KOMBINASI STEGANOGRAFI LSB DAN KRIPTOGRAFI CEASAR CHIPER UNTUK PENGAMANAN DATA PADA MEDIA CITRA DIGITAL

Samy Yeverson Doo[1], Jodi S. A Zacharias[2], Yunita Sari Tanggela[3]

[1,2,3] Jurusan Teknik Elektro, Fakultas Sains dan Teknik, ,Universitas Nusa Cendana
[1)]Email: samyeverson@staf.undana.ac.id
[2)]Email: jodyzacharias@gmail.com
[3)]Email: sari_tanggela@gmail.com

ABSTRAK

Ada begitu banyak cara untuk mengamankan sebuah data atau informasi. Beberapa diantaranya menggunakan steganografi sementara lainnya menggunakan teknik kriptografi. Pada penelitian ini, digunakan kombinasi kedua cara tersebut untuk meningkatkan tingkat keamanan data. Pertama, data atau informasi tersebut diproses dengan teknik kriptografi yang disebut dengan Caesar Cipher. Kemudian setiap karakter dari data tersebut disembunyikan didalam image dengan metode LSB. Hasilnya menunjukan bahwa saat penyisipan digunakan bit ke 4 sampe bit ke 8 maka kualitas dari image akan menjadi buruk karena MSE menunjukan angka 47,508 sementara PSNR-nya berkisar pada angka 30 sampai 36 dB. Hasil terbaik didapat bila dipakai sampai dengan 3 bit terakhir dari setiap pixel image RGB.

ABSTRACT

There are so many methods to secure the data or information. Some of those are based on steganography and the others are protected by cryptography technique. In this research, we use both ways to increase the security level. First, the data are processing by cryptography technique called Caesar Cipher in order to change an information that we want to protected become a Cipher text. Then each character of that text is concealed within an image LSB method. To evaluate the quality of the image, two parameters which are MSE and PSNR are involved. The result shows that when we use LSB from 4th bit to 8th bit, quality of the image is poor because MSE shows number of 47,508 while the value of PSNR are between 30 to 36 dB.

Keywords : Cryptography, Steganography, Ceasar Cipher, LSB

1. PENDAHULUAN

Seiring perkembangan zaman, kebutuhan manusia akan informasi semakin meningkat. Ditengah-tengah perkembangan teknologi informasi yang kian semarak, internet tidak lagi menjamin penyediaan informasi yang aman. Mengatasi hal tersebut berbagai cara untuk meningkatkan keamanan data terus dikembangkan, diantaranya kriptografi dan steganografi.

Steganografi adalah seni dan ilmu menyembunyikan data pada media lain sebagai *cover* sehingga terlihat samar. Kriptografi adalah seni dan ilmu menjaga kerahasiaan data. Pada kriptografi, data asli diubah menjadi bentuk lain yang tidak dapat dibaca. Penggabungan steganografi dan kriptografi secara bersamaan dapat meningkatkan pengamanan data.

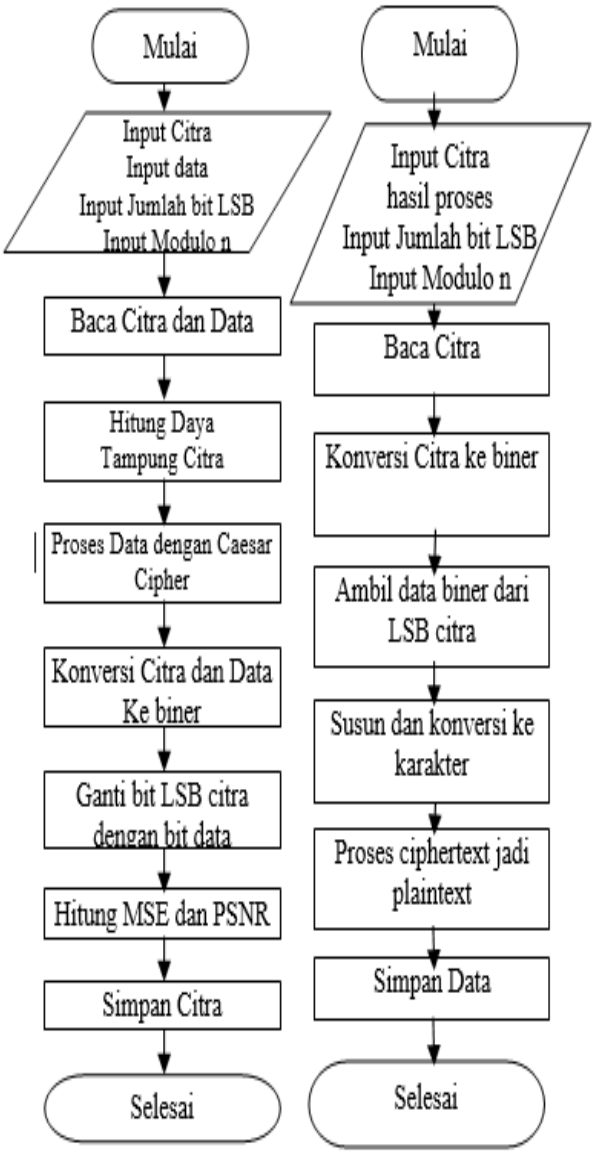
Metode penggabungan steganografi dan kriptografi banyak dikembangkan. Pada umunya teknik yang digunakan yaitu dengan mengenkripsi peasn terlebih dahulu, kemudian menyisipkannya media *cover.* Namun, proses penyisipan dapat berpengaruh pada kualitas media *cover* tersebut.

