BAB I
PENDAHULUAN

1.1. Latar Belakang

Semakin berkembangnya dan semakin canggihnya teknologi, membuat pekerjaan yang dilakukan oleh manusia menjadi semakin ringan. Banyak dampak positif yang manusia rasakan terutama dalam akses komunikasi yang tidak terbatas ruang dan waktu, sehingga baik perangkat komputer maupun telepon gengam dapat saling terhubung dan dengan mudahnya dapat bertukar data. Seiring dengan kemudahan dirasakan, juga muncul dampak negatifnya, salah satunya ancaman yang ada dunia maya dapat membuat kebanyakan orang khawatir akan keamanan informasi yang akan dikirimnya. Hal semacam ini tentunya dapat membuat informasi yang dikirim menjadi terhambat, sedangkan informasi tersebut sangat penting bagi orang-orang tersebut.

Masalah keamanan merupakan salah satu aspek penting dalam pengiriman data dan informasi dalam suatu jaringan. Salah satu cara yang biasa digunakan untuk mengamankan data adalah dengan memanfaatkan steganografi. Steganografi merupakan suatu seni untuk menyembunyikan suatu data, di mana data tersebut disembunyikan ke dalam suatu media yang tampak biasa saja. Digital steganografi memerlukan suatu media sebagai tempat penyembunyian informasi. Secara teori penyisipan informasi pada data digital dengan menggunakan teknik steganografi dapat dilakukan pada semua format data digital yang ada dalam komputer sebagai media penyamarannya, sebagai contoh format teks, format citra, bahkan untuk format audio, asalkan file-file tersebut mempunyai bit-bit data redundan yang dapat dimodifikasi[1].

Teknik steganografi semakin dibutuhkan guna memberikan keamanan dalam proses mengirim informasi terutama yang berhubungan dengan citra. Steganografi merupakan cara untuk menyembunyikan suatu pesan atau informasi rahasia ke dalam media lain. Steganografi hampir sama dengan kriptografi, dalam arti masih ada perbedaan di mana kriptografi berfokus pada menjaga isi rahasia

pesan, sedangkan steganografi berfokus pada menjaga keberadaan pesan rahasia. Pesan yang dienkripsi menggunakan algoritma kriptografi akan menimbulkan kecurigaan dan akan memicu seseorang untuk berusaha memecahkannya. Berbeda dengan steganografi, penyembunyian pesan dengan teknik ini akan menyembunyikan pesan ke dalam citra digital dan tidak akan menimbulkan kecurigaan terhadap orang yang melihatnya, karena citra yang sudah disisipkan tidak berubah secara kasat mata.

Algoritma steganografi yang paling populer adalah Least Significant Bit (LSB). Least Significant Bit adalah salah satu metode untuk menyembunyikan pesan ke dalam media digital dengan cara menyisipkan pesan tersebut pada satu *bit* paling kanan piksel obyek. Algoritma ini merupakan jenis steganografi subtitusi, yaitu menggantikan setiap *bit* paling kanan dari masing-masing nilai warna piksel citra dengan setiap *bit-cipher-text*. Proses subtitusi ini dilakukan secara berurutan untuk setiap piksel. Setelah pesan disisipkan, file citra yang merupakan hasil steganografi tersebut dapat dikirimkan kepada si penerima pesan. Dengan adanya steganografi, semua pihak yang tidak berhak untuk mengakses informasi tidak akan menyadari keberadaan informasi karena yang dikirimkan adalah file citra dan bukan *cipher-text*. Hal inilah yang menjadikan steganografi sebagai pelengkap keamanan steganografi.

Algoritma Fisher-Yates Shuffle adalah sebuah algoritma yang menghasilkan permutasi acak dari suatu himpunan terhingga, dengan kata lain untuk mengacak suatu himpunan tersebut. Jika di implementasikan dengan benar maka hasil dari algoritma ini tidak akan berat sebelah, sehingga setiap permutasi memiliki kemungkinan yang sama. Algoritma Fisher-Yates Shuffle penulis pandang dapat diterapkan pada steganografi citra digital, sehingga penulis mengambil penelitian dengan judul **"IMPLEMENTASI APLIKASI STEGANOGRAFI PADA CITRA DIGITAL DENGAN ALGORITMA FISHER-YATES SHUFFLE DAN LSB".**

Penelitian terdahulu yang digunakan sebagai acuan dalam penelitian ini yaitu: Penelitian Yohanes Julianto dan Kristoforus Jawa Bendi[2] pada tahun 2015 berjudul "Sistem Steganografi Dengan Metode Least Significant Bit (LSB)

