PENYEMBUNYIAN PESAN MENGGUNAKAN STEGANOGRAFI DENGAN METODE LSB DAN ENKRIPSI KRITOGRAFI

***Lekso Budi Handoko*[1] *, Chaerul Umam*[2]**
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
e-mail: handoko@dsn.dinus.ac.id, chaerul.umam@dsn.dinus.ac.id

ABSTRAK

Steganografi adalah sebuah teknik untuk menyembunyikan pesan dengan menggunakan sebuah media atau juga disebut cover. Sedangkan LSB (Least Significant Bit) adalah sebagai algoritma atau metode menyembunyikan pesan yang akan disisipkan. Seperti pada perangkat keamanan lainnya, steganografi dapat digunakan pengamanan seperti citra dengan watermarking dengan alasan untuk perlindungan copyright. Metode LSB yang digunakan pada teknik steganography tergolong mudah pada penerapannya. Dasar dari metode ini adalah bilangan berbasis biner atau dengan kata lain angka 1 dan angka 0. Metode LSB berhubungan dengan ukuran 1 bit dan ukuran 1 byte, yang terdiri dari 8 bit data. Dalam penelitian ini penulis menggabungkan metode LSB dengan kriptografi metode Caesar Cipher. Dari hasil penggabungan metode antara LSB dan kriptografi akan sulit dipecahkan, karena memiliki dua tingkat keamanan. Dari hasil penelitian dapat diambil kesimpulan bahwa sistem pengamanan pesan menggunakan kriptografi dan steganografi terbagi menjadi empat, yaitu Encode, Decode, Enkripsi dan Dekripsi. Tujuan utama untuk mengamankan subtansi data rahasia dengan cara menyamarkan dengan sebuah media agar sulit untuk teridentifikasi.

***Kata kunci**: steganografi, LSB, enkripsi, dekripsi,*

kriptografi **1. PENDAHULUAN**

Kebutuhan manusia terhadap kemajuan terknologi informasi saat ini tidak dapat dipungkiri, dikarenakan sangat memudahkan setiap orang dalam melakukan aktivitasnya dengan menggunakan teknologi. Namun perkembangan teknologi tersebut turut pula meningkatkan kejahatan yang berbentuk pencurian data atau pembajakan oleh orang lain yang tidak memiliki hak akses atas data atau file tersebut untuk mendapatkan keuntungan. Berdasarkan ketentuan undang-undang no 28 tahun 2014 tentang hak cipta bahwa pembajakan adalah pelanggaran hak cipta, dimana karya cipta fotografi perlindungannya berlaku selama 50 tahun sejak pertama kali pengumuman. Oleh karena itu, kerahasiaan dan keamanan informasi menjadi sangat penting terutama untuk pesan-pesan pribadi. Adapun cara untuk melindungi informasi dari gambar digital dapat dilakukan dengan memasukkan pesan teks [1], di mana teks berisi informasi dari fotografer atau pemilik gambar digital. Pada penilitian ini akan memberikan solusi untuk mengatasi hal tersebut dengan metode steganografi dan kriptografi sehingga menjadi hal yang menarik pada penelitian dibidang ini.

Steganografi adalah salah satu teknik yang paling penting digunakan untuk menanamkan pesan rahasia dalam sebuah gambar sehingga data yang ditransmisikan tidak bisa diketahui oleh orang lain yang tidak memiliki wewenang. Steganografi membutuhkan setidaknya dua properti. Properti pertama adalah wadah (cover) dan yang kedua adalah data atau pesan yang disembunyikan [2]. Least Significant Bit (LSB) adalah salah satu metode steganografi yang dapat digunakan untuk menanamkan pesan rahasia dalam sebuah citra digital. Proses memasukkan metode pesan LSB (Least Significant Bit) adalah dengan memasukkan bit pesan ke setiap bit terakhir dari citra digital [3]. Pada makalah ini menggunakan LSB 3-3-2, dimana tiga bit pertama dari pesan rahasia disisipkam kedalam 3 bit LSB dari pixel merah, 3 bit berikutnya dalam LSB piksel Hijau. Sisa 2 bit pesan rahasia disisipkan ke bit LSB piksel Biru. Karena warna biru lebih sensitif untuk mata dan perubahan yang signifikan dalam warna ini dapat dengan mudah diperhatikan oleh mata manusia, oleh karena itu hanya dua bit dari piksel biru yang telah diambil untuk penyematan data.

