METODE PENGAMANAN UNTUK FILE BERTIPE DOKUMEN MENGGUNAKAN KOMBINASI ALGORITMA KRIPTOGRAFI *INTERNATIONAL DATA ENCRYPTION ALGORITHM* (IDEA) DAN STEGANOGRAFI *LEAST SIGNIFICANT BIT (LSB)*

Romario Hendrawan

Jurusan Teknik Informatika-S1, Fakultas Ilmu Komputer

Universitas Dian Nuswantoro Semarang

Jln. Nakula I no 5-17 Semarang 50131 INDONESIA

111201005293@mhs.dinus.ac.id

Pertukaran suatu informasi pada jaman global ini semakin menjadi sebuah kebutuhan vital dalam berbagai aspek kehidupan. Namun terdapat beberapa informasi penting dimana informasi tersebut diminati oleh berbagai pihak yang juga memiliki kepentingan didalamnya. Dalam hal ini masalah keamanan dan kerahasiaan data adalah suatu hal yang sangat penting, maka harus ada perlindungan terhadap data yang kita miliki. Enkripsi merupakan proses penyandian plainteks menjadi cipherteks, teknik enkripsi digunakan sebagai teknik pengamanan data asli yang diubah menjadi data rahasia. Selanjutnya dekripsi merupakan proses mengembalikan cipherteks menjadi plainteks, maka dengan cara ini pesan asli tidak akan terbaca oleh pihak yang tidak berkepentingan. Salah satu teknik untuk mengamankan file yaitu dengan mengimplementasikan kriptografi metode IDEA (*International Data Encryption Algorithm*). Namun penggunaan satu metode masih dapat menimbulkan kecurigaan, untuk melengkapi agar data dapat tersembunyi dengan aman dan tidak tidak menimbulkan kecurigaan. Penggunaan Steganografi LSB (*Least Significant Bit*) akan menjadi kombinasi yang baik. Steganografi *least significant bit* merupakan suatu teknik menyisipkan informasi penting kedalam suatu media seperti image. Dengan menggunakan metode ini maka perubahan yang terjadi tidak menimbulkan kecurigaan karena secara kasat mata tidak menimbulkan perubahan yang besar.

Kata kunci : international data encryption algorithm, least significant bit, kriptografi, steganografi, file dokumen

An exchange of information on the global era is increasingly becoming a vital necessity in many aspects of life. However, there is some important information where the information is in demand by various parties who also have an interest therein. In this case the problem of security and confidentiality of data is a very important thing, then there must be protection of the data we have. Encryption is the process of encoding the plaintext into ciphertext, encryption techniques are used as a security technique that changed the original data into data confidential. Furthermore, decryption is the process of restoring the ciphertext into plaintext, so in this way the original message will not be read by unauthorized parties. One technique

for securing file is to implement cryptographic methods IDEA (International Data Encryption Algorithm). However, the use of the method can still cause suspicion, to supplement that data can be safely concealed and does not arouse suspicion. The use of Steganography LSB (Least Significant Bit) will be a good combination. Least significant bit Steganography is a technique to insert essential information into a medium like image. By using this method, the changes do not arouse suspicion because it is invisible to the eye does not cause large changes.

Keyword : international data encryption algorithm, least significant bit, cryptography, steganography, document file

I. PENDAHULUAN

Dimasa saat ini penggunaan teknologi informasi tidak dapat dihindari lagi karena dengan adanya perkembangan teknologi informasi pengguna mendapatkan kemudahan dalam menemukan informasi yang mereka inginkan dengan cepat dan mudah. Internet sebagai contohnya, memungkinkan penggunanya mendapatkan informasi yang mereka inginkan dengan cepat, salah satunya informasi tersebut dapat berupa file ataupun data. Informasi terdapat dua jenis yaitu informasi rahasia dan informasi yang tidak rahasia. Untuk informasi yang tidak rahasia semua orang dapat membukanya maupun menggunakannya, akan tetapi berbeda dengan informasi yang bersifat rahasia karena tidak semua orang berhak untuk mendapatkan informasi tersebut. Guna untuk melindungi keamanan file rahasia ini, dibutuhkan perlindungan data yang menggunakan sebuah algoritma keamanan data, dan yang sering digunakan adalah kriptografi dan steganografi.[1] Dua algoritma ini memiliki keunggulan dalam hal pengamanan data. Kriptografi dan Steganografi memiliki metode berbeda walaupun dua algoritma ini sama-sama untuk mengamankan data.

