Aplikasi Algoritma Kriptografi dan Steganografi untuk Keamanan Informasi Berbasis Teks

Wiji Lestari[1], **Supardi**[2], **Afu Ichsan Pradana**[3]

[1] *Program Studi Sistem Informasi, STMIK Duta Bangsa Surakarta*
[1]wijiles912@gmail.com
[2,3]*Program Studi Teknik Informatika, STMIK Duta Bangsa Surakarta*

ABSTRACT

This study will produce a system of text-based information security applications using cryptography algorithms Hill Code and Steganography LSB (Least Significant Bit). System information security applications are built to be used for text-based data security. The algorithms used for cryptography is Hill Code with a matrix of 2 x 2sebagai encryption keys, whereas the description used for the inverse of a matrix initial key. Steganography algorithm used is the LSB (Least Significant Bit) insertion in every bit of content (confidential data) into a low bit or bits of the far right. As known to a bitmap (.bmp) 24 bits consist of three pixels in which each pixel is a collection of 8 bits or 1 byte (a value between 0 to 255atau in binary format between 00000000 to 11111111), who presented the value of the intensity of the light that forms the base color namely red, green or blue (red-green-Blue or RGB). Thus in each pixel can be inserted 3 content. The results of the implementation and testing of the system shows that the system is running well, the implementation of the algorithm results are consistent with the manual calculation.

Keywords*: Information Security, Cryptography, Steganography, Hill Code, Least Significant Bit*

I. PENDAHULUAN

Keamanan informasi menjadi hal yang sangat penting dalam perkembangan teknolog dan informasi, terutama kerahasiaan informasi terhadap pihak-pihak yang tidak berkaitan. Masalah keamanan sering kurang mendapat perhatian dari perancang dan pengelola informasi (Ariyus, 2008). Semakin banyak informasi yang disimpan, dikelola dan di-*sharing*-kan maka semakin besar pula resiko terjadi kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan (Sharma, et al, 2013). Berbagai langkah ditempuh mulai dari menyandikan pesan sampai menyembunyikan pesan di dalam media lain.

Di bidang keamanan data, istilah kriptografi dan steganografi banyak dikenal. Kriptografi adalah suatu ilmu ataupun seni yang mempelajari bagaimana sebuah data dikonversi ke bentuk tertentu yang sulit untuk dimengerti. Kriptografi bertujuan untuk menjaga kerahasiaan informasi atau data supaya tidak dapat diketahui oleh pihak yang tidak berhak (*unauthorized person*). Sedangkan steganografi menurut Soraireh (2013) adalah seni dan ilmu menyembunyikan informasi dalam dokumen penutup seperti gambar digital, teks, suara, dan video dengan cara menyembunyikan keberadaan data yang disembunyikan dalam data lain.

Pada penelitian ini diaplikasikan algoritma *Hill Code* pada Kriptografi dengan menggunakan matriks 2 x 2 dan algoritma steganografi dengan teknik *Least Significant Bit (LSB)*. *Input* sistem ini berupa teks dan tanpa spasi, *output* menggunakan huruf kapital. Sistem ini berjalan pada sistem *Android* dengan versi minimal 4.4.2 *Jelly Bean.*

II. KAJIAN LITERATUR

A. Penelitian yang Terkait

Penelitian-penelitian yang terkait dengan penelitian ini, Saraireh (2013) melakukan penelitian dengan judul *A Secure Data Communication System Using Cryptography and Steganography*. Pada penelitian mengaplikasikan sistem keamanan data dengan menggabungkan Kriptografi dan Steganografi menggunakan *high level security, scalability* dan *speed* serta menggunakan DWT (*Discrete Wave Transform*) untuk steganografi-nya.

Sharma, et al (2013) melakukan penelitian dengan topik *Secure Image Hiding Algorithm using Cryptography and Steganography*. Pada penelitian ini memadukan sistem keamanan Kriptografi dengan algoritma *Blowfish* dan Steganografi menggunakan algoritma LSB.

