

BAB I

PENDAHULUAN

I.1. Latar Belakang

Seiring dengan sangat pesatnya perkembangan jaringan data dan kemajuan teknologi informasi khususnya di bidang komputer memungkinkan seorang untuk berkomunikasi dan bertukar informasi dengan orang lain di dunia maya. Pertukaran informasi di dunia maya atau yang biasa disebut internet. Dalam dunia maya ini bisa mendapat banyak informasi yang kita butuhkan hanya membutuhkan sebuah perangkat yang terhubung ke internet. Informasi yang kita dapatkan bisa bermacam-macam format, diantaranya : teks, citra, *audio*, maupun *video*. Seiring dengan kemajuan teknologi seperti itu akan menimbulkan beberapa ancaman terhadap informasi yang di dapatkan, hal tersebut membutuhkan sebuah keamanan untuk informasi tersebut.

Pengamanan informasi tersebut sangat dibutuhkan untuk menjaga kerahasiaan dari informasi yang dikeluarkan. Oleh karena itu dibutuhkan sebuah system keamanan data yang dapat mengikuti perkembangan teknologi di dunia maya sehingga data/informasi yang dikirimkan tidak jatuh kepada orang yang tidak berhak atau memodifikasinya. Sekarang ini terdapat system pengamanan data yang biasa dikenal dengan kriptografi.

Kriptografi merupakan satu bidang ilmu yang mempelajari tentang bagaimana merahasiakan suatu informasi penting kedalam suatu bentuk yang tidak dapat dibaca oleh siapapun serta mengembalikannya kembali menjadi informasi semula dengan menggunakan berbagai macam teknik yang telah ada

sehingga informasi tersebut tidak dapat diketahui oleh pihak manapun yang bukan pemilik atau yang tidak berkepentingan. (Saipul, 2012 : 5)

Kriptografi tidak hanya digunakan untuk data dalam bentuk teks, melainkan juga diterapkan untuk data dalam bentuk citra (gambar). Citra (gambar) merupakan salah satu bentuk multimedia yang penting. Citra menyajikan informasi secara visual dan informasi yang disajikan secara tekstual. Diantara file bentuk digital, file citra (digital) yang paling rentan untuk operasi illegal berupa duplikat, modifikasi, bahkan untuk dipalsukan. Sehingga banyak informasi berupa data citra (gambar) yang perlu diamankan dan dijaga kerahasiaannya agar tidak disalahgunakan oleh orang yang tidak berhak. Oleh karena itu diperlukan aplikasi yang dapat membantu pemakai menjaga kerahasiaan dari data/informasi yang mereka miliki. Untuk menjamin keamanan data berupa citra digital yang ditransmisikan, maka citra digital dienkripsi dengan cipher enkripsi (algoritma enkripsi) menjadi *cipher image* atau gambar yang tidak memiliki arti. Setelah sampai di tujuan, maka *cipher image* didekripsikan kembali dengan *cipher* dekripsi menjadi citra yang serupa dengan citra asli yang diterima oleh penerima.

Dari sekian banyak jenis kriptografi yang ada, tidak semuanya bisa diterapkan untuk mengenkripsi data citra (gambar). Namun hal ini biasa diatasi dengan menggunakan metode *vigenere chiper* dengan penambahan dan pengurangan RGB pada citra. Berdasarkan penjelasan diatas maka penulis tertarik untuk menulis judul **“Perancangan Aplikasi Keamanan Citra Dengan Penambahan Dan Pengurangan Nilai RGB Menggunakan Metode *Vigenere Chiper*”**.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Adapun identifikasi masalah dalam penulisan skripsi ini adalah:

1. Rentannya sistem keamanan data pada jaringan computer.
2. Adanya pihak yang tidak berhak untuk mengetahui privasi atau kerahasiaan data pada saat pengiriman berlangsung.
3. Sistem keamanan data yang mudah dipecahkan orang lain.
4. Sulitnya dalam merancang dan mengimplementasikan sistem keamanan data.

I.2.2. Rumusan Masalah

Adapun perumusan masalah pada perancangan aplikasi keamanan citra dapat dirumuskan sebagai berikut:

1. Bagaimana aplikasi ini akan menghilangkan keaslian file citra?
2. Bagaimana aplikasi ini mengacak nilai RGB dan merubah keaslian warna citra?
3. Bagaimana menerapkan metode vigenere chipper pada keamanan citra?

I.2.3. Batasan Masalah

Adapun batasan masalah dalam perancangan aplikasi keamanan citra adalah sebagai berikut :

1. Aplikasi ini hanya digunakan untuk enkripsi file berbasis *image*
2. Aplikasi ini digunakan untuk file *image* berekstensi .jpg
3. Metode yang digunakan adalah *vigenere chipper*

4. Data diamankan pada saat proses pengiriman citra
5. Aplikasi yang dibangun tidak hanya dibatasi untuk mengenkripsi file citra, tetapi juga dapat mengembalikan dan mendiskripsikannya sehingga didapat pesan asli.
6. Dalam merancang aplikasi, penulis menggunakan bahasa pemrograman *Visual Basic .Net 2010*

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Berdasarkan perumusan masalah di atas maka tujuan yang ingin dicapai dalam penulisan skripsi ini adalah sebagai berikut :

1. Membuat sebuah aplikasi yang mampu mengamankan file citra dengan baik.
2. Menghasilkan sebuah sistem keamanan data citra dengan menggunakan metode *vigenere chiper*.
3. Menghasilkan citra yang tidak sesuai dengan aslinya agar tidak dapat dibaca untuk dilihat pengguna lain.