Algoritma kriptografi merupakan algoritma yang dapat melakukan pengamanan pada sebuah data yang akan dilindungi. Dalam hal ini data yang ingin dilindungi akan disandikan, guna untuk melindungi kerahasiaan dari suatu data. Contoh nyata kriptografi dalam kehidupan sehari-hari yaitu terdapat pada PIN mesin ATM, password komputer, password ID game Online, dll. Dalam algoritma ini suatu data nantinya akan di enkripsi sehingga bentuk file nantinya tidak dapat dibuka seperti sebelum di enkripsi, penggunaan algoritma kriptografi saat ini sangatlah banyak salah satu contohnya adalah International Data Encryption Algorithm.

IDEA dirancang untuk menggantikan algoritma DES. IDEA sendiri sebenarnya adalah bentuk revisi kecil dari PES (Proposed Encryption Standard). Pada awalnya IDEA disebut sebagai IPES (Improved Proposed Encryption Standard). IPES kemudian dikomersilkan dengan nama IDEA dan dipatenkan[2].

Dengan di kombinasikannya algoritma kriptografi dengan steganografi akan meningkatkan kualitas keamanan data. Penggunaan algoritma steganografi ini banyak menggunakan format digital yang dijadikan sebuah media penyembunyian. Pada dasarnya steganografi adalah ilmu dan seni menyembunyikan pesan rahasia. Steganografi metode EoF(End of File) menggunakan cara dengan menyisipkan data, file hasil enkripsi dari steganografi ini tidak mengalami perubahan signifikan dari segi visual dalam kasat mata[3].

Dari penjabaran diatas maka penelitian ini akan mengimplementasikan kedua metode yaitu kriptografi metode International Data Encryption Algorithm (IDEA) dan steganografi Least Significant Bit (LSB) pada file bertipe dokumen.

II. METODE YANG DIUSULKAN

1.1 Tinjauan Studi

Penelitian yang sudah dilakukan berkaitan dengan steganografi Least Significant Bit dengan mengkombinasikan antara Algoritma Kriptografi Vignere dan RC4 yang dilakukan oleh Basuki Rakhmat dan Muhammad Fairuzabadi, M.kom[1] ini mengintegrasikan kriptografi dan steganografi dalam sebuah sistem aplikasi. Pesan teks terlindungi dengan algoritma kriptografi dan tersembunyi dalam sebuah gambar.

Kholidya Yuli Wardani, M.Zen, S.Hadi, ST. MSc, Mike Yuliana, ST.MT[2] meneliti tentang algoritma IDEA yang menerima masukan berupa 64-bit plaintext dan 128-bit kunci, dan menggunakan subkey 16-bit. Keduanya sama-sama beroperasi dalam 64-bit block, yang terdiri dari 8 putaran identik dan sebuah output transformasi. IDEA memiliki fungsi enkripsi yang kuat dan aman.

Adira[4] meneliti tentang Analisis dan Perancangan Aplikasi Steganografi pada Citra Digital Menggunakan Metode Least Significant Bit (LSB) yang menunjukkan hasil bahwa kualitas image tetap terjaga walaupun image sudah disisipi pesan, namun ukuran file akan lebih besar.

Aditya, y. Pratama, A. , & Nurlifa, A[5] melakukan penelitian tentang Studi Pustaka Untuk Steganografi dengan beberapa metode, mendapatkan hasil bahwa jika dilihat berdasarkan ukuran stego image LSB lebih baik karena tidak mengubah ukuran file yang disisipi.

