KOMBINASI STEGANOGRAFI-KRIPTOGRAFI CITRA MENGGUNAKAN LSB DAN DES

Ibnu Utomo WM[1*], Wellia Shinta Sari[2], Christy Atika Sari[3], De Rosal Ignatius Moses Setiadi[4]

[1]Program Studi Manajemen Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro

[2]Jurusan Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro

[3,4]Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro

Jl. Imam Bonjol 207 Semarang 50131

[*]Email: ibnu.utomo.wm@dsn.dinus.ac.id

Abstrak

Penggabungan dua buah teknik data hiding dapat dilakukan dengan batasan kemiripan metode atau hubungan algoritma satu dengan yang lain pada posisi saling melengkapi. Steganografi dan kriptografi, berdasarkan kesamaannya dalam tujuan proteksi data memunculkan peluang untuk dapat dikombinasikan. Least Significant Bit (LSB) yang merupakan algoritma dalam steganografi terbutki mudah untuk diterapkan dan cepat dalam komputasi namun kurang tahan serangan. Untuk menambah ketahanan terhadap serangan, dalam makalah ini LSB akan dikombinasi dengan Data Encryption Standard (DES). DES tahan terhadap serangan namun butuh banyak langkah. Paper ini menganalisa hasil enkripsi pada kombinasi LSB-DES dengan tujuan perolehan nilai PSNR yang tinggi. Dalam makalah ini juga telah diilustrasikan perubahan teks asli menjadi cipherteks dengan pada sejumlah batasan bit pesan pada file .txt. Ukuran file citra yang digunakan yaitu 512x512 piksel dan pesan 128 karakter. Pesan yang digunakan dalam bentuk file .txt. ekperimen telah menghasilkan nilai SSIM dan PSNR yang tinggi pada sisi steganografi. Sedangkan proses ektraksi pesan berhasil dilakukan dan telah dihitung waktu tempuhnya.

***Kata kunci**: DES, kriptografi, LSB, steganografi*

1. PENDAHULUAN

Dalam implementasinya kriptografi menjadi teknik data hiding yang paling populer. Sejak zaman Yunani kuno, kriptografi sudah digunakan dan terus berkembang sampai saat ini. Perkembangan kriptografi mulai dari media sampai ke algortimanya. Saat ini, banyak algoritma dirancang dan dikembangkan untuk memberikan keamanan terhadap informasi yang tersebar di seluruh dunia melalui jaringan (Rachmawanto and Sari, 2015). Algoritma ini dapat digolongkan sebagai algoritma *Symmetric* dan *Asymmetric* (Rahim and Ikhwan, 2016). Masalah penting yang membedakan mereka adalah penggunaan kunci. Dalam algoritma simetrik, hanya satu kunci yang digunakan dan ini disebut sebagai kunci privat. Dengan kata lain, algoritma simetrik juga disebut sebagai algoritma kunci pribadi karena menggunakan kunci pribadi baik untuk enkripsi dan dekripsi. Algoritma kunci asimetris menggunakan dua kunci, yang dapat didefinisikan sebagai kunci pribadi dan kunci publik (Prasetiyo, Rahmat and Beta, 2014). Kunci *private* digunakan untuk tujuan enkripsi sedangkan kunci publik digunakan untuk tujuan dekripsi. Algoritma ini juga disebut sebagai algoritma kunci publik. Dalam keuntungan untuk kunci pribadi, algoritma kunci publik menggunakan metode matematika komputasional dan kompleks.

Dalam algoritma kunci simetrik, kunci yang sama digunakan untuk baik enkripsi maupun dekripsi. Cukup dapat dipahami baik sebagai pengirim dan penerima menggunakan kunci yang sama untuk mengirim atau menerima pesan, misalnya DES, AES, *Caesar Cipher, Vigenere Cipher*, dan lainnya. DES dikenal aman karena proses pengacakan kuncinya yang menggunakan S-Box (Savitri, 2006). Di sisi lain terdapat metode lain yang juga dapat digunakan untuk melakukan proteksi data dengan tujuan *secret communication*, yaitu steganografi. Pada model umum steganografi, LSB sering digunakan karena kemudahan dalam implementasi (Anand and Sharma, 2014).