Teracak"; Penelitian Nur Aisyah[3] pada tahun 2016 berjudul "Implementasi Metode Fisher Yates Shuffle Untuk Pengacakan Pertanyaan Pada Game Ali And The Labirin"; Penelitian Bryan Mayers Talapessy, Magdalena A, Ineke Pakereng, Evangs Mailoa[4] pada tahun 2014 berjudul "Perancangan Aplikasi Steganografi Menggunakan Algoritma Fisher"; Penelitian Ryan Nugraha, dkk.[5] pada tahun 2016 berjudul "Penerapan Algoritma Fisher-Yates Pada Aplikasi The Lost Insect Untuk Pengenalan Jenis Serangga Berbasis Unity 3D"; dan Penelitian Abe-Ibijila dan Abejide Olu[6] pada tahun 2012 berjudul "Merancang Aplikasi A Simulated Enhancement Of Fisher-Yates Algorithm For Shuffling In Virtual Card Games Using Domain Specific Data Structures".

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah penelitian ini adalah: "Bagaimana mengimplementasikan aplikasi steganografi pada citra digital dengan algoritma Fisher-Yates Shuffle dan LSB?"

1.3. Batasan Masalah

Adapun hal-hal yang menjadi batasan pada penelitian ini antara lain:

1. Pesan yang disisipi ke dalam media pembawa berupa teks. Selain itu, media pembawa dapat disisipkan file dengan ekstensi apa saja, selama ukurannya tidak lebih besar dibandingkan media pembawa.
2. Media pembawa (*cover object*) yang digunakan adalah file citra dengan ekstensi (*.jpg, *.jpeg, *.png, *.bmp, *.gif, *.tiff) dan hasil keluaran yang dijadikan *stego-image* adalah file citra dengan ekstensi (*.png, *.bmp).

1.4. Metodologi Penelitian

Metodologi penelitian yang digunakan terdiri dari:

1. Model pengembangan perangkat lunak yang digunakan adalah Waterfall dengan tahapan: identifikasi masalah dan studi literatur, perancangan sistem, perancangan prototipe, pengujian sistem dan analisis hasil pengujian, serta pemeliharaan.

2. Object Oriented Programming (OOP) digunakan sebagai metode pengembangan perangkat lunak.
3. Alat bantu pengembangan perangkat lunak menggunakan UML (Unified Modeling Language), yang terdiri dari Activity Diagram, Use Case Diagram, Class Diagram, dan Sequence Diagram.

1.3. Tujuan dan Manfaat Penelitian

1.3.1. Tujuan

Tujuan penelitian ini adalah mengimplementasikan aplikasi steganografi pada citra digital dengan algoritma Fisher-Yates Shuffle dan LSB.

1.3.2. Manfaat

a. Bagi Penulis
   1) Menambah wawasan dan sebagai referensi pengetahuan tentang teknik steganografi.
   2) Mengetahui proses-proses yang terjadi pada pengamanan data teks ke dalam file citra hasil steganografi yang berformat BMP dan PNG.

b. Bagi Pemakai
   1) Sebagai referensi dan alternatif untuk metode pengiriman pesan rahasia secara aman.
   2) Melindungi informasi yang dianggap penting dan rahasia dari pihak yang tidak bertanggung jawab, sehingga informasi yang diterima tetap aman dan terjaga kerahasiaannya dengan kondisi yang sebenar-benarnya.

1.4. Sistematika Penulisan

Sistematika penulisan laporan ini dibagi ke dalam lima bab sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, metodologi penelitian, tujuan dan manfaat penulisan, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menjelaskan tentang teori tentang RAD (Rapid Application Development), Object Oriented Programming (OOP), UML, Keamanan Informasi, Citra Digital, Pengukuran *Error* Citra, Steganografi, LSB, Fisher-Yates Shuffle, Kriptografi, .NET Platform, .NET Framework, Pengujian Black Box, tinjauan perangkat lunak, dan penelitian terkait.

BAB III METODE PENELITIAN

Bab ini menjelaskan tentang model pengembangan perangkat lunak, metode penelitian sistem, dan alat bantu pengembangan sistem.

BAB IV PEMBAHASAN DAN HASIL

Bab ini membahas mengenai analisa masalah, perancangan sistem, perancangan antar muka aplikasi, dan implementasi.

BAB V PENUTUP

Bab ini membahas tantang kesimpulan dari bab-bab sebelumnya serta saran yang diberikan berdasarkan hasil kesimpulan tersebut.