Penelitian yang telah dilakukan oleh Brian Al Bahr[7], mengenai International Data Encrypted Algorithm, berpendapat bahwa algoritma ini (IDEA) menyediakan keamanan yang cukup tinggi yang tidak didasarkan atas kerahasiaan algoritmanya akan tetapi lebih ditekankan pada keamanan/kerahasian kunci yang digunakan.

1.2 Algoritma International Data Encryption Algorithm (IDEA)

IDEA merupakan salah satu algoritma simetris yang beroperasi pada sebuah blok pesan terbuka 64bit, menggunakan kunci 128bit untuk proses enkripsi dan dekripsi. Keluaran dari algoritma ini adalah blok pesan terenkripsi 64bit. Proses dekripsi menggunakan blok penyandian (algoritma) yang sama dengan proses enkripsi dimana kunci dekripsinya diturunkan dari kunci enkripsi. IDEA menggunakan proses iterasi yang terdiri dari 8 putaran dan 1 transformasi keluaran pada putaran ke8,5. Dimana setiap 1 iterasi terdapat 14 langkah perhitungan yang dirangkum sebagai berikut:

1) Perkalian X1 dengan Z11
2) Penjumlahan X2 dengan Z21
3) Pejumlahan X3 dengan Z 31
4) Perkalian X4 dengan Z41
5) Operasi XOR hasil langkah 1) dan 3)
6) Operasi XOR hasil angkah 2) dan 4)
7) Perkalian hasil langkah 5) dengan Z51
8) Penjumlahan hasil langkah6) dengan langkah7)
9) Perkalian hasil langkah 8) dengan Z61
10) Penjumlahan hasil langah 7) dengan 9)
11) Operasi XOR hasil langkah 1) dan 9)
12) Operasi XOR hasil langkah 3) dan 9)
13) Operasi XOR hasil langkah 2) dan 10)
14) Operasi XOR hasil langkah 4) dan 10)

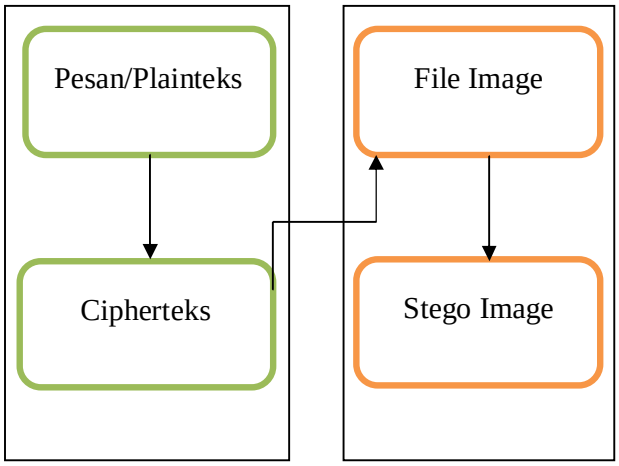
1.3 Metoe Least Significant Bit (LSB)

Metode Least Significant Bit (LSB) merupakan salah satu dari beberapa jenis metode steganografi dan akan diterangkan pada pembahasan berikut. Bit atau binary digit adalah unit dasar penyimpanan data di dalam komputer, nilai bit suatu data adalah 0 atau 1. Semua data yang ada pada komputer disimpan ke dalam satuan bit ini, dan dimasukkan ke suatu media digital yaitu gambar, suara, ataupun video. Jenis-jenis format pewarnaan di dalam media gambar, seperti grayscale, RGB, dan CMY. Sebagai contoh pewarnaan monochrome bitmap (menggunakan 1 bit 2 untuk tiap pixelnya), RGB - 24 bit (8 bit untuk Red, 8 bit untuk Green, dan 8 bit untuk Blue), Grayscale-8 bit (menentukan tingkat kehitaman suatu pixel berdasarkan nilai bitnya [8].

Metode yang akan digunakan untuk menyembunyikan pesan pada media digital dapat dijelaskan sebagai berikut. Pada file image, pesan dapat disembunyikan dengan menggunakan cara menyisipkan pada bit terendah atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut. Seperti kita ketahui untuk file bitmap 24 bit maka setiap pixel pada gambar terdiri dari tiga warna susunan yaitu merah, hijau, biru yang masing-masing disusun dengan bilangan 8 bit.