Kami telah menerapkan metode yang diusulkan dengan Matlab, dan mengevaluasinya dalam beberapa percobaan. Hasil eksperimen kami menunjukkan bahwa kunci rahasia yang dihasilkan oleh metode memiliki keacakan yang cukup baik dan ruang kunci yang sangat besar. Waktu dan biaya ruang dari metode ini terutama berasal dari prosedur komputasi dan penyimpanan kunci. Enkripsi dan waktu dekripsi kurang dari satu detik untuk citra *grayscale* 512x512 piksel dalam eksperimen. Citra *grayscale* dipilih karena komputasionalnya lebih sederhana dibanding dengan citra berwarna.

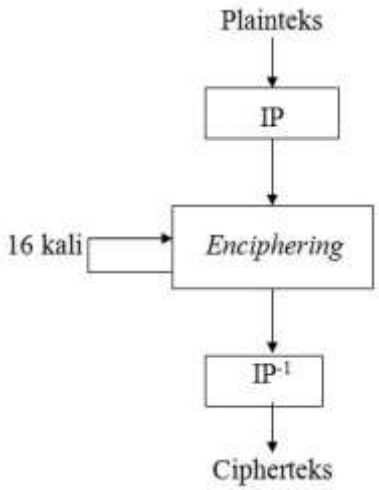
2. DATA ENCRYPTION STANDARD (DES)

Data Encryption Standard (DES) adalah standar kriptografi yang diusulkan sebagai algoritma untuk item aman dan rahasia pada tahun 1970 dan diadopsi sebagai standar federal Amerika oleh National Bureau of Standards (NBS) pada tahun 1973. DES adalah sebuah blok cipher, yang berarti bahwa selama proses enkripsi, plaintext dipecah menjadi blok-blok panjang tetap dan setiap blok dienkripsi pada saat yang bersamaan (Ardiansyah *et al.*, 2017). Pada dasarnya dibutuhkan 64 bit input teks biasa dan kunci 64-bit (hanya 56 bit digunakan untuk tujuan konversi dan sisa bit digunakan untuk pengecekan paritas) dan menghasilkan teks cipher 64-bit dengan enkripsi dan yang dapat didekripsi lagi ke dapatkan pesan menggunakan kunci yang sama. DES menggunakan operasi jaringan Fiestel seperti tampak pada Persamaan (1) dan Persamaan (2).

$$Li = R(i-1) \quad (1)$$

$$Ri = L(i-1) \oplus f(R(i-1), Ki) \quad (2)$$

Di dalam proses enciphering (Kusuma *et al.*, 2017), blok plaintext dibagi menjadi dua bagian, kiri (L) dan kanan (R), dengan masing-masing panjangnya 32 bit. Kedua bagian ini akan diproses menjadi 16 putaran DES. Di setiap putaran i, blok R adalah input untuk fungsi transformasi yang disebut fungsi f. Dalam fungsi f, blok R digabungkan dengan kunci internal K. Output fungsi f akan dioperasikan dengan blok L untuk mendapatkan blok R baru sesuai Persamaan 2; blok L baru diambil dari blok R sebelumnya sesuai Persamaan 1. Untuk model operasi DES dengan kunci 64 bit dapat dilihat pada Gambar 2.

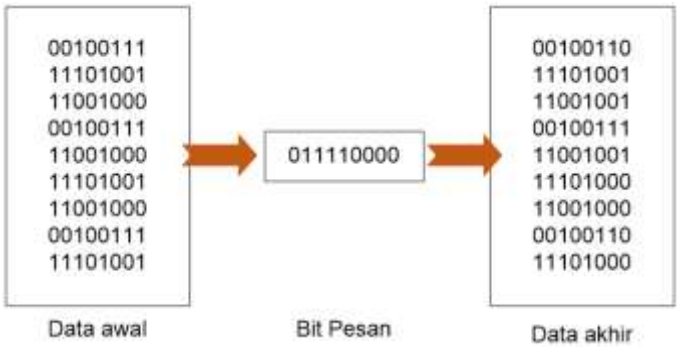


Gambar 1. Model umum operasi DES

3. LEAST SIGNIFICANT BIT

LSB adalah bit terendah dalam serangkaian angka dalam biner. misalnya dalam bilangan biner: 10110001, bit yang paling tidak signifikan adalah paling kanan 1. Steganografi berbasis LSB adalah salah satu metode steganografi (Kurdi, Elzein and Zeki, 2016), yang digunakan untuk menanamkan data rahasia ke dalam bit terkecil yang paling tidak signifikan dari nilai-nilai pixel dalam gambar sampul (Garg and Gulati, 2012).