Seperti yang diusulkan peneliti [4], sistem baru untuk menanamkan pesan rahasia dalam gambar cover menggunakan metode penyisipan LSB berbasis Hash (3, 3, 2) dengan algoritma cipher Affine. Sistem yang dirancang untuk mengenkripsi data dan menyembunyikan semua data di dalam pola dalam pesan untuk menjaga privasi data. Kemudian, sistem telah dikembangkan berdasarkan algoritma kriptografi dan steganografi.

Penerapan teknik steganografi tidak cukup untuk memberikan keamanan pada pengiriman pesan, untuk itu perlu adanya modifikasi dengan menggabungkan teknik steganografi dan kriptografi. Kriptografi adalah teknik untuk mentransfer informasi dengan aman di antara dua pihak dengan mempertahankan kerahasiaan data dengan melibatkan algoritma dan nilai kunci untuk mengubah informasi menjadi format yang tidak dapat dipahami oleh pengguna yang tidak sah atas informasi terserbut [5]. Kriptografi mengubah data asli (plaintext) menjadi data yang dienkripsi (ciphertext). Modifikasi ini berperan penting untuk mencapai kemampuan implant yang lebih tinggi dan tingkat deformasi rendah [6].

Caesar cipher adalah salah satu algoritma cipher klasik yang pertama dikenal dalam perkembangan ilmu kriptografi karena paling tua dan paling sederhana sehingga sangat mudah untuk digunakan [7]. Dalam

prosesnya, caesar cipher melakukan pergeseran terhadap semua karakter 3 pada plainteks dengan nilai pergeseran yang sama dengan jumlah kuncinya maksimal hanya 26 kunci, sehingga algoritma ini tingkat keamanannya rendah. Untuk itu perlu adanya modifikasi dengan algoritma lain. Pada penelitian ini menggunakan algoritma vigenere cipher.

2. METODE PENELITIAN

Penelitian ini bertujuan untuk mengimplementasikan Teknik Steganografi dengan metode LSB (Least Significant Bit) dan enkripsi kriptografi pada proses penyisipan pesan kedalam citra menggunakan software MATLAB R2015a.

2.1 Konsep Steganografi

Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya [8]. Media yang digunakan umumnya merupakan suatu media pembawa informasi rahasia, dimana disinilah fungsi dari teknik steganografi yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas.

Gambar 1. coba4.bmp.

2.2 Metode LSB (Least Significant Bit)

Metode LSB (*Least Significant Bit*) digunakan dalam teknik *Steganografi* dikarenakan tergolong mudah dalam penerapannya. Dasar dari metode ini adalah bilangan berbasis biner atau dengan kata lain angka 0 dan 1 [9]. Karena data digital merupakan susunan antara angka 0 dan angka 1 maka proses penerapannya lebih mudah. Metode ini berhubungan erat dengan ukuran 1 bit dan ukuran 1 byte 1 bit data dapat dikatakan terdiri dari 8 bit data. Dimana bit pada posisi paling kanan yang disebut dengan bit pada posisi LSB (*Least Significant Bit*) [10]. Teknik steganografi dengan menggunakan metode LSB (*Least Significant Bit*) adalah teknik dimana kita mengganti bit pada posisi LSB pada data dengan bit yang dimiliki oleh data yang akan disembunyikan. Karena bit yang diganti hanyalah bit yang paling akhir, maka meskipun data telah berubah, kita tetap tidak akan bisa mengenalinya, karena *stego* yang dihasilkan hampir sama persis dengan media sebelum disisipi oleh data yang ingin disembunyikan [11].

00100111	11101001	11001000	00100111	11001000	11101001	11001000	00100111

Gambar 2. Ilustrasi metode LSB

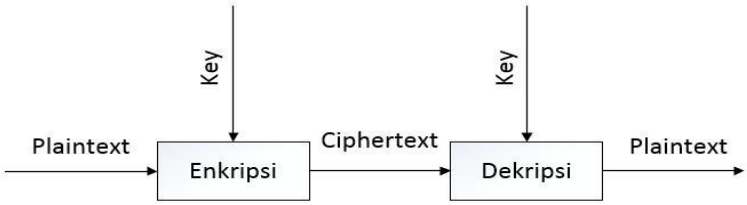
Dari data diatas akan disisipkan suatu pesan rahasia yang berupa data biner dengan nilai bit 01001000

00100110	11101001	11001000	00100110	11001001	11101000	11001000	00100110

Gambar 3. Pesan yang disisipkan

2.1.2 Kriptografi

Kriptografi (cryptography) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, integritas data, serta autentika data [5]. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula diartikan sebagai ilmu atau seni yang menjaga keamanan pesan. Pada prinsipnya, Kriptografi memiliki 4 komponen utama yaitu:Plaintext yaitu pesan yang dapat dibaca, Ciphertext yaitu pesan acak yang tidak dapat dibaca, Key yaitu kunci untuk melakukan kriptografi, Algorithm yaitu metode untuk melakukan enkripsi dan dekripsi [6].



