PENGGABUNGAN STEGANOGRAFI LSB DAN LCG UNTUK PENGAMANAN DATA DOKUMEN PADA FILE GAMBAR

[1]Dzulkifli Nur Rahman (10018156), [2]Eko Aribowo (0006027001)
Program Studi Teknik InformatikaUniversitas Ahmad Dahlan
Jl. Prof. Dr. Soepomo, Telp. (0274) 379418
Email : djulkiplie@gmail.com[1], ekoab@tif.uad.ac.id[2]

ABSTRAK

Perkembangan teknologi saat ini berjalan sangat pesat dalam berbagai aspek. Salah satu aspek yaitu internet, yang memungkinkan untuk terhubung keseluruh dunia tanpa batas ruang dan waktu. Dengan internet akan memudahkan untuk saling berbagi informasi digital yang dapat berbentuk teks, gambar, audio maupun video. Selain kemudahan yang ditawarkan, tentunya ada ancaman keamanan yang dihadapi seperti mengakses informasi yang bukan menjadi haknya. Dengan adanya resiko tersebut perlu dibuat sebuah mekanisme untuk mengatasi ancaman keamanan. Melindungi data digital menggunakan enkripsi teks biasa masih mengundang kecurigaan bagi pihak yang melihatnya. Oleh karena itu informasi perlu disamarkan ke media tertentu.

Subjek dalam penelitian ini yaitu bagaimana mengimplementasikan steganografi untuk mengamankan data menggunakan metode *least significant bit* dan *linear congruential generator.* Tahap penelitian dimulai dari pengumpulan data dilakukan dengan metode studi pustaka, *browsing* dan *running* program steganografi. Tahapan dalam pengembangan aplikasi ini meliputi analisis sistem, analisa kebutuhan, perancangan DFD (*Data Flow Diagram*), perancangan antarmuka, implementasi program dan pengujian sistem menggunakan *black box test* dan *alpha test*.

Hasil dari penelitian ini adalah sebuah aplikasi **penggabungan steganografi lsb dan lcg untuk pengamanan data dokumen pada file gambar**yang dapat digunakan untuk menyembunyikan *file* dokumenberformat .doc dan .docx ke dalam sebuah *file* gambar berformat bitmap dengan menggunakan password. Hasil uji coba menunjukkan bahwa aplikasi ini mampu melakukan proses penyisipan dan penguraian pesan dan berguna untuk mengamankan data.

Kata kunci : Steganografi, Kriptografi, *Least Significant Bit*, *Linear Congruential Generator*

1. Pendahuluan

1.1 Latar Belakang Masalah

Perkembangan teknologi saat ini berjalan sangat pesat dalam berbagai aspek. Salah satu aspek yaitu internet, yang memungkinkan untuk terhubung keseluruh dunia tanpa batas ruang dan waktu. Dengan internet akan memudahkan untuk saling berbagi informasi digital yang dapat berbentuk teks, gambar, audio maupun video. Selain kemudahan yang ditawarkan, tentunya ada ancaman keamanan yang dihadapi seperti mengakses informasi yang bukan menjadi haknya bahkan sampai menyebarkan virus. Dengan adanya resiko tersebut perlu dibuat sebuah mekanisme untuk mengatasi ancaman keamanan atau melindungi data-data digital dari hal yang bertujuan untuk mengganggu bahkan merusaknya [1].

Dalam sebuah gambar dapat tersirat banyak makna yang berbeda bagi orang yang melihatnya, sehingga setiap orang akan memiliki argumen yang bermacam-macam sesuai dengan apa yang disimpulkan oleh pemikirannya sendiri. Disisi lain ada gambar yang memang dipersiapkan oleh pembuatnya agar penikmat gambar dapat mengartikan satu gambar menjadi dua atau lebih arti yang berbeda. Hal tersebut banyak dijumpai dalam kehidupan nyata, dimana gambar dijadikan sebuah media pembelajaran bahkan media promosi suatu produk. Berdasarkan perbedaan argumen tentang gambar tersebut dan tidak hanya sekedar menikmati gambar, maka gambar itu juga bisa dijadikan sebagai media untuk menyembunyikan sesuatu di dalam gambar tersebut. Sesuatu dalam hal ini dapat dikatakan sebagai *information hidding*, atau yang sering disebut dengan penyembunyian informasi ke dalam media lain seperti gambar.