1.4 Prosedur Pengenkripsian dan Pendekripsian

1. Prosedur pengenkripsian dengan metode *International Data Encryption Algorithm* (IDEA) dan *Least Significant Bit* (LSB)



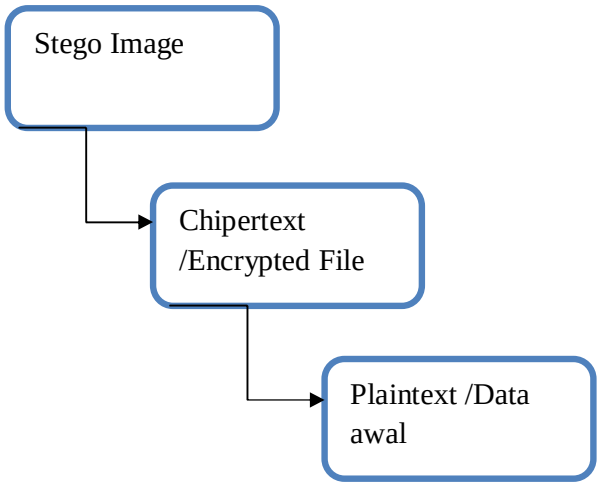
Proses Kriptografi Proses Steganografi

Gambar 3.1 Prosedur Pengenkripsian dan Stego

Berdasarkan gambar diatas, proses enkripsi dan penyisipan menggunakan International Data Encrypted Algorithm (IDEA) dan Least Significant Bit (LSB). Adapaun langkah-langkahnya akan dijelaskan sebagai berikut :

1. Lakukan pengenkripsian data/plainteks dengan menggunakan metode International Data Encrypted Algorithm (IDEA) untuk mendapatkan chiperteks/Encrypted file.
2. Pilih file image yang akan digunakan sebagai wadah untuk menampung pesan yang sudah dienkripsi/cipherteks.
3. Lakukan penyisipan cipherteks/Encrypted file menggunakan metode Least Significant Bit (LSB)

2. Prosedur pendekripsian dengan metode *International Data Encryption Algorithm* (IDEA) dan *Least Significant Bit* (LSB)



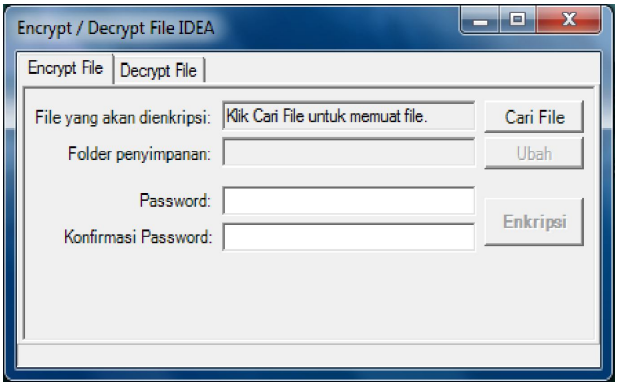
Gambar 3.2 Prosedur Pendekripsian dan Unstego

Dari gambar diatas dapat dijelaskan bahwa proses Unstego dan Dekripsi menggunakan International Data Encrypted Algorithm (IDEA) dan Least Significant Bit (LSB). Adapun langkah-langkahnya akan dijelaskan sebagai berikut :

1. Lakukan proses unstego pada file Stego-Image untuk mendapatkan encrypted file.
2. Dekripsikan kembali encrypted file yang sudah didapat untuk mendapatkan pesan/plainteks.

III. IMPLEMENTASI

Hasil pemodelan perangkat lunak dapat dilihat pada gambar berikut ini.



