KOMBINASI KRIPTOGRAFI *CAESAR CIPHER* DAN STEGANOGRAFI *LEAST SIGNIFICANT BIT* (LSB) PADA CITRA BERFORMAT BITMAP

Sonny Christian Budianto[1], Bowo Nurhadiyono[2]
Universitas Dian Nuswantor, Ilmu Komputer, Teknik Informatika
JL. Imam Bonjol 205, Semarang, Jawa Tengah, 50131, (024) 3517261
E-mail : sonnychristian91@gmail.com[1], masowo68@gmail.com[2]

Abstrak

Perkembangan teknologi informasi saat ini sangat membantu manusia dalam bertukar informasi dalam bentuk file. Diantaranya file tersebut bersifat rahasia dan sangat penting sehingga tidak boleh diketahui oleh pihak lain. Adapun cara untuk menjaga keamanan data atau pesan rahasia yang sudah dilakukan sejak dulu yaitu tehnik kriptografi. Dalam penelitian ini tehnik penyembuyian data menggunakan kombinasi antara tehnik kriptografi dan steganografi. Tehnik kriptografi yang digunakan adalah Caesar Cipher dan untuk tehnik steganografinya menggunakan metode Least Significant Bit (LSB). Untuk penulisan tugas akhir ini penulis memfokuskan hanya pada penyembuyian teks pesan pada gambar. Metode Caesar Cipher dipilih karena dalam pengimplementasiannya sangat mudah dan untuk kunci yang digunakan pergeseran dapat ditentukan oleh pengirim dan penerima pesan.

Kata Kunci: *Caesar Cipher,LSB,Citra,Teks*

Abstract

The development of information technology today is a very helpful man in exchanging information in the form of a file. Among the files are confidential and very important so as not to be known by others. As for how to maintain the security of confidential data or messages that have been done long ago that cryptographic techniques. In this research technique hiding data using a combination of cryptography and steganography techniques. Cryptographic technique used is the Caesar Cipher and for steganography techniques using Least Significant Bit (LSB) . For this thesis the author focuses only on hiding message text on the image. Methods Caesar Cipher been very easy in its implementation and to use the shift key may be specified by the sender and the recipient.

.

Keywords: *Caesar Cipher,LSB,Image,Text*

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini sangat membantu manusia dalam melakukan aktivitasnya. Termasuk dalam bertukar informasi dalam bentuk *file* menjadi hal yang biasa di era komputerisasi saat ini. Banyak diantaranya *file* tersebut bersifat rahasia dan sangat penting sehingga tidak boleh diketahui oleh pihak lain. Seiring dengan perkembangan teknologi informasi tersebut, semakin berkembang pula kejahatan yang berupa pencurian data oleh pihak yang tidak memiliki wewenang atas data atau file tersebut. Oleh karena itu, pada saat ini telah dilakukan berbagai upaya untuk menjaga keamanan data dan mengatasi serangan-serangan tersebut. [1].

Adapun cara untuk menjaga keamanan data atau pesan rahasia yang sudah dilakukan sejak jaman Yunani kuno yaitu dengan menggunakan tehnik kriptografi. Dengan kriptografi data atau pesan rahasia dapat terjaga keamanannya, namun tehnik ini mudah terdeteksi oleh pihak ketiga karena pesan yang yang dikirim telah berbentuk acak, sehingga menimbulkan kecurigaan pihak lain. Untuk itu diterapkan tehnik lain untuk meningkatkan keamanan data tersebut yaitu dengan tehnik *steganography* yang dalam bahasa Yunani berarti pesan tersembunyi. *Steganography* merupakan salah satu tehnik untuk menyembunyikan suatu pesan atau data rahasia dalam wadah (media) digital. Pada *steganography* data atau pesan rahasia disamarkan dalam bentuk yang relatif aman sehingga tidak menimbulkan kecurigaan pihak lain. *Steganography* dapat diterapkan dalam berbagai macam bentuk data, yaitu image, audio, dan video [2].