Dengan munculnya *information hidding* tersebut, maka dapat dilakukan penyisipan informasi rahasia ke dalam satu gambar. Metode ini tentunya tidak menarik perhatian sehingga media penampung yang membawa pesan tidak menimbulkan kecurigaan bagi pihak ke tiga. Untuk mengetahui informasi rahasia yang sudah disisipkan ke dalam gambar juga memerlukan mekanisme yang akan banyak memakan waktu. Hal ini tentunya akan berbeda jika informasi hanya dilakukan dengan enkripsi teks saja yang akan mengundang kecurigaan bagi penerimanya. Oleh karena itu informasi perlu disamarkan ke media tertentu [2].

Steganografi adalah ilmu menyembunyikan teks pada media lain yang telah ada sehingga teks yang tersembunyi menyatu dengan media itu. Media tempat penyembunyian pesan tersembunyi dapat berupa media teks, gambar, audio atau video. Steganografi yang kuat memiliki sifat media yang telah tertanam teks tersembunyi sulit dibedakan dengan media asli namun teks tersembunyi tetap dapat diekstrasi [3].

Salah satu metode steganografi pada media gambar misalnya dengan mengubah nilai *Least Significant Bit* (LSB) pada *byte* intensitas piksel dengan teks yang ingin disembunyikan. Metode LSB ini memanfaatkan banyaknya warna pada media gambar bitmap 24 bit yang tersusun lebih dari 16 jt warna. Sebelum disisipkan ke dalam tiap bit terakhir komponen tiap warna, tentunya *plaintext* akan dienkripsi dengan kunci yang dibangkitkan terlebih dahulu sehingga menghasilkan *ciphertext*.

Berdasarkan informasi diatas, maka akan dibuat sebuah gabungan dengan menerapkan metode LSB dan LCG yang dibentuk kedalam Tugas Akhir untuk menyelesaikan studi di Universitas Ahmad Dahlan dengan judul "Penggabungan Steganografi LSB Dan LCG Untuk Pengamanan Data Dokumen Pada File Gambar".

2. Landasan Teori

2.1 Kriptografi

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan, data atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna [2]. Ada juga pengertian lain bahwa kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Definisi ini mungkin cocok pada masa lalu dimana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat dan mata-mata. Namun saat ini kriptografi lebih dari sekedar *privacy*, tetapi juga untuk tujuan data *integrity*, *authentication* dan *non-repudiation*. Tidak semua aspek keamanan informasi ditangani oleh kriptografi. [2]

2.2 Steganografi

Steganografi adalah teknik menyembunyikan suatu informasi yang rahasia atau sensitif pada suatu media perantara agar tidak terlihat seperti semestinya. Kata steganografi diambil dari bahasa yunani yaitu *Steganos* (menyembunyikan) dan *Graptos* (menulis) [4]. Dengan menggukan steganografi, pesan rahasia dapat disisipkan ke dalam sebuah media yang tidak mencurigakan dan mengirimnya tanpa ada seorang pun yang mengetahui keberadaan pesan tersebut.

2.3 Citra Gambar

2.3.1 Konsep Citra Gambar

Citra gambar adalah data yang ditampilkan dalam bentuk gambar sehingga memiliki arti tertentu. Sebuah citra gambar menyimpan data berupa bit yang dapat dimengerti oleh manusia dengan visualisasi bit tersebut pada kanvas menjadi gambar. Pengolahan yang dapat dilakukan terhadap citra gambar antara lain adalah menampilkan bentuk gambar, melakukan perubahan terhadap gambar (*image editing*), dan pencetakan citra gambar ke atas media berupa kertas.