Mahajan & Sachdeva (2013) melakukan penelitian dengan judul *A Study of Encryption Algorithms AES, DES and RSA for Security*. Pada penelitian ini dilaksanakan studi penggunaan algoritma AES (*Advance Encryption Standard*) , DES (*Data Encryption Standard*) dan algoritma RSA. Pada penelitian dihasilkan perbandingan kinerja dari tiga algoritma tersebut.

B. Keamanan Sistem Informasi

Keamanan merupakan aspek yang penting untuk sistem informasi. Bermacam cara untuk menjaga sebuah sistem agar kerahasiaan dari informasi tetap terjaga. Pentingnya informasi menyebabkan sering kali informasi hanya boleh diakses oleh pihak-pihak tertentu. Jatuhnya informasi ke tangan pihak lain yang tidak diharapkan dapat menimbulkan kerugian bagi pemilik informasi (Saraireh, 2013).

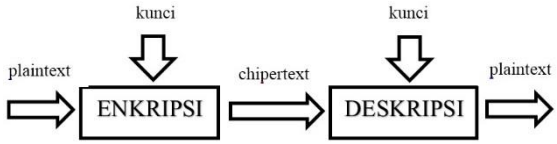
Keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik.

Keamanan sistem informasi dapat diartikan sebagai kebijakan, prosedur, dan pengukuran teknis yang digunakan untuk mencegah akses yang tidak sah, perubahan program, pencurian, atau kerusakan fisik terhadap sistem informasi. Sistem pengamanan terhadap teknologi informasi dapat ditingkatkan dengan menggunakan teknik-teknik dan peralatan-peralatan untuk mengamankan perangkat keras dan lunak komputer, jaringan komunikasi, dan data (Mahajan & Sachdeva, 2013).

C. Algoritma Kriptografi

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berartirahasia dan *graphia* berarti tulisan. Menurut terminologinya, kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain.

Kriptografi adalah suatu studi teknik matematika yang berhubungan dengan aspek keamanan informasi seperi kerahasiaan, integritas data, autentikasi entitas dan autentikasi keaslian data. Kriptografi tidak hanya berarti penyediaan keamanan informasi, melainkan sebuah himpunan teknik-teknik. (Ariyus, 2008).



Gambar 1. Mekanisme Kriptografi

D. Algoritma *Hill Code*

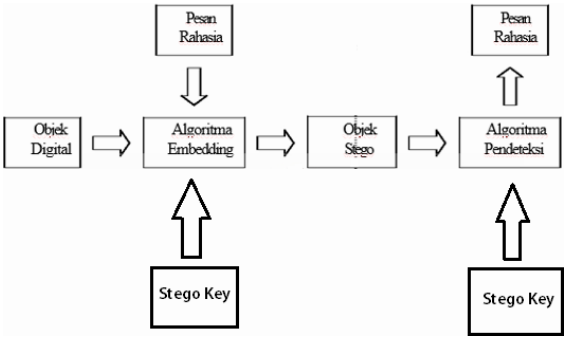
Algoritma *Hill Code* merupakan salah satu sistem kripto polialfabetik yang berarti setiap karakter alfabet bisa dipetakan ke lebih dari satu macam karakter. Kode ini ditemukan pada tahun 1929 oleh Lester S. Hill (Ariyus, 2008). Misalkan m adalah bilangan bulat positif dan $P = C = (Z_{26})^m$. Ide dari kode Hill adalah mengambil m kombinasi linier dari m karakter alfabet dalam satu elemen teks asli sehingga dihasilkan m alfabet karakter dalam satu elemen teks asli.

E. Algoritma Steganografi

Citra merupakan gambar pada bidang dua dimensi yang dihasilkan melalui proses digitasi.

Saat ini peredaran citra di internet sangat banyak sehingga sulit untuk menemukan *file* asli citra tersebut. Untuk menjaga keaslian dari suatu citra, dapat juga menggunakan steganografi. Sehingga steganografi tidak hanya dapat digunakan untuk menyembunyikan pesan atau informasi, tetapi juga dapat digunakan sebagai proteksi hak cipta dan keaslian suatu citra.