2. METODE YANG DIUSULKAN

2.1 Tinjauan Pustaka

Tabel1. Penelitian Terdahulu

No	Nama Peneliti	Judul
1	Mukharrom Edisuryana, R.Rizal I, Maman S	Aplikasi Steganografi pada Citra berformat Bitmap
2	Budi Prasetiyo	Kombinasi Steganografi Bit Matching dan Kriptografi DES untuk Pengamanan Data

Dalam penelitian diatas peneliti mengaplikasikan tehnik kriptografi dan steganografi pada citra. Peneliti menggunakan metode-metode kriptografi dan steganografi yang sudah ada.

2.2 Kriptografi

Kriptografi (*chryptography*) berasal dari dua kata dalam Bahasa Yunani, yaitu "*cryptos*" yang berarti rahasia, dan "*graphein*" yang berarti tulisan. Jadi, kriptografi dapat diartikan sebagai tulisan rahasia.

Secara umum, kriptografi terdiri dua proses utama, yaitu enkripsi dan dekripsi. Proses enkripsi akan mengubah pesan asli (plainteks) menjadi pesan terenkripsi dengan menggunakan algoritma dan kunci tertentu yang tidak dapat dibaca secara langsung (cipherteks). Proses dekripsi merupakan kebalikan dari proses enkripsi, yaitu proses untuk memperoleh kembali plainteks dari cipherteks menggunakan kunci dan algoritma tertentu [7]. Contoh penggunaan metode Caesar Cipher dalam mengacak pesan asli:

Pesan asli (plaintext):

"we will meet at mid night"

Dengan kunci 11, Berarti dari kalimat diatas kita konversikan menjadi angka

dari setiap huruf menjadi sebagai berikut:

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19

Cara mendapatkan pesan acak (ciphertext) dengan kunci 11 yaitu dengan menambahkan setiap nilai dari pesan asli (plaintext) dengan kunci 11 maka akan didapatkan:

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4

Jika lebih dari 20 setelah ditambah dengan kunci maka akan dikurangi dengan 26 seperti 22 + 11 = 33 – 26 = 7. Setelah diubah menjadi huruf akan mendapatkan pesan tersandi (ciphertext):

"H P H T W W X P P E L E X T O Y T R S E"

2.3 Steganografi

Steganografi *(steganography)* adalah tehnik menyembunyikan data rahasia didalam wadah (media) digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara (audio), teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara , teks, atau video [1]. Ada dua proses utama dalam steganografi digital yaitu penyisipan (*insertion/embeding*) dan ekstraksi (*extraction/decoding*) pesan. Pesan (*embed*) dapat berupa *plaintext*, *ciphertext*, citra, atau apapun yang dapat ditempelkan ke dalam *bit-stream*. *Embedding* merupakan proses menyisipkan *embed* ke dalam berkas yang masih asli yang belum dimodifikasi, yang disebut media *cover* (*cover object*). Kemudian *media cover* dan *embed* yang ditempelkan membuat media stego (*stego object*). *Extraction* adalah proses menguraikan pesan yang tersembunyi dalam media stego. Ringkasnya, steganografi adalah teknik menanamkan *embed message* pada suatu *cover object*, dimana hasilnya berupa *stego object.*

2.3.1 Least Significant Bit

Teknik steganografi dengan menggunakan metode *Least Significant Bit* (LSB) adalah tehnik yang paling sederhana dan mudah untuk diimplementasikan. Metode ini menggunakan citra digital sebagai cover objectnya. Pada susunan bit didalam sebuah byte (1 byte = 8bit), ada bit yang paling berarti *Most Significant Bit* (MSB) dan bit yang paling kurang berarti yaitu *Least Significant Bit* (LSB). Sebagai contoh byte 11010010, angka bit 1 (pertama yang digaris-bawahi) adalah bit MSB dan angka bit 0 (terakhir yang digaris-bawahi) adalah bit LSB. Misalkan segmen piksel-piksel citra gambar yang sudah dikonversikan ke biner sebelum disisipi pesan adalah:

00110011 10100010 11100010
10101011 00100110 10010110
11001001 11111001 10001000
10100011

Pesan rahasia yang telah dikonversi kedalam biner misalkan '1110010111', maka setiap bit dari pesan tersebut menggantikan posisi LSB dari segemen piksel-piksel citra menjadi (digaris bawahi):