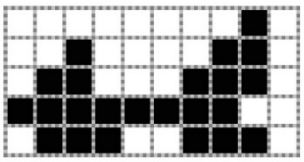
Citra gambar terdiri dari piksel-piksel berukuran kecil yang membentuk sebuah bentuk gambar yang dapat dilihat oleh mata manusia. Kepadatan piksel-piksel yang ada dalam gambar ini disebut dengan resolusi. Semakin besar resolusi maka kualitas gambar dari citra gambar tersebut semakin baik.

2.3.2 Representasi Citra Gambar

Pada citra gambar, data yang ada direpresentasikan dalam bentuk matriks. Matriks tersebut berukuran sesuai dengan ukuran jumlah pikselnya. Jika suatu citra gambar memiliki ukuran 100x100 piksel, maka matriks yang merepresentasikan citra gambar tersebut memiliki dimensi 100x100. Setiap elemen matriks terdiri dari bit-bit warna yang menyusun piksel tersebut.

Jika pada sebuah citra gambar dengan warna hitam-putih dan berukuran 10x5 piksel didefinisikan bahwa bit 0 menandakan warna piksel putih dan bit 1 merupakan representasi warna piksel hitam, maka contoh representasi matriks M dan gambar dari citra gambar tersebut dapat dilihat pada Gambar 1 [5].

$$M = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$



Gambar 1. Representasi Citra Gambar dalam Matriks [9]

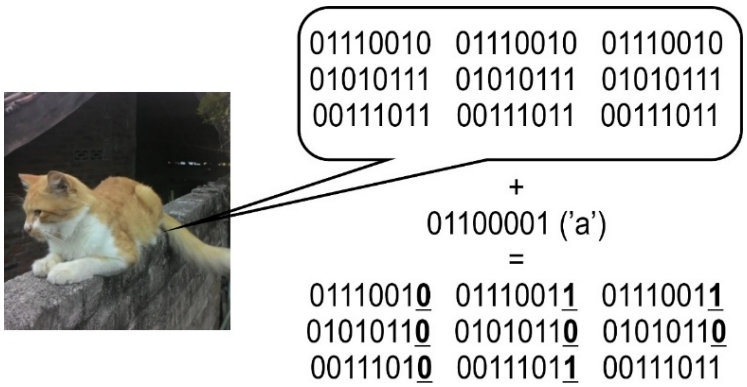
2.3.3 Warna Pada Citra Gambar

Citra gambar memiliki beberapa jenis cara pewarnaan. Tiap jenis pewarnaan ini memiliki karakteristik masing-masing. Jenis pewarnaan ini memberikan pengaruh pada citra gambar sehingga memiliki jumlah warna yang berbeda (perbedaan kualitas warna) dan pengaruh pada ukuran dokumen.

2.4 Least Significant Bit

Least Significant Bit merupakan metode steganografi yang paling sederhana. Untuk menjelaskan metode ini perlu menggunakan citra gambar sebagai *covertext*. Setiap *pixel* di dalam gambar berukuran 1 sampai 3 *byte*. Pada susunan bit dalam sebuat *byte,* adabit yang paling berarti (*Most Significant Bit)* dan bit yang kurang berarti *(Least Significant Bit)*. Misalnya pada byte 10011100, bit terahir yang digaris bawahi merupakan bit LSB. Bit yang cocok untuk diganti dengan bit pesan adalah bit LSB, sebab modifikasi hanya mengubah nilai byte tersebut satu lebih tinggi atau satu lebih rendah [2].

Contoh penggunaan metode LSB pada gambar bitmap 24 bit, diambil sebuah daerah yang memiliki tiga piksel, dimana masing-masing piksel memiliki 24 bit data yang terdiri dari 8 bit warna merah, 8 bit warna hijau dan 8 bit warna biru. Pesan yang disisipkan adalah sebuah karakter ‘a’, dengan bilangan ASCIInya adalah 97 atau 01100001 dalam format biner. Hasil dari penyisipan ditunjukkan dengan bit yang bergaris bawah sebagai bit pesan, dimana bit yang dicetak tebal adalah bit yang berubah seperti yang terlihat pada Gambar 2.



