Kombinasi Kriptografi RC4 dan Steganografi LSB Pada Citra Digital Dengan Format Bitmap untuk Menjaga Keamanan Pesan

Ellya Helmud
Dosen STMIK Atma Luhur Pangkalpinang
Email : ellyahelmud@atmaluhur.ac.id

Abstrak

Keamanan dan kerahasiaan suatu pesan merupakan hal yang harus dijaga. Kebutuhan untuk menjaga keamanan pesan dan menjaga kerahasiaan pesan dibutuhkan dua metode yang berbeda, dimana untuk menjaga keamanan pesan digunakan kriptografi dan untuk menjaga kerahasiaan pesan digunakan steganografi. Pada penelitian ini, penulis mengkombinasikan kriptografi dan steganografi untuk menjaga keamanan dan kerahasiaan pesan. Kriptografi yang digunakan menggunakan algoritma RC4 dan steganografi yang digunakan menggunakan metode Least Significant Bit (LSB). Pada penelitian ini pengujian dilakukan dengan perangkat lunak Visual Studio 2008 dan untuk hasil gambar yang dihasilkan diuji menggunakan Matlab R2015b. Pengujian waktu pada proses enkripsi dan dekripsi menggunakan algoritma RC4 dilakukan sebanyak 10 kali dari jumlah karakter 100 hingga 1000 karakter, kemudian gambar yang dihasilkan mempunyai nilai error dan nilai kualitas yang tidak jauh berbeda.

Kata Kunci: *Kriptografi, Steganografi, LSB, RC4*

I. INTRODUCTION

Interaksi manusia dengan manusia maupun interaksi antara manusia dengan komputer adalah hal yang terjadi hampir setiap saat pada era globalisasi ini dimanapun dan dikalangan masyarakat apapun. Seiring dengan perkembangan hal tersebut, keamanan data maupun keamanan pesan menjadi bagian yang harus diperhatikan, karna kerahasiaan dan keamanan pesan atau data harus tetap terjaga. Sehingga terhindar dari orang yang tidak berkepentingan atau pihak ketiga dalam penyalahgunaan data atau informasi dari pesan yang dikirimkan. Dalam hal ini kriptografi membantu manusia dalam mengamankan pesan yang dikirimkan, sedangkarn kriptografi membantu manusia dalam menajga kerahasiaan pesan yang ada.

Didorong oleh kegunaan yang penting tadi, teknik algoritma kriptografi dan steganografi telah berkembang sejak zaman dahulu kala. Mulai dari era sebelum masehi, hingga sekarang algoritma kriptografi dan steganografi ini selalu berkembang. Mulai dari algoritma Caesar Cipher yang tergolong sederhana hingga algoritma Advanced Encryption Standar (AES) yang digunakan saat ini. Namun demikian, penelitian akademis yang ekstensif dalam bidang kriptografi masih tergolong baru, yaitu sekitar pertengahan 1970-an. Pada waktu tersebut, dua buah algoritma dikeluarkan, yaitu metode FSA dan DES yang dikembangkan oleh IBM. RC4 merupakan salah satu algoritma kunci simetris yang berbentuk stream cipher, yaitu memproses unit atau input data pada satu saat. Unit atau data pada umumnya sebuah byte atau kadang-kadang bit. Algoritma ini tidak harus menunggu sejumlah input data tertentu sebelum diproses, atau menambahkan byte tambahan untuk mengenkripsi. Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA. RC4 merupakan enkripsi stream simetrik proprietary yang dibuat oleh RSA *Data Security Inc* (RSADSI).

Pada penelitian kali ini penulis menggunakan algoritma LSB sebagai metode penelitiannya. Data akan disegmentasikan pada beberapa citra digital sehingga memungkinkan pengiriman data dengan ukuran yang besar. Dengan mengembangkan metode steganografi maka pengiriman data yang dilakukan tidak hanya memiliki tingkat keamanan yang baik, namun juga memiliki efisiensi dalam proses penyembunyian data yang cukup tinggi yaitu sekitar 30%. LSB merupakan salah satu metode dalam steganografi yang mengambil bit-bit terakhir warna pada citra dan menggantinya

dengan bit-bit data. Banyak cara yang dapat dilakukan untuk mengganti bit-bit warna pada citra, antara lain dengan melakukan operasi penambahan atau pengurangan nilai warna pada citra, atau juga dengan cara melakukan operasi AND dan OR antara bit-bit warna dengan bit-bit data.