00110011 10100001 11100011
10101010 00100110 10010111
11001000 11111001 10001001
10100011

2.4 Citra Digital

Citra digital adalah gambar dua dimensi yang dapat ditampilkan pada layar monitor komputer sebagai himpunan berhingga (*diskrit*) nilai digital yang disebut *pixel* (*picture*

elemen). Citra digital tersusun dalam bentuk raster (*grid* atau kisi). Setiap kotak yang terbentuk disebut *pixel* (*picture element*) dan memiliki koordinat (x,y). *Pixel* merupakan suatu elemen citra yang memiliki nilai yang menujukkan intensitas warna [9]. Citra digital dapat didefenisikan sebagai Fungsi dua variabel f(*x*,*y*), dimana *x* dan *y* adalah koordinat spasial dan nilai f(*x*,*y*) merupakan intensitas citra suatu titik. Piksel(0,0) terletak pada sudut kiri atas pada citra, indeks *x* begerak ke kanan dan indeks *y* bergerak ke bawah. Konvensi ini dipakai merujuk pada cara penulisan larik yang digunakan dalam pemrograman komputer.

Citra digital dapat dibagi menjadi 3 macam berdasarkan warna-warna penyusunnya :

1. Citra biner (*monochrome*), atau disebut juga *binary image*, yaitu citra yang setiap pikselnya hanya memiliki kemungkinan dua warna.
2. Citra *grayscale* (citra keabuan), citra ini terdiri atas warna abu-abu. Setiap piksel citra grayscale merepresentasikan derajat keabuan atau intensitas warna putih.
3. Citra berwarna (true color), yaitu citra yang nilai pikselnya merepresentasikan warna tertentu. Setiap piksel pada citra berwarna memiliki warna yang merupakan kombinasi dari tiga warna dasar *red green* dan *blue.*

2.4.1 Format Data Bitmap

Pada format bitmap, citra disimpan sebagai suatu matriks dimana masing-masing elemennya digunakan untuk menyimpan informasi warna untuk setiap piksel. Jumlah warna yang dapat disimpan ditentukan dengan satuan *bit*-per-piksel. Semakin besar ukuran bit-per-piksel dari suatu bitmap, semakin banyak pula jumlah warna yang dapat disimpan. Format bitmap ini sangat cocok digunakan untuk menyimpan citra seperti foto, lukisan, dan frame video karena memiliki banyak variasi dalam bentuk dan warna.

Pada citra bitmap jumlah warna yang dapat disimpan ditentukan oleh banyaknya bit yang digunakan untuk menyimpan setiap titik dari bitmap yang menggunakan satuan bpp (*bit* per piksel). Dalam *Windows* dikenal bitmap dengan 1, 8, 16, dan 24 *bit* per piksel. Jumlah warna maksimum yang dapat disimpan dalam suatu bitmap adalah sebanyak 2^n, dimana n adalah banyaknya bit yang digunakan untuk menyimpan satu titik dari bitmap.

Citra bitmap memiliki kelebihan untuk memanipulasi warna, tetapi untuk mengubah objek lebih sulit. Tampilan bitmap mampu menunjukkan kehalusan gradiasi bayangan dan warna dari sebuah gambar. Oleh karena itu, bitmap merupakan media elektronik yang paling tepat untuk gambar-gambar dengan perpaduan gradasi warna yang rumit seperti, foto, kamera digital, video capture, dan lain-lain.

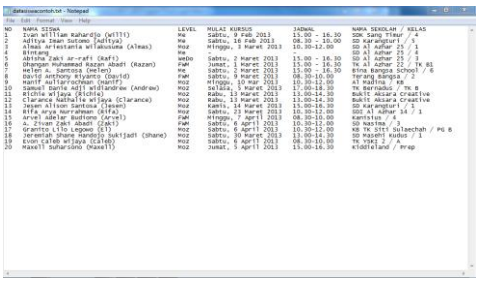
3. HASIL DAN PEMBAHASAN

3.1 Proses Enkripsi dan Penyisipan

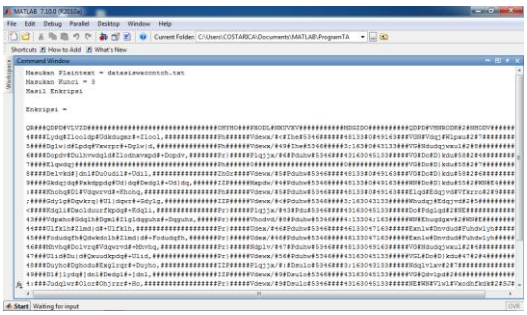
Proses ini *plaintext* atau data dilakukan enkripsi dan disisipkan kedalam citra bitmap.

