersembunyi, asalkan berkas tersebut memiliki bit-bit data redundan yang dapat dimodifikasi. Setelah dimodifikasi berkas media tersebut tidak akan banyak terganggu fungsinya dan kualitasnya tidak akan jauh berbeda dengan aslinya (Batara, 2006). *Berkas* citra merupakan media yang sering digunakan dalam dunia internet maupun dunia citra digital, ukuran *berkas*nya relatif kecil apabila dibandingkan dengan berkas *audio* atau *video*.

Salah satu format *berkas* citra yang paling sering ditemui di dunia internet maupun dunia *digital* adalah GIF. Berkas dengan format GIF berukuran lebih kecil jika dibandingkan dengan format lain untuk citra yang sama, Hal ini terjadi karena GIF menggunakan tipe kompresi *lossless*. Hal ini berarti bahwa citra tidak mengalami kehilangan kualitas ketika dikompresi (Agustinus, 2006). Seiring beragamnya pilihan media yang digunakan pada steganografi dalam dunia modern sekarang ini, maka makin beragam pula algoritma steganografi yang digunakan.

Salah satu algoritma steganografi yang digunakan untuk menyembunyikan pesan dalam berkas citra dengan format GIF adalah Gifshuffe. Algoritma Gifshuffle pada intinya memanfaatkan palet warna berkas GIF sebagai media penyisipan pesan. Dalam algoritma ini tidak terjadi perubahan apapaun dalam data berkas GIF. Sehingga menambah aspek *fidelity* dari algoritma ini.

Sesuai dengan namanya Gifshuffle akan melakukan "*shuffle*" terhadap palet warna dari sebuah berkas GIF, *shuffle* jika diterjemahkan ke dalam bahasa Indonesia berarti mengacak. Sehingga dapat diartikan bahwa GifShuffle adalah algoritma yang memanfaatkan penukaran posisi ke 256 palet warna dalam berkas citra berformat GIF. Hal tersebut aman dilakukan karena dua buah berkas GIF dengan palet warna yang berbeda akan ditampilkan secara sama persis.

Penilaian sebuah algoritma steganografi yang baik dapat dinilai dari beberapa faktor yaitu *imperceptibility* atau keberadaan pesan dalam media penampung tidak dapat dideteksi, *fidelity* yaitu mutu media penampung setelah ditambahkan pesan rahasia tidak jauh berbeda dengan mutu media penampung sebelum ditambahkan pesan, *recovery* yaitu pesan rahasia yang telah disisipkan dalam media penampung harus dapat diungkap kembali dan *robustness* yaitu pesan yang disembunyikan harus tahan terhadap berbagai operasi manipulasi yang dilakukan pada media penampung (E.T. Sobirina, 2009).

Masalah yang timbul adalah apakah algoritma Gifshuffle baik atau layak untuk digunakan dalam steganografi. Oleh karena itu akan dilakukan pengujian terhadap algoritma Gifshuffle. Pengujian tersebut meliputi pengujian terhadap ketahanan citra penampung pesan, untuk melihat apakah pesan yang disisipkan masih dapat diektraksi kembali meskipun citra mengalami beberapa perubahan akibat operasi manipulasi seperti operasi geometrik seperti rotasi, translasi (*flip*) dan *scaling* serta penambahan efek seperti efek *grayscale*.

1.2. Rumusan Masalah

Sesuai dengan latar belakang yang telah dijelaskan di atas, maka dapat dirumuskan sebuah pokok permasalahan, yaitu:

1. Bagaimana mengimplementasikan steganografi sebagai salah satu teknik untuk mengamankan data digital dengan algoritma Gifshuffle?
2. Bagaimana hasil pengujian ketahanan algoritma Gifshuffle terhadap berbagai operasi manipulasi yang dilakukan pada media penampung?

1.3. Tujuan Penelitian

Tujuan Tujuan dari penulisan tugas akhir ini adalah :

1. Mengimplementasikan teknik steganografi dengan algoritma Gifshuffle untuk mengamankan data digital.
2. Melakukan pengujian *robustness* (ketahanan) algoritma Gifshuffle terhadap beberapa operasi manipulasi yang dilakukan pada media penampung.
3. Melakukan analisa terhadap citra stego setelah dilakukan penambahan operasi manipulasi.

1.4. Batasan Masalah

Dalam tugas akhir ini pembahasan hanya terbatas pada pengamananan data untuk data teks (*.txt) dengan media citra non-transparan berformat GIF dengan menerapkan algoritma Gifshuffle.

1.5. Manfaat Penelitian

Manfaat yang dapat diambil dari penulisan tugas akhir ini adalah :

1. Memahami penerapan algoritma Gifshuffle untuk steganografi sebagai teknik pengamanan data digital.
2. Memberikan pandangan bahwa steganografi dengan menggunakan algoritma Gifshuffle menambah tingkat pengamanan data digital.

1.6. Metodologi Penelitian

Metodologi yang diterapkan dalam pembuatan skripsi ini, antara lain:

1. Eksplorasi dan Studi Literatur

   Eksplorasi dan studi literatur dilakukan dengan mempelajari konsep-konsep yang berkaitan dengan skripsi ini, seperti steganografi, algoritma *Gifshuffle*, citra digital, melalui literatur-literatur seperti buku (*textbook*), paper, dan sumber ilmiah lain seperti situs internet ataupun artikel dokumen teks yang berhubungan.

2. Analisis dan Perancangan Perangkat Lunak

   Analisis dan perancangan perangkat lunak dilakukan untuk menentukan permasalahan mengenai bahasa pemrograman yang akan digunakan, struktur data, input/output program, dan permasalahan teknik algoritma yang akan dimplementasikan.

3. Implementasi Program dan Pengujian Performansi

   Detail mengenai implementasi program dilakukan sesuai hasil analisis pada tahapan sebelumnya.

4. Hasil Akhir dan Penarikan kesimpulan

   Analisis hasil dilakukan untuk mengetahui performansi pembangunan aplikasi steganografi dengan menggunakan algoritma *gifshuffle* serta pengujian terhadap media penampung, jika ternyata hasilnya baik, maka dilakukan analisis akhir untuk mengetahui penyebabnya, selanjutnya dilakukan penarikan kesimpulan.

1.7. Sistematika Penulisan

BAB I : PENDAHULUAN

Dalam bab ini dijelaskan peranan steganografi khususnya dalam sistem pengamanan data yang termuat dalam latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Dalam bab ini dijelaskan dasar-dasar teori yang menjadi acuan dalam proses pembuatan aplikasi steganografi.

BAB III : METODOLOGI PENELITIAN

Dalam bab ini dijelaskan metode yang digunakan dan tahapan-tahapan teknik steganografi dalam bentuk algoritma.

BAB IV : HASIL PENELITIAN DAN PEMBAHASAN

Dalam bab ini dijelaskan mengenai implementasi program, uji coba dan analisanya.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini berisi kesimpulan dan saran.

DAFTAR PUSTAKA