I.3.2. Manfaat

Manfaat yang diharapkan dari penulisan skripsi ini adalah :

1. Memberikan pengetahuan tentang bagaimana caranya sebuah aplikasi kriptografi dapat mengamankan file citra.
2. Pengembangan sistem dan aplikasi ini dapat digunakan untuk sistem pengamanan file lainnya.

3. Dengan adanya sistem ini dapat membantu dalam ilmu pengetahuan khususnya jaringan.

I.4. Metodologi Penelitian

Berisi langkah-langkah yang diperlukan untuk mencapai tujuan perancangan yang dilakukan. Adapun metodologi dalam pengumpulan data adalah sebagai berikut:

1. Pengumpulan Data

Yaitu mengumpulkan data dari buku , artikel dan karya ilmiah maupun situs internet dan sumber lainnya yang menunjang dalam penulisan skripsi ini.

2. Pengujian dan analisis hasil

Tahapan dimana penulis melakukan analisis terhadap cara kerja dari algoritma serta kekurangan dan kelebihan algoritma, setelah terlebih dahulu dilakukan uji coba terhadap algoritma tersebut dalam melakukan proses pengamanan citra.

3. Studi Kepustakaan (*Library Research*)

Penulis melakukan studi pustaka untuk memperoleh data yang ada hubungannya dengan konsep keamanan data, citra, kriptografi dan algoritma *vigenere cipher*, serta uraian teoritis bahasa pemrograman dengan *Visual Basic* 2010.

I.5. Keaslian Penelitian

Tabel dibawah ini merupakan perbandingan antara penelitian yang dilakukan sebelumnya dengan penelitian yang dirancang penulis:

Tabel I.1. Tabel Perbandingan Penelitian

No	Nama Peneliti	Judul	Sistem Yang Dihasilkan
1	Rohmat Nur Ibrahim, 2012.	Kriptografi Algoritma DES, AES/Rijndael, Blowfish Untuk Keamanan Citra Digital Dengan Menggunakan Metode Discrete Wavelet Transformation (DWT).	Proses pengacakan citra digital menggunakan metode Transformasi Wavelet Diskrit sehingga proses tersebut menghasilkan pengolahan dan pengacakan dari sisi piksel lebih cepat
2	Rinaldi Munir, 2012.	Algoritma Enkripsi Citra Digital Berbasis Chaos Dengan Penggabungan Teknik Permutasi Dan Teknik Substitusi Menggunakan Arnold Cat Map Dan Logistic Map	Algoritma ini mampu mengenkripsi sembarang citra (baik citra grayscale maupun berwarna) dengan baik. Analisis korelasi menunjukkan bahwa pixel-pixel didalam chipper image tidak berkorelasi, sehingga membuat serangan dengan analisis statistik menjadi sulit.

Berdasarkan dari penelitian sebelumnya, maka penulis melakukan penelitian yang berbeda dengan penelitian sebelumnya. Dimana penulis membuat sebuah penelitian dengan judul “ Perancangan Aplikasi Keamanan Citra Dengan Penambahan dan Pengurangan Nilai RGB Menggunakan Metode *Vigenere Chipper*

“*Vigenere chiper* merupakan satu jenis kriptografi klasik yang pada dasarnya adalah melakukan substitusi *cipher* abjad majemuk (*polyalphabetic substitution*). Proses enkripsi dilakukan dengan penambahan dan penurangan dan merubah nilai warna RGB. Berbeda nilai kunci yang digunakan, berbeda pula hasil enkripsi citra .

I.5. Sistematika Penulisan

Sistematika penulisan skripsi ini dibagi menjadi lima bab yang merangkum tiap tahapan yang penulis lakukan, antara lain:

BAB I : PENDAHULUAN

Menguraikan tentang latar belakang, identifikasi masalah, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II : LANDASAN TEORI

Membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap hasil penelitian tentang keamanan citra.

BAB III : ANALISIS DAN PERANCANGAN

Bab ini menjelaskan mengenai analisa dan perancangan tampilan *form* dan aplikasi , pemilihan *software* yang digunakan dan analisis perhitungan algoritma kriptografi simetris.

BAB IV : HASIL DAN UJI COBA

Merupakan tahapan hasil dari perancangan dan pengujian terhadap program yang dibuat pada keamanan citra.

BAB V : KESIMPULAN DAN SARAN

Merupakan tahap akhir yang menyajikan kesimpulan yang diperoleh dari semua pembahasan serta saran untuk pengembangan perancangan aplikasi selanjutnya.