Berikut tampilannya :

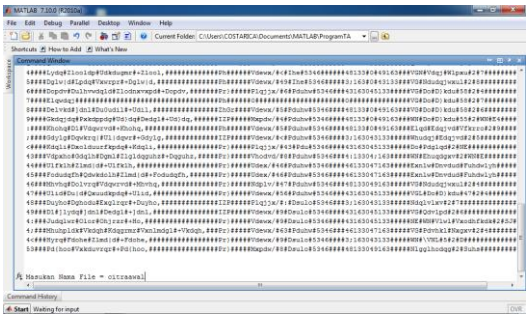
Gambar 1. *Plaintext* atau data



Gambar 2. Hasil Enkripsi *Plaintext* atau data

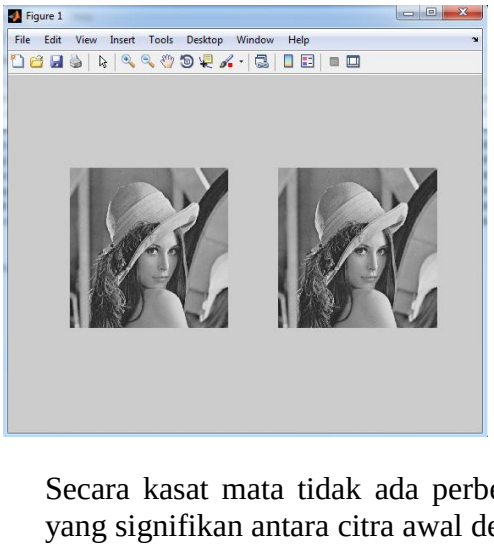


Gambar 3. Proses input citra sebagai *Cover Object*



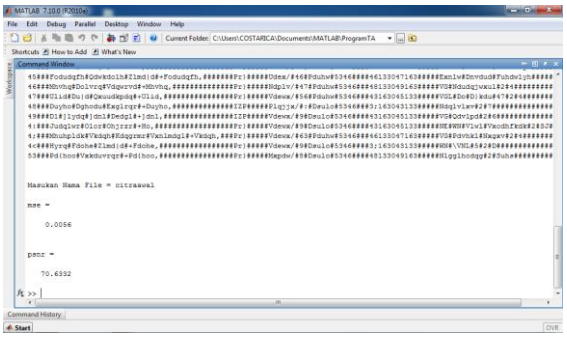
Setelah memasukan file citra sebagai *cover object*, hasil dari penyisipan *ciphertext* kedalam *cover object* adalah citra baru yang diberi nama *CitraStego*.

Gambar 4. Hasil Citra Stego



Secara kasat mata tidak ada perbedaan yang signifikan antara citra awal dengan citra yang sudah disisipi pesan, hal ini di buktikan dengan pengujian perhitungan menggunakan *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR).

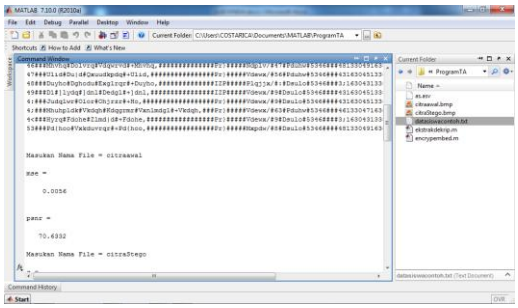
Gambar 5. Hasil Perhitungan *MSE* dan *PSNR*