Gambar 2. Proses Penyisipan dengan Metode LSB

Akibat dari penyisipan ini adalah bertambah atau berkurangnya nilai warna tertentu pada piksel tersebut sebesar 1 bit dan manusia tidak dapat mendeteksi perubahan yang sekecil ini. Oleh karena efek perubahan yang kecil, metode LSB merupakan metode yang paling populer digunakan. Akan tetapi gambar hasil penyisipan ini tidak tahan terhadap manipulasi gambar, seperti mengubah ukuran resolusi gambar atau pengubahan format gambar ke dalam format lain. Perlakuan demikian akan merusak bit-bit pesan didalamnya, sehingga pesan tidak dapat dibaca kembali [2].

2.5 Kriptografi LCG

Pembangkit bilangan acak kongruen-lanjar (LCG) adalah salah satu pembangkit bilangan acak tertua dan sangat terkenal. LCG didefinisikan dalam relasi rekurens $x_n=(ax_{n-1}+b)$ mod $m$yang dalam hal ini,

x_n= bilangan acak ke-n dari deretnya
x_{n-1}= bilangan acak sebelumnya
a = faktor pengali
b = increment
m = modulus

Keunggulan LCG terletak pada kecepatannya dan hanya membutuhkan sedikit operasi bit. Dalam kasus ini LCG digunakan untuk membangkitkan bilangan acak dari kunci yang akan di XOR kan dengan *plaintext*. [2]

2.6 Data Flow Diagram

Data Flow Diagram (DFD) merupakan diagram yang mengunakan notasi-notasi atau simbol-simbol untuk menggambarkan sistem jaringan kerja antar fungsi-fungsi yang berhubungan satu sama lain dengan aliran dan penyimpanan data [6]. DFD sering digunakan untuk menggambarkan suatu sistem yang telah ada atau sistem baru yang akan dikembangkan secara logika tanpa mempertimbangkan lingkungan fisik dimana data tersebut mengalir atau dimana data tersebut akan disimpan. Salah satu keuntungan menggunakan diagram aliran data adalah memudahkan pemakai yang kurang menguasai bidang computer untuk mengerti sistem yang akan dikerjakan.

DFD terdiri dari diagram konteks (*context diagram*) dan diagram rinci *(level diagram*). Diagram konteks adalah diagram yang terdiri dari suatu proses dan menggambarkan ruang lingkup suatu sistem. Diagram konteks merupakan level tertinggi dari DFD yang menggambarkan seluruh *input* ke sistem atau *output* dari sistem. Dalam diagram konteks biasanya hanya ada satu proses. Tidak boleh ada *store* dalam diagram konteks. Diagram rinci adalah diagram yang menguraikan proses apa yang ada dalam diagram level di atasnya.

2.7 Konversi

Fungsi yang digunakan untuk mengonversi nilai intensitas pixel yang masih berupa angka desimal menjadi angka biner selain itu juga digunakan untuk mengkonversi kode ASCII dari pesan menjadi angka biner [7]. Fungsi yang digunakan untuk mengkonversi angka biner menjadi angka desimal dalam menentukan nilai intensitas piksel yang telah diubah, selain itu juga digunakan dalam mengkonversi nilai-nilai palet yang menunjukkan baris dan kolom menjadi angka desimal untuk mengetahui baris dan kolom terakhir pesan disisipkan. Kegunaan lain dari fungsi desimal dalam steganografi yakni mengkonversi biner menjadi desimal yang akan menunjukkan kode ASCII pesan.

2.8 BIT

Bit adalah sebuah digital dari sistem bilangan binary (*binary numeral system*), yaitu sistem bilangan berbasis 2. *Binary digits* ini hampir selalu digunakan sebagai dasar perhitungan kemampuan menampung pada media penyimpan data (*storage*), perhitungan secara digital dan pembelajaran teori informasi secara digital. Sebuah bit dari storage adalah laksana sebuah saklar lampu (*light switch*) yang bisa dihidupkan dan dimatikan [8].

2.9 Byte

Untuk lebih memberi arti, bit di atas selanjutnya digabung (dikombinasikan nilai-nilainya) dan saling bertalian (correspondence) yang disebut dengan byte. Sederhananya, kumpulan bit yang membentuk sebuah informasi disebut dengan byte. Istilah byte juga digunakan sebagai satuan terkecil alamat (address) di mikroprosesor [8].