Steganografi adalah Metode *Word Mapping* digunakan untuk mengamankan data pesan yang dikirimkan dalam bentuk kalimat yang akan dikirimkan melalui media dengan menggunakan lima tahap dalam perubahan pesannya. (Banerjee, 2011: p98).



Gambar 2. Mekanisme Steganografi

Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari bidang jenis teknik untuk melakukan sebuah tugas dalam mengamankan pesan rahasia dalam sebuah berkas. Sebuah program steganografi dibutuhkan untuk menemukan kelebihan *bits* dalam keamanan *file* yang dapat digunakan untuk mengamankan pesan rahasia di dalamnya, memilih beberapa di antaranya untuk digunakan dalam menyelubungi data dan penyelubungan data dalam *bits* dipilih sebelumnya.

F. *Least Significant Bit* (LSB)

Metode yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda (Stallings, 2011). Contohnya, pada berkas *image* pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data *pixel* yang menyusun *file* tersebut. Pada berkas *bitmap* 24 bit, setiap *pixel* (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (*byte*) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian, pada setiap *pixel* berkas *bitmap* 24 bit kita dapat menyisipkan 3 bit data.

Least significant bit (LSB) merupakan salah satu teknik dalam steganografi. Teknik LSB yaitu menggantikan bit terakhir pada gambar dengan bit yang akan disembunyikan (pesan). Misalkan bit pada gambar dengan ukuran 3 pixel sebagai berikut:

(00111111 11101001 11001000)
(00111111 11001000 11101001)
(11000000 00100111 11101001)

Pesan yang akan disisipkan adalah karakter "A" yang memiliki biner 10000001, *stegoimage* yang akan dihasilkan adalah:

(00111111 11101000 11001000)
(00111110 11001000 11101000)
(11000000 00100111 11101001)

Ada dua teknik yang dapat digunakan pada LSB, yaitu penyisipan secara sekuensial dan secara acak. Penyisipan sekuensial dilakukan berurutan sedangkan penyisipan acak dilakukan dengan memasukan kata kunci (*stego key*).

III. METODOLOGI PENELITIAN

Pada tahapan ini dilaksanakan analisis kebutuhan dan perancangan sistem.

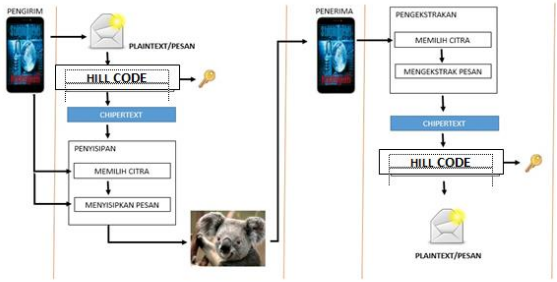
Tabel 1. Kebutuhan Minimum Sistem

Kebutuhan	Keterangan
Sistem Operasi	Windows 7 dan sesudahnya
Prosesor	*Dual Core 2.20 GHz*
Memori	*2 GB DDR2 800 MHz*
Monitor	*Monitor 14 inch (1366X768)*
Smartphone	*Android 4.2.1*
IDE*(Integrated Development Environment)*	Eclipse
Sistem Operasi HP	Minimal versi *Android 4.2.1* (*Jelly Bean*)

Analisis kebutuhan meliputi: kebutuhan perangkat keras dan lunak, kebutuhan konten

Searching dan kebutuhan fungsional dan performa.

Diagram alir penelitian seperti Gambar 3.