misalnya 240 dapat disembunyikan di dalam delapan *byte* pertama dari tiga piksel dalam gambar 24 bit sesuai pada ilustrassi Gambar 2.

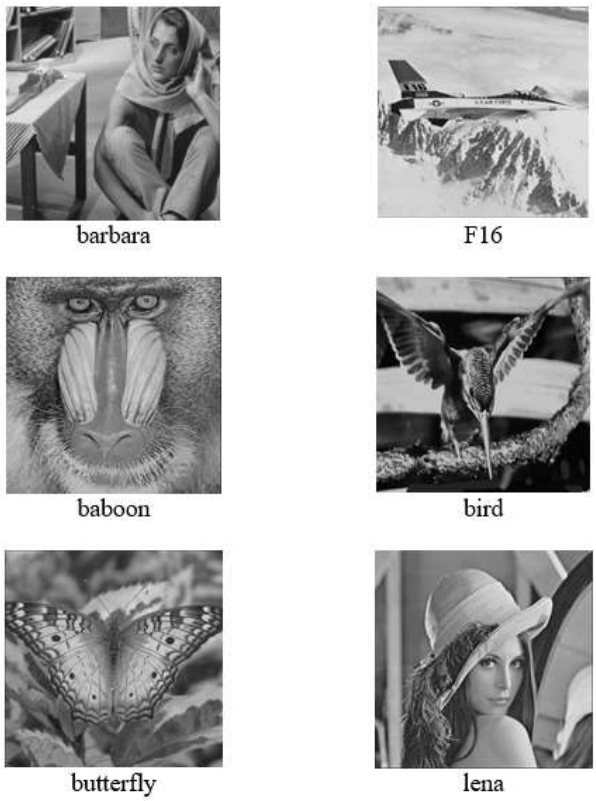


Gambar 2. Ilustrasi perubahan bit pada LSB

Pada Gambar 2, telah disembunyikan $240_{(10)}$ dalam gambar digital langkah pertama adalah mengubah 240 menjadi angka biner yaitu 011110000 maka data 9 bit ini diganti oleh setiap bit paling signifikan dari piksel gambar data awal.

4. HASIL ESKPERIMEN DAN PEMBAHASAN

Pada implementasi kriptografi simteris DES dengan steganografi LSB, eksperimen dilakukan pada 5 buah gambar *grayscale* 512x512 piksel yang terlebih dahulu di LSB kemudian dienkripsi menggunakan DES. Kunci yang digunakan yaitu 128 karakter yaitu "Karya ilmiah ini merupakan salah satu karya ilmiah dalam luaran penelitian IPTEKS UDINUS tahun ini dalam bentuk jurnal nasional.". Uji coba dilakukan pada 6 buah gambar berbeda sebagai citra cover, dan kunci yang digunakan adalah tetap 128 karakter. Berikut adalah citra terpilih untuk uji coba.



Gambar 3. Data citra uji

Hasil implementasi telah diukur menggunakan (MSE) dan *Peak Signal to Noise Ratio* (PSNR) sesuai persamaan (3) dan persamaan (4) serta waktu tempuh enkripsi dekripsi.