Upaya untuk meminimalisir perubahan kualitas *cover* dapat dilakukan dengan penyisipan pada bit terakhir (steganografi *Least Significant Bit).* Perubahan kualitas *cover* tidak tampak kasat mata. Teknik ini dilakukan dengan mencocokan bit pesan pada *cover,* kemudian diubah dengan proses enkripsi (kriptografi *Caesar Chiper*).

2. METODE PENELITIAN

Pada penelitian ini dipakai 4 buah gambar berformat .bmp dengan resolusi 24 bit. Ukuran ke 4 gambar tersebut berbeda satu sama lain dengan besar dimensi pixel x pixel filenya sebesar 250x110 (menangis bmp), 256 x 143 (buncit .bmp), 243 x 182 (intan.bmp) dan 300 x 225 (bunga.bmp). Besar ukuran dimensi gambar pixel x pixel kemudian dihitung maksimum daya tampung dari file tersebut sesuai dengan jumlah bit LSB yang

mau dipakai. Jika dipakai 1 bit setiap komponen RGB maka ada 3 bit setiap pixel yang bisa dipakai. Jika dipakai gambar menangis.bmp maka daya tampung file tersebut sebesar (3x250x110)/8 = 10312 karakter. Total karakter tersebut akan disimulasikan pada setiap file sesuai dengan maksimum daya tampungnya. Awalnya data akan dilakukan proses kriptografi untuk mengacak data. Pada proses kriptografi dengan Caesar Cipher,



Gambar 1.(a) Proses Enkripsi dan (b) Proses Dekripsi

disimulasikan dengan modulo 1 sampai 4. Selanjutnya proses penyisipan ke gambar dengan teknik LSB. Hasilnya akan diproses dengan menghitung nilai MSE dan PSNR-nya. Disamping itu juga dilihat secara *Human Visual System* (HVS). Data dalam citra kemudian diextract kembali apakah sesuai atau tidak.

Bagaimana citra diproses untuk dapat menampung data dijelaskan dalam bentuk *flow chart* pada gambar 1.

Pengukuran kualitas citra hasil steganografi dilakukan dengan menggunakan *Peak Signal-to-Noise* Ratio (PSNR) ntuk mengevaluasi perbedaan antara citra hasil dan citra original. Untuk mendapatkan nilai PSNR dicari terlbih dahulu nilai Mean Square Error dari citra yang diuji. Mean Square Error (MSE) adalah tingkat kesalahan piksel-piksel citra hasil pemrosesan sinyal terhadap citra original. Untuk lebar dan tinggi citra original adalah m dan n, di mana I adalah citra original dan K adalah citra hasil, maka persamaan MSE ditunjukkan oleh persamaan :

$$MSE = \frac{1}{3mn}\sum_{l=1}^{3}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j)-K(i,j)\right]^2 \quad \text{.....(1)}$$

Peak Signal to Noise Ratio (PSNR) merupakan nilai (rasio) yang menunjukan tingkat toleransi *noise* tertentu terhadap banyaknya noise pada suatu piksel citra. *Noise* adalah kerusakan piksel pada bagian tertentu dalam sebuah citra sehingga mengurangi kualitas piksel tersebut. Dengan kata lain PSNR merupakan suatu nilai yang menunjukkan kualitas suatu piksel citra. Persamaan untuk PSNR ditunjukkan oleh persamaan :

$$PSNR = 20 * \log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \quad \text{.....(2)}$$

Nilai maksimum dari piksel dalam citra adalah 255. PSNR yang lebih tinggi menunjukkan bahwa kualitas citra hasil lebih baik dan hampir sama dengan citra originalnya.