Gambar 3. Diagram Alir Penelitian

Pada aplikasi ini menggunakan dua algoritma yang dikombinasikan, yaitu algoritma kriptografi *Hill Code* untuk proses enkripsi pesan dan algoritma steganografi metode *Least significant bit* (LSB) yang akan digunakan untuk menyisipkan pesan yang telah dienkripsi ke dalam citra. Adapun tahapan - tahapan yang dilakukan setiap prosesnya sebagai berikut:

1) **Proses enkripsi dan penyisipan**
   a. Menuliskan pesan yang akan di enkripsi
   b. *Input key* untuk keamanan berupa matriks 2 x 2
   c. Setelah pesan terenkripsi pilih citra yang digunakan sebagai wadah penyisipan
   d. Tombol kirim untuk menyimpan citra yang berisi pesan enkripsi dan memilih media untuk pengiriman citra tersebut.
2) **Proses penguraian dan deskripsi**
   a. Pilih citra yang berisi pesan
   b. *Input key* untuk keamanan berupa *invers* matriks 2 x 2
   c. Pesan akan terdeskripsi dan dapat di baca

IV. IMPLEMENTASI SISTEM

Bagian ini adalah bagian terpenting dalam pembuatan aplikasi keamanan pesan, yaitu bagaimana tahapan *coding* dari aplikasi untuk menerapkan perancangan yang telah dilakukan terhadap sistem. Dalam pembuatan aplikasi terdapat beberapa tahapan dalam *coding* yaitu membuat *project*, membuat desain *interface* beserta *activity*,dan *setting string*.

A. Implementasi *Software* dan *Hardware*

Implementasi sistem pada *software* dan *hardware* bertujuan untuk melihat apakah sistem bisa bekerja dan berjalan dengan baik pada *software* maupun sistem *computer* dan *handphone*.

Gambar 4. Menu Utama

Tahapan terakhir dalam implementasi adalah pengujian aplikasi yang sudah jadi dalam bentuk APK menggunakan *smartphone* Android. Dalam tahap ini ada tiga macam cara pengujian, yang pertama pengujian tampilan aplikasi terhadap *smartphone* Android dan kedua pengujian aplikasi dengan metode *black box*.

B. Implementasi Algoritma Kriptografi dan Steganografi

Implementasi algoritma ini menguji kesesuaian antara perhitungan manual dengan perhitungan dengan sistem. Pada tahapan ini menguji apakah algoritma Kriptografi *Hill Code* dan Algoritma Steganografi LSB berjalan dengan baik.

Tabel 2. Hasil implementasi algoritma

No	Teks Input	Teks Output Manual	Teks Output Sistem	Keterangan
1	Saya	SAYA	SAYA	sesuai
2	Duta	DUTA	DUTA	sesuai
3	Benar	BENAR	BENAR	sesuai
4	Enkripsi	ENKRIPSI	ENKRIPSI	sesuai
5	Teks	TEKS	TEKS	sesuai

V. KESIMPULAN DAN SARAN

A. Kesimpulan

1. Sistem aplikasi keamanan dengan menggunakan Algoritma Kriptografi *Hill Code* dan Algoritma Steganografi LSB dapat digunakan untuk keamanan informasi berbasis teks
2. Pengujian dan implementasi sistem keamanan dengan Algoritma Kriptografi dan Steganografi berjalan dengan baik sesuai dengan analisis dan perancangan.

B. Saran

Perlunya penelitian lanjut dengan membandingkan berbagai algoritma pada Kriptografi dan Steganografi.

REFERENSI

Ariyus, Dono. 2008. *Pengantar Ilmu Kriptografi*, Penerbit Andi Yogyakarta.

Mahajan, P., Sachdeva, A. 2013. *A Study of Algorithms AES, DES and RSA for Security*, Global Journal of Computer Science and TechnologyNetwork, Web & Security, Volume 13, Issue 15, Version 1.0 year 2013, online ISSN: 0975-4172, print ISSN: 0975-4350

Saraireh, S.2013. *A Security Data Communication System using Cryptography and Steganography*, International Journal of Computer Network & Communication (IJCNC), Vol.5, No.3, May 2013

Sharma, H., Arya, M., Goyal, D. 2013. *A Study of Encryption Algorithm using Cryptography and Steganography*, IOSR Journal of Computing Engineering (IOSR-JCE), e-ISSN : 2278-0661, p-ISSN:

Stallings, W.,2011. *Criptography And Network Security*, Principles And Practice, Edisi ke-4.New York: Prentice Hall