$$MSE = \frac{\sum_{i=1}^{x} \sum_{j=1}^{y} \left(f(i,j) - f'(i,j)\right)^2}{x * y} \quad (3)$$

$$PSNR = 10\, log10(\frac{255^2}{\sqrt{MSE}}) \quad (4)$$

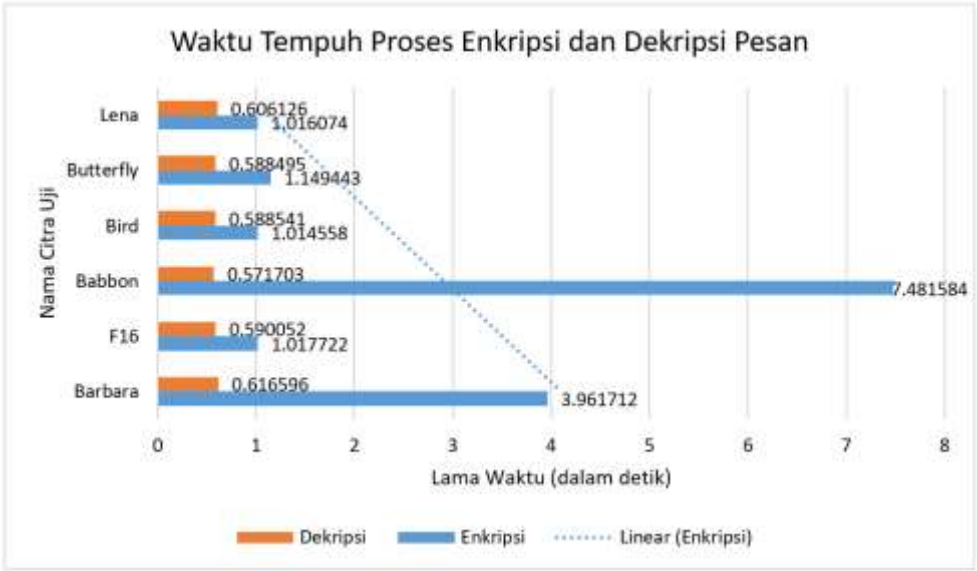
Pada persamaan (3) dan persamaan (4), diketahui bahwa:
f : citra asli
f' : citra hasil operasi
i : jumlah baris dalam citra
j : jumlah kolom dalam citra

MSE dan PSNR digunakan untuk menghitung selisih citra asli dan citra hasil pengolahan algoritma tertentu. Apabila nilai PSNR yang didapat lebih dari 40 dB (Irawan *et al.*, 2017), maka dapat dinyatakam bahwa citra tersebut tidak mengalami perubahan wujud yang dignifikan sehingga tidak dapat dibedakan secara kasat mata.

Tabel 1. Perolehan Nilai SSIM dan PSNR steganografi

Nama Citra	SSIM	PSNR
Barbara	1	75.2066
F16	1	75.2320
Baboon	1	79.9947
Bird	1	75.1813
Butterfly	1	75.2833
Lena	1	75.2150

Dari Tabel 1 di atas, dapat disimpulkan bahwa PSNR yang diperoleh jauh di atas standard. Hal ini tentu menjadi pembuktian terhadap kapabilitas algoritma yang diimplementasikan yaitu LSB dalam steganografi. Sedangkan nilai *Structural Similarity Index Measuement* (SSIM) yang diperoleh yaitu 1, yang berarti sempurna (Durga, Mamatha and Bindu, 2015). Pada Gambar 3, akan diilustrasikan waktu tempuh untuk proses enkripsi dan dekripsi menggunakan kombinasi LSB-DES pada seluruh citra uji.



Gambar 4. Grafik perbandingan waktu enkripsi dan dekripsi

Berdasarkan Gambar 2, terlihat adanya perbedaan pada proses enkripsi dan dekripsi. Proses enkripsi cenderung lebih lama dibanding waktu enkripsi. Bahkan pada citra babbon, waktu enkripsi merupakan waktu terlama dari keseluruhan proses enkripsi. Jarak antar kebutuhan waktu enkripsi dan dekripsi sangat signifikan. Apabila dikaitkan dengan Tabel 1, pda citra babbon mendapat nilai PSNR tertinggi yaitu 79,9947 dB. Dengan demikian dapat disimpulkan bahwa nilai PSNR yang tinggi tidak selalu berkaitan dengan waktu tempuh proses enkripsi yang cukup lama. Pada citra barbara perolehan PSNR yaitu 75.2066 dB, namun nilai PSNR hampir setara dengan citra lain yang waktu enkripsi dan dekripsinya tidak terpaut lama.