Gambar 4. 1 Tampilan awal proses enkripsi

a. Proses Enkripsi

Dalam tahap ini file dokumen akan menjadi sebuah *plaintext* dan akan diberikan sebuah password. File yang telah di enkripsi akan berubah menjadi file bertipe ".encrypt" dan merupakan *ciphertext*.

b. Proses Dekripsi
Pilih file yang akan didekripsi, pilih *Decrypt File*, setelah didapatkan ciphertext kemudian klik tombol Dekripsi. Maka didapatkan pesan rahasia/*plaintext* awal. File yang telah di dekripsi akan berubah menjadi normal kembali sesuai dengan format awal file dan menjadi bisa dibuka kembali atau dapat digunakan normal.

IV. HASIL DAN PEMBAHASAN

Peneliti melakukan pengujian sebanyak 15 kali dengan 3 jenis file yang berbeda (txt, docx, pdf), membuktikan bahwa pengamanan dengan menggunakan kombinasi dua algoritma *International Data Encryption Algorithm* (IDEA) dan *Least Significant Bit* (LSB) terbukti aman dan tidak dapat dibedakan secara kasat mata.

V. PENUTUP

5.1 Kesimpulan

Dari hasil perancangan dan pembuatan program aplikasi kriptografi dengan algoritma International Data Encryption Algorithm (IDEA) dan steganografi Least Significant Bit (LSB) ini, dapat diambil kesimpulan sebagai berikut:
1. Dari hasil yang telah dilakukan membuktikan bahwa file yang telah dienkripsi tidak dapat dibuka secara normal.
2. Hasil percobaan selanjutnya dengan menyisipkan file ke dalam gambar tidak mengubah kualitas gambar.
3. File dapat terlindungi dengan aman dan tidak rusak, dengan catatan tidak dilakukan pengeditan.
4. Dengan menggunakan 2 metode ini tidak akan menimbulkan kecurigaan terhadap pihak-pihak yang tidak berhak untuk membuka isi pesan.Dari hasil perancangan dan pembuatan program aplikasi kriptografi dengan penggabungan

5.2 Saran

Saran-saran yang berguna untuk pengembangan sistem dan aplikasi ini adalah sebagai berikut:
1. Dalam melakukan penyisipan pesan diharapkan untuk menyesuaikan ukuran gambar yang akan digunakan nantinya.
2. Aplikasi pengamanan data ini dapat diterapkan di instansi yang memiliki beberapa dokumen yang harus dijaga.

REFERENCES

[1] Basuki Rahmat, Muhammad Fairuzabadi, M.Kom, *Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenere dan RC4*. Yogyakarta: Univeraitas PGRI Yogyakata, 2010.

[2] Kolidya Yuli Wardani, M.Zen S.Hadi, ST. MSc, Mike Yuliana, ST.MT, *Implementasi Metode Kriptografi IDEA pada Priority Dealer untuk Layanan Pemesanan dan Laporan Penjualan Hanphone Berbasis Web* . Surabaya: ITS.

[3] Ema dan Sukrisno Utami, Implementasi Steganografi EoF dengan Gabungan Enkripsi Rijndael, Shift Cipher dan Fungsi Hash. Yogyakarta, 2007.

[4] Adira, Analisis Dan Perancanga Aplikasi Steganografi pada Citra Digital Menggunakan Metode Least Significant Bit(LSB). UIN, 2010.

[5] Yogie Aditya, Andika Pratama, Alfian Nurlifa , Studi Pustaka Untuk Steganografi Dengan Beberapa Metode . Yogyakarta: UII, 2010.

[6] Nurhayati, Dwi, Oky, ST, MT (2010). Keamanan Multimedia. Universitas Diponegoro.

[7] Brian Al Bhar, International Data Encryption Algorithm. Bandung:Institut Teknologi Bandung,2010.

[8] Basuki, Kurni, Dwi., S.Si., M.kom. , & Maulana, M. , Ahmad. , & N. , Uzzin, Isbat. , S.kom.(2009) Data Hiding Steganograph Pada File Image Menggunakan Metode Least Significant Bit. Industrial Electronic Seminar. , ITS Surabaya.

[9] Abdul Hanan, Metode Enkripsi dan Dekripsi Data Menggunakan Kriptografi IDEA. Banda Aceh, 2013.