Gambar 4. Alur enkripsi dan dekripsi

Enkripsi (Encryption) adalah sebuah proses menjadikan pesan yang dapat dibaca (plaintext) menjadi pesan acak yang tidak dapat dibaca (ciphertext). Berikut ini adalah contoh enkripsi yang digunakan oleh Julius Caesar, yaitu dengan masing-masing huruf dengan 3 huruf selanjutnya (disebut juga Additive/Subtitution Cipher):

Plaintext	Ciphertext
rumah	dgymt
motor	yafad
kompor	waybad
dst...	...

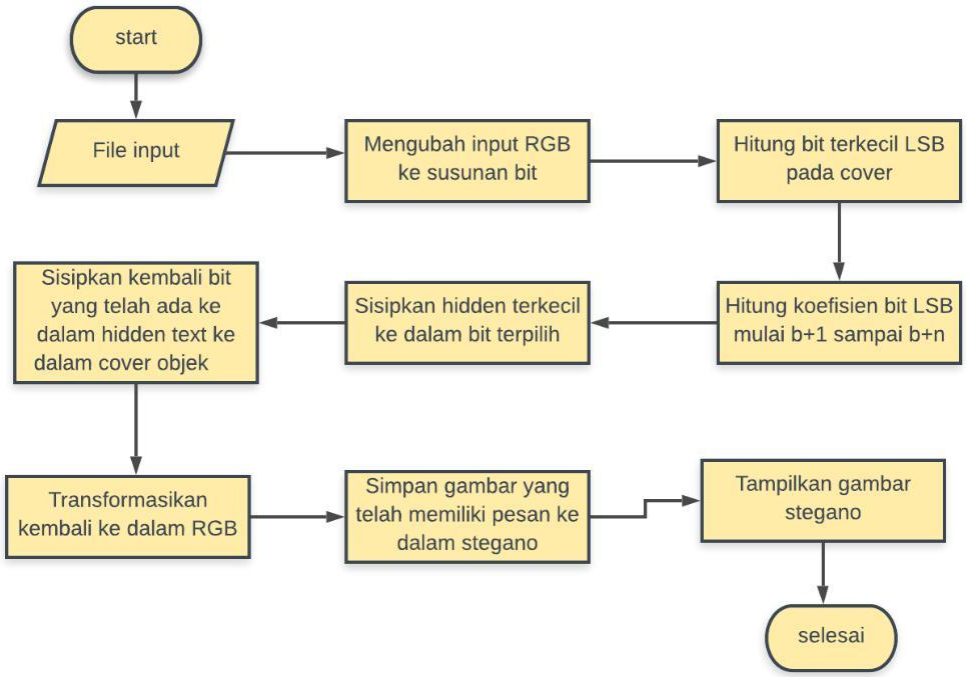
Dekripsi merupakan proses kebalikan dari enkripsi dimana proses ini akan mengubah ciphertext menjadi plaintext dengan menggunakan algoritma ‘pembalik’ dan key yang sama. Contoh:

Ciphertext	Plaintext
dgymt	rumah
yafad	motor
waybad	kompor
dst...	...

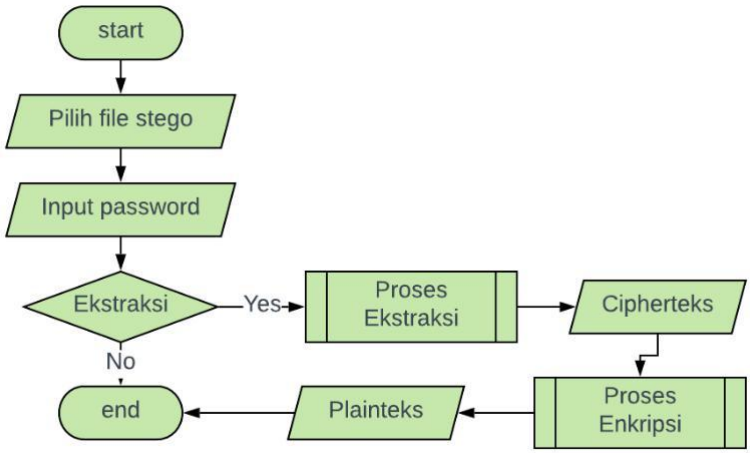
Berikut ini merupkaan tahapan analisis yang telah dilakukan:

1. Pada LSB bagian stegano ada 2 bagian yaitu embed dan ekstrak pada pesan yang akan disembunyikan diubah menjadi biner.
2. Pesan yang sudah dalam bentuk biner kemudian disisipkan ke dalam cover pada bit terakhir cover yang akan disembunyikan.
3. Biner yang telah diambil pada proses ekstraki sehingga dalam bentuk enkripsi.
4. Steganografi LSB (Least Significant Bit) dengan ekripsi kriptografi yaitu dengan pesan yang sudah di enkripsi akan diubah menjadi biner kriptografi.
5. Pesan yang sudah di embed dengan kripto akan membentuk ekstrasi
6. Lalu pesan yang sudah di ekstrasi dengan metode kriptografi dalam bentuk biner akan di dekripsi menjadi text.

Dalam sebuah perancangan sistem tentunya sangat penting dalam pembuatan perangkat lunak. Flowchart dipakai untuk menggabungkan struktur menyeluruh dan aliran sistem ke pengguna akhir karena sistem ini dapat menawarkan tampilan fisik yang berperan penting pada keterkaitan hardware dan data media.



Gambar 5. Proses Embed Metode LSB



Gambar 6. Proses Kriptografi

2.3 Peak Signal to Noise Ratio

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR diukur dalam satuan desibel. Standar nilai PSNR untuk citra dengan bit depth 8 bit adalah 30dB - 40dB atau lebih [5]. MSE adalah nilai error kuadrat rata-rata antara citra cover dengan citra tersteganografi. Semakin rendahnilai MSE maka akan semakin baik, dan semakin besar nilai PSNR maka semakin baik kualitas citra steganografi.

$$PSNR = 10 \log 10 \frac{MAX^2}{MSE} \quad (1)$$

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \left[f((i,j) - g(i,j)) \right]^2 \quad (2)$$

$$RMSE = \sqrt{\frac{1}{m \times n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \left[f(i,j - g(i,j)) \right]^2} \quad (3)$$

Dimana:

MSE = Nilai Mean Square Error citra steganografi

m = Panjang citra stego (dalam pixel)
f(i,j) = nilai piksel dari citra cover
n = lebar citra stego (dalam pixel)
g(i,j) = nilai piksel pada citra stego

3. HASIL DAN PEMBAHASAN

Potongan Program LSB (Least Significant Bit) yang telah dilakukan dalam percobaan ini.

```
for i = 1 : height
        for j = 1 : width
             LSB = mod(double(c(i,j)), 2);
            if (k>m || LSB == b(k))
                s(i,j) = c(i,j);
            else
                if(LSB == 1)
                    s(i,j) = c(i,j) - 1;
                else
                    s(i,j) = c(i,j) + 1;
                end
            k = k + 1;
        end
        end
    end
```

Potongan Program Enkripsi

```
plainteks = 'udinus';
key = input('masukkan key= ');
disp('plainteks anda adalah');
disp(plainteks);
plainteks = upper(plainteks)
plainteks = abs(plainteks)
chiperteks = mod (plainteks +key-'A',26) + 'A';
chiperteks = char(chiperteks);
disp('chiperteks adalah');
disp(chiperteks);
```

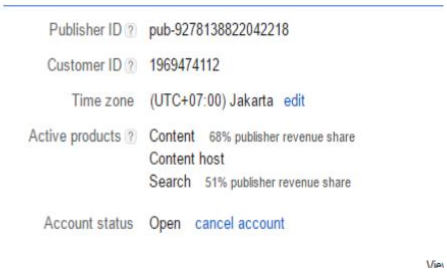
Potongan Program Dekripsi

```
plainteks = 'udinus';
key = input('masukkan key= ');
disp('plainteks anda adalah');
disp(plainteks);
plainteks = upper(plainteks)
plainteks = abs(plainteks)
chiperteks = mod (plainteks -key-'A',26) + 'A';
chiperteks = char(chiperteks);
disp('chiperteks adalah');
disp(chiperteks);
```

Tabel 1 Hasil Pengujian Menggunakan Cover Image

Pesan yang disisipkan	Plaintext (dalam bentuk ASCII)	Kunci	Chipertext	Cover Image	Stego Image
udinus	85 68 73 78 85 83	1234098765	XGLQXV	coba4.bmp	coba4.bmp
Sedang ujian	83 69 68 65 78 71 32 85 74 73 65 78	0987654321	JVUREXKL AZRE	coba4.bmp	coba4.bmp
Harap tenang ada ujian	72 65 82 65 80 32 84 69 78 65 78 71 32 65 68 65 32 85 74 73 65 78	72462582753 7645	OHYHWAA LUHUNAH KHABQPH U	ads.PNG	ads.PNG

Gambar 7. coba4.bmp



Gambar 8. ads.PNG

4. KESIMPULAN

Kesimpulan harus mengindikasi secara jelas hasil-hasil yang diperoleh, kelebihan dan kekurangannya, serta kemungkinan pengembangan selanjutnya.