Tabel 2. Hasil perubahan bentuk cipherteks pada seluruh citra uji

Panjang Pesan	Cipherteks
128 karakter	ùìD<• ä¥Ó±Ví T€ Ô`."Ø•ü-²0ôtõtG] ÆÞ4t>”Eå"(8D- 4□„Æ- jÀþ‹¯cc-}ZFáùÃÎÇ_‘C© □]‡.¦¤'h#¸ '»Q¥Zz□() ’ ·°—¹_v¶o[rÕæiØ¢É ôµ g°p¶/gÓÔ=C|
128 karakter	Karya ilmiah ini merupakan salah satu karya ilmiah dalam luaran penelitian IPTEKS UDINUS tahun ini dalam bentuk jurnal nasional.

Tabel 2, membuktikan bahwa seluruh citra uji ketika diproses menggunakan kunci 128 karakter yang ditetapkan maka secara keseluruhan menghasilkan cipherteks yang sama. Hasil pada tabel diatas membuktikan bahwa proses enkripsi LSB-DES berjalan sesuai dengan prosedur enkripsi yang benar. Sedangkan hasil dekripsi juga telah dapat kembali seperti pesan semula yang digunakan untuk enkripsi.

5. KESIMPULAN

Kombinasi Steganografi dan Kriptografi telah selesai diimplementasikan. Pada proses enkripsi dengan LSB dapat dilihat perolehan nilai SSIM seluruh citra uji menghasilkan nilai 1 yang berarti sempurna. Dalam penelitian ini, SSIM digunakan untuk melengkapi perhitungan PSNR yang riskan pada perubahan bit citra digital. Nilai PSNR untutk seluruh citra lebihdari standrd yang ditentukan dan rata-rata menghasilkan 76.01882 dB. Sedangkan PSNR tertinggi diperoleh citra babbon dengan 79,9947 dB dan terendah pada citra bird yaitu 75.1813 dB. Untuk waktu enkripsi dan dekripsi pada semua citra hampir seimbang kecuali pada citra babbon. Dari kesimpulan di atas, lama waktu enkripsi dan dekripsi tidak selalu dapat dikaitkan dengan tingginya nilai PSNR dan SSIM yang diperoleh.

DAFTAR PUSTAKA

Anand, K., and Sharma, R., (2014), ‘Data Security using LSB and MSB Image Steganography’, *IJEE*, 1(6), pp. 10–13.

Ardiansyah, G. *et al.,* (2017), ‘Hybrid Method using 3-DES , DWT and LSB for Secure Image Steganography Algorithm’, in *2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, pp. 248–253.

Durga, K. V., Mamatha, G., and Bindu, C. H., (2015), ‘SVD based image watermarking with firefly algorithm’, in *2015 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE, pp. 1–7. doi: 10.1109/ICCCI.2015.7218081.

Garg, R., and Gulati, T., (2012), ‘Comparison Of Lsb & Msb Based Steganography In Gray-Scale Images’, *International Journal of Engineering Research & Technology (IJERT)*, 1(8), pp. 1–6.

Irawan, C. *et al.,* (2017), ‘Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption’, in *International Conference on Informatics and Computational Sciences (ICICoS)*.

Kurdi, M. M., Elzein, I. A., and Zeki, A. M., (2016), 'Least Significant Bit (LSB) and Random Right Circular Shift (RRCF) in Digital Watermarking', in, pp. 111–116.

Kusuma, E. J. *et al.*, (2017), 'An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption', in *International Conference on Innovative and Creative Information Technology (ICITech)*, pp. 1–5.

Prasetiyo, B., Rahmat, G., dan Beta, N., (2014), 'Kombinasi Steganografi Bit Matching dan Kriptografi DES untuk Pengamanan Data', *Scientific Journal of Informatics*, 1(1), pp. 79–93.

Rachmawanto, E. H., and Sari, C. A., (2015), 'Keamanan File Menggunakan Teknik Kriptografi Shift Cipher', *Techno.COM*, 14(4), pp. 329–335.

Rahim, R., and Ikhwan, A., (2016), 'Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher', *IJSRST*, 2(6), pp. 71–78.

Savitri, D. I., (2006), 'Analisis Keamanan Algoritma Kriptografi DES , Double DES , dan Triple DES', (13503081), pp. 1–15.