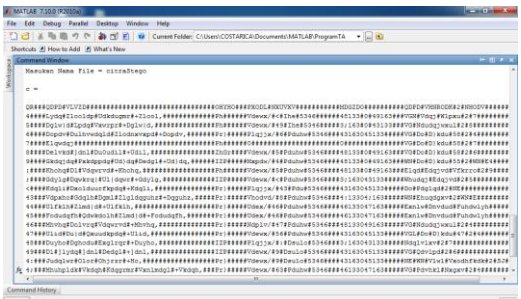
3.2 Proses Ekstraksi dan Dekripsi

Proses ini adalah proses dimana CitraStego dilakukan ekstraksi atau pengambilan ciphertext didalam citra. Setelah proses ekstraksi selesai, ciphertext didekripsi agar pesan asli dapat terbaca kembali.

Gambar 6. Input CitraStego yang akan diekstraksi

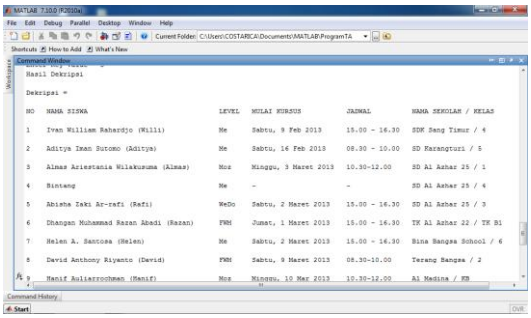


Gambar 7. Hasil Ekstraksi



Setelah didapatkan *ciphertext* didalam citrastego kemudian *ciphertext* harus dilakukan dekripsi menggunakan kunci yang sama ketika proses enkripsi agar pesan dapat terbaca kembali.

Gambar 8. Hasil Dekripsi *Ciphertext*



4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

1. Pada tahap Enkripsi dengan metode *Caesar Chiper* perlu diperhatikan karakter pesan dan karakter pengganti spasi agar tidak saling tumpang tindih.
2. Dari pengujian menggunakan perhitungan MSE dan PSNR citra awal dengan citra yang sudah disisipi , citra stego bisa dikatakan baik karena pesan didalamnya tidak hancur dan citra tidak mengalami perubahan yang signifikan.
3. Dari pengujian di atas dapat disimpulkan bahwa citra awal atau original dengan citra yang sudah disisipi pesan secara kasat mata tidak ada perbedaan yang mencolok.

4.2 Saran

1. Untuk penelitian selanjutnya dapat dilakukan dengan menggunakan citra berwarna (RGB).
2. Proses penyisipan dapat dilakukan dengan memilih piksel secara acak.

DAFTAR PUSTAKA

[1] Munir, Rinaldi., (2004), Pengolahan Citra Digital Dengan Pendekatan Algoritmik". Bandung: Penerbit Informatika.

[2] Munir, Rinaldi., (2006). "Kriptografi". Bandung : Penerbit Informatika.

[3] Mukharrom Edisuryana, R. Rizal Isnanto, and Maman Somantri, "*Aplikasi Steganografi Pada Citra Berformat Bitmap dengan Menggunakan Metode End Of File",* Jurusan Tehnik Elektro Universitas Diponegoro, Semarang, *TRANSIENT, VOL.2, NO. 3, SEPTEMBER 2013*

[4] Budi, Prasetyo, *Kombinasi Steganografi Bit Matching dan Kriptografi DES untuk Pengamanan Data,* Tesis S-2 Program Studi Magister Sistem Informasi, Universitas Diponegoro, Semarang.

[5] Tri, Cahyadi, *Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher pada Citra JPEG,* Jurusan Tehnik Elektro Universitas Diponegoro, Semarang. *TRANSIENT, VOL 1, NO 5, DESEMBER 2012, ISSN : 2302-9927, 282*

[6] Wandani, H, *Implementasi Sistem Keamanan Data dengan Menggunakan Tehnik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem,* Skripsi S-1, Universitas Diponegoro, Semarang

[7] Ariyus, Dony. 2009. Keamanan Multimedia. Andy Publisher

[8] Hidayatno, A, *Steganografi dan Watermarking – Pengolahan Citra Digital,* Tehnik Elektro Universitas Diponegoro, Semarang.