Berdasarkan dari hasil dan pembahasan yang telah dilakukan maka dapat ditarik kesimpulan bahwa Teknik Steganografi dengan metode LSB (Least Significant Bit) dan Enkripsi Kriptografi yang tepat untuk diimplementasikan dalam pengamanan pesan yang disisipkan pada file image. Hasil dari proses embed dan ekstrak dari metode LSB (Least Significant Bit) dari hasil embed dan ekstrak tersebut diambil bit yang terakhir yang berupa angka 0 atau angka 1. Seperti pada percobaan Tabel 1 untuk mengetahui hasil sebelum dan sesudah dicover image. Begitu pula pada proses selanjutnya yaitu Kriptografi yang terdapat didalamnya memiliki 4 komponen utama yaitu:Plaintext yaitu pesan yang dapat dibaca, Ciphertext yaitu pesan acak yang tidak dapat dibaca, Key yaitu kunci untuk melakukan kriptografi, Algorithm yaitu metode untuk melakukan enkripsi dan dekripsi. Jadi, aplikasi ini dapat diimplementasikan untuk mengamankan pesan teks dengan cover stegano dan juga enkripsi kriptografi.

Kelebihan dari keamanan berlapis :

1. Metode LSB (Least Significant Bit) dapat menyembunyikan pesan yang sulit untuk dipecahkan
2. Citra yang telah disisipkan pada cover image ditambah dengan enkripsi kriptografi akan semakin sulit untuk dipecahkan oleh orang yang tidak berkepentingan.
3. Dibutuhkan key untuk mengkodekan enkripsi pada pesan yang disembunyikan.
4. Pesan yang sudah dienkrip kemudian akan menjadi ciphertext kemudian diembed.
5. Setelah itu didekrip dan akan menjadi plaintext, sehingga pesan yang disembunyikan akan semakin aman.

DAFTAR PUSTAKA

[1] O. E. Omolara, A. I. Oludare, and S. E. Abdulahi, "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication," *Comput. Eng. Intell. Syst.*, vol. 5, no. 5, pp. 2222–1719, 2014.

[2] C. A. Sari and E. H. Rachmawanto, "Gabungan Algoritma Vernam Chiper Dan End of File," *Techno.COM*, vol. 13, no. 3, pp. 150–157, 2014.

[3] M. Jain and S. K. Lenka, "Secret data transmission using vital image steganography over transposition cipher," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, pp. 1026–1029.

[4] A. M. Abdullah and R. H. H. Aziz, "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm," *Int. J. Comput. Appl.*, vol. 143, no. 4, pp. 0975 – 8887, 2016.

[5] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "A Good Performance OTP Encryption Image based on DCT-DWT Steganography," *TELKOMNIKA*, vol. 15, no. 4, pp. 1987–1995, 2017.

[6] P. Bindlish, "Study of RSA, DES and Cloud Computing," *Int. J. Adv. Res. Comput. Sci.*, vol. 7, no. 3, pp. 211–215, 2016.

[7] M. Mohan, M. K. K. Devi, and V. J. Prakash, "Security Analysis and Modification of Classical Encryption Scheme," *Indian J. Sci. Technol.*, vol. 8, no. 8, pp. 542–548, 2015.

[8] B. Datta, P. K. Pal, and S. K. Bandyopadhyay, "Multi-bit Data Hiding in Randomly Chosen LSB Layers of an Audio," in *2016 International Conference on Information Technology (ICIT)*, 2016, no. July, pp. 283–287.

[9] P. V Maitri and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm," in *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016*, 2016, pp. 1635–1638.

[10] C. Irawan, D. R. I. M. Setiadi, C. A. Sari, and E. H. Rachmawanto, "Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption," in *International Conference on Informatics and Computational Sciences (ICICoS)*, 2017.
[11] M. Baritha Begum and Y. Venkataramani, "LSB Based Audio Steganography Based On Text Compression," *Procedia Eng.*, vol. 30, pp. 703–710, 2012.