Pengujian hasil kriptografi dilakukan dengan melihat perbedaan antara plaintext dengan ciphertext dari pesan yang akan disisipkan. Seluruh proses penyisipan maupun ekstraksi atau pengambilan data kembali dilakukan secara otomatis dengan bantuan software. Dalam hal ini dilakukan dengan bantuan GUI Matlab.

3. HASIL DAN PEMBAHASAN

Kualitas citra hasil dilihat dari dua aspek. Pertama, membandingkan kualitas citra hasil dengan citra original seperti yang terlihat oleh *Human Visual System* (HVS). Kedua, pengukuran menggunakan Peak Signal-*to-Noise* Ratio (PSNR) untuk mengevaluasi perbedaan antara citra hasil dan citra original.

Ke-empat image masih menunjukan kualitas yang baik karena nilai MSE masih dalam *range* nol dan PSNR diatas 50 dB (gambar 2) Ini berarti bahwa citra asli secara HVS tidak jauh berbeda dengan citra yang telah diproses. Gambar 3 menampilkan perbandingan salah satu citra yang diproses dari 2 bit sampai dengan 7 bit.

Gambar 2. Penyisipan menggunakan 1 Bit dengan jumlah karakter sesuai daya tampung citra.

Gambar 3. Hasil penyisipan 2 bit sampai 7 bit

Dari gambar 3 tersebut terlihat bahwa pada saat disisipkan 2 bit dan 3 bit, nilai MSE masih dibawah 4. Saat disisipi 4 bit maka nilainya maningkat diatas 13 yang menyebabkan PSNR menjadi 36,74 dB. Ini sudah kurang baik hasilnya. Demikian pula saat disisipi dengan 5 bit sampai 7 bit. Penurunan kualitas gambar sangat terlihat jelas. Penggunaan sampai 8 bit tidak ditampilkan lagi karena hasilnya lebih jelek dari 7 bit. Artinya secara HVS, penyisipan sampai dengan 3 bit menunjukan hasil yang baik.

Menyangkut pengambilan data kembali dari citra tidak menemui kendala bila data yang disisipkan pada citra sesuai dengan daya tampung citra tersebut. Dan juga, modulo yang dipakai pada saat diacak harus sama dengan yang dipakai pada saat ekstraksi.

4. KESIMPULAN

1. Jumlah karakter pesan teks harus sama atau kurang dari daya tampung maksimal citra penampung, jika lebih maka akan terjadi kesalahan. *Modullo* yang digunakan pada saat penyisipan dan pengekstrakan juga harus sama.
2. Secara *Human Visual System* (HVS) citra hasil dengan menggunakan kombinasi metode kriptografi *Caesar cipher* dan metode steganografi LSB untuk penggunaan 1 bit, 2 bit, 3 bit, tampak sama dengan citra aslinya dan sangat sulit untuk dibedakan. Sedangkan hasil pengujian sampai bit ke 6, 7 dan 8, pada image terjadi penurunan intensitas warna.

DAFTAR PUSTAKA

[1]. Ariyus, Doni 2010, " *Pengantar Ilmu Kriptografi".* Jakarta : Andi

[2]. Ahmad, Usman 2005, *" Pengolahan Citra Digital & Teknik Pemogramannya "* Yogyakarta : Informatika

[3]. Cole, Eric 2013, *" Hiding in Plain Sight : Steganography and The Art of Covert Communication ".*

[4]. Indrajit, Richard Eko, *" Manajemen Keamanan Informasi dan Internet ".* Jakarta : Elex Media Komputindo

[5]. Kromodimoeljo, Sentot 2010, *" Teori dan Aplikasi Kriptografi ".*

[6]. Kadir, Abdul 2012, " *Teori dan Aplikasi Pengolahan Citra ".* Yogyakarta : Andi

[7]. Munir, Rinaldi 2008, *" Kriptografi ".* Bandung : Informatika : Andi

[8]. Prasetyo, Eko 2011, *" Pengolahan Citra Digital dan Aplikasinya Menggunakan Matlab ".* Gresik : Andi

[9]. Sadikin, Rifki 2012, *" Kriptografi Untuk Keamanan Jaringan ".* Jakarta : Andi