II. RELATED WORK

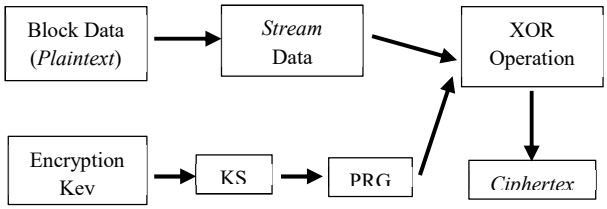
Keamanan data penting dalam suatu perusahaan. Keamanan dan integritas data adalah sesuatu yang harus diperhatikan. Upaya untuk menjaga agar informasi tidak terjerumus ke tangan orang-orang yang tidak berwenang dituntut perlunya menerapkan mekanisme keamanan yang baik. Ada banyak metode kriptografi yang umum dapat diterapkan, dalam klasifikasi umumnya terdiri dari dua, metode Symmetric dan Asymmetric. Dalam penelitian ini, dilakukan analisis dalam perspektif keamanan data dan kompleksitas komputasi dengan menggunakan dua jenis metode kriptografi, untuk implementasinya, menciptakan sistem dimana data ditransmisikan (plaintext) yang pertama dienkripsi oleh pengirim menghasilkan data terenkripsi (ciphertext) dan Akan dikirim ke receiver untuk melakukan proses dekripsi agar menghasilkan data yang utuh seperti sebelumnya [2].

Keamanan dan kerahasiaan data saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus yang melibatkan keamanan data sekarang merupakan pekerjaan yang membutuhkan biaya penanganan dan keamanan yang sangat banyak. Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi yang tidak dapat dibaca atau dipahami oleh siapapun, kecuali untuk penerima yang berhak, maka penerapan sistem keselamatan dirancang dengan metode enkripsi da ta dengan menggunakan algoritma RC4. RC4 (Rivets Cipher 4) adalah cipher aliran Synchrony, yang memiliki kunci simetris dan mengenkripsi digit plaintext adalah digit per byte menurut byte atau dengan menggabungkannya dengan operasi biner XOR dengan nomor acak [3].

Dengan pesatnya telekomunikasi dan komputer sangat memungkinkan pengguna menyimpan data secara digital. Dalam hal ini masalah keamanan dan kerahasiaan data adalah barang semut yang sangat impor, maka harus ada perlindungan untuk data rahasia. Teknik dalam ilmu kriptografi adalah salah satu cara yang bisa mengamankan data dari gangguan orang lain. Kriptografi adalah seni untuk mengamankan pesan ke dalam pesan yang tidak dikenali. Juga dikenal sebagai Rijndael Advanced Encryption Standard (AES) adalah algoritma enkripsi kriptografi yang digunakan. Namun, dengan menggunakan metode ini masih bisa menimbulkan kecurigaan, agar melengakapi bisa menyembunyikan data dengan aman dan tidak menimbulkan kecurigaan. Penggunaan steganografi yang paling sedikit signifikan (LSB) menjadi salah satu hak pilihin. Sedikit yang paling penting adalah metode untuk memasukkan sepotong informasi rahasia pada objek media lain seperti gambar atau jpg. Metode ini tidak menyebabkan perubahan besar pada gambar yang digunakan oleh mata telanjang [4]. Sedangkan kriptografi adalah ilmu yang mempelajari bagaimana menjaga agar data atau pesan tetap aman saat dikirim, dari pengirim ke penerima tanpa campur tangan orang lain. Tujuan dari penelitian ini adalah untuk memberikan keamanan maksimal terhadap citra digital, dengan menggunakan metode steganografi Least Significant Bit (LSB) dan algoritma kriptografi RC4 stream cipher. Hasil yang diharapkan dari penelitian ini adalah untuk menjamin penerapan citra digital [5]

III. RC4

RC4 memiliki sebuah S-Box, S0, S1,….S255 yang brisi permutasi dari bilangan 0 sampai 255. Dalam algoritma enkripsi metode ini akan membangkitkan pseudorandom *byte* dari *key* yang akan dikenakan operasi XOR terhadap *plaintext* untuk menghasilkan *ciphertext*.