2.10 ASCII

Satu *byte* dapat dikatakan sebagai sebuah karakter (seperti sebuah huruf, sebuah angka, atau sebuah tanda baca). Tetapi, karena satu *byte* merupakan sekumpulan dari *bit*, maka, kombinasi yang seperti apa dari *bit* yang akan membentuk sebuah *byte* ?. Tentu saja, hal ini memerlukan kesepakatan dari beberapa pengguna (pihak yang terkait).Salah satunya, menghasilkan kesepakatan yang memunculkan kode ASCII (American Standard Code for Information Interchange) yaitu sistem pengkodean yang berbasis pada alpabet Inggris. ASCII disepakati pada tahun 1964 oleh American Standard Assosiation [8].

3. ANALISIS DAN PERANCANGAN

3.1 Subjek Penelitian

Subyek penelitian ini adalah bagaimanamenggabungkan steganografi LSB dan LCG untuk pengamanan data dokumen pada file gambar, dalam sebuah program aplikasi menggunakan bahasa pemrograman Borland Delphi 7.Beberapa bahan penelitian yang akan digunakan dalam penelitian ini seperti, fiile data atau pesan yang akan disisipkan. *File* yang akan dijadikan sebagai bahan penelitian yaitu *file* data atau pesan berformat .doc atau .docx.*File* gambar yang digunakan sebagai media penyisipan data atau pesan. *File* gambar tersebut dapat berformat .bmp. Metode steganografi dalam penyisipan pesan menggunakan metode LSB dan LCG.Keamanan pada saat penyisipan pesan kedalam *file* gambar menggunakan kunci.

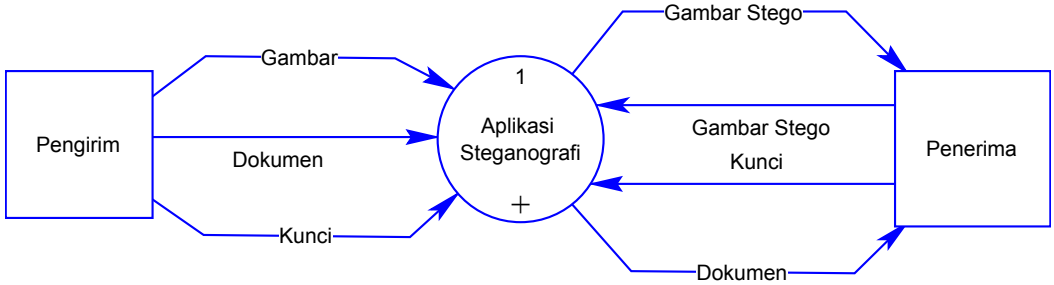
Pertimbangan penelitian ini menggunakan unsur multimedia seperti *file* gambar yang disisipi pesan yaitu agar pesan atau data yang akan disampaikan dapat tersembunyi dengan aman serta dapat terkamuflase dengan *file* gambar tersebut. Hal ini dilakukan agar informasi penting yang akan disampaikan tetap aman dan sukar untuk diketahui pihak yang tidak berkepentingan.

3.2 Perancangan

Perancangan sistem merupakan tahapan dimana mulai dirancangnya suatu perangkat lunak dengan menganalisi beberapa komponen yang diperlukan sistem agar dapat memenuhi fungsionalitas yang diperlukan.

3.2.1 Perancangan Diagram Konteks

Diagram ini adalah diagram level tertinggi dari *Data Flow Diagram* (DFD) yang menggambarkan hubungan sistem dengan lingkungan lainnya. Tahapan ini digunakan untuk menggambarkan seluruh sistem yang akan dibuat, yang nantinya akan diimplementasikan dalam sebuah program aplikasi. Adapun cara pembuatan diagram konteks yaitu menentukan nama sistem, batasan sistem apa saja yang ada dalam sistem dan menentukan apa yang diterima atau diberikan dari atau pada sistem, seperti yg terlihat pada Gambar 3.



Gambar 3. Diagram konteks level 0