Gambar 1 Diagram Proses Enkripsi RC4

Penjelasan perhitungan algoritma RC4:

Array S Array K
0 1 2 3 2 5 7 3
i = 0
j = (0 + S[0] + K [0 mod 4]) mod 4 = (0 + 0 + 2) mod 4 = 2
Swap (S[0],S[2])
2 1 0 3
i = 1
j = (2 + S[1] + K [1 mod 4]) mod 4 = (2 + 1 + 5) mod 4 =0
Swap (S[1],S[0])
1 2 0 3
i = 2
j = (0 + S[2] + K [2 mod 4]) mod 4 = (0 + 0 + 7) mod 4 = 3
Swap (S[2],S[3])
1 2 3 0
i = 3
j = (3 + S[3] + K [3 mod 4]) mod 4 = (3 + 0 + 3) mod 4 = 2
Swap (S[3],S[2])
1 2 0 3
Array S
1 2 0 3
i = 0, j = 0
i = (0 + 1) mod 4 = 1
j = (0 + S[1]) mod 4 = (0+ 2) mod 4 = 2
swap (S[1],S[2])
1 0 2 3
K1 = S[(S[1]+S[2]) mod 4] = S[2 mod 4] = 2
K1 = 00000010
i = (1 + 1) mod 4 = 2
j = (2 + S[2]) mod 4 = (2+ 2) mod 4 = 0
swap (S[2],S[0])
2 0 1 3
K2 = S[(S[2]+S[0]) mod 4] = S[3 mod 4] = 3
K2 = 00000011
i = (2 + 1) mod 4 = 3
j = (0 + S[3]) mod 4 = (0+ 3) mod 4 = 3
swap (S[3],S[3])
1 0 2 3
K3 = S[(S[3]+S[3]) mod 4] = S[6 mod 4] = 2
K3 = 00000010
i = (3 + 1) mod 4 = 0
j = (3 + S[0]) mod 4 = (3+ 1) mod 4 = 0
swap (S[0],S[0])
1 0 2 3
K1 = S[(S[0]+S[0]) mod 4] = S[2 mod 4] = 2
K1 = 00000010

HALO :
01001000 01000001 01001100 01001111

Key :
00000010 00000011 00000010 00000010

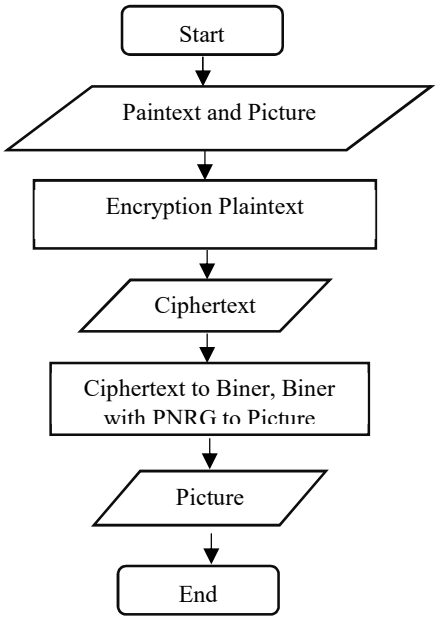
Cipherteks :

01001010 01000010 01001110 01001101
(L) (B) (N) (M)

IV. EXPERIMENTAL

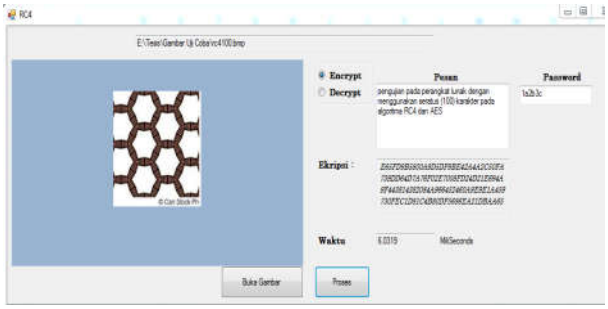
Implementation Encryption and Decryption

Characters	100
Key	1a2b3c
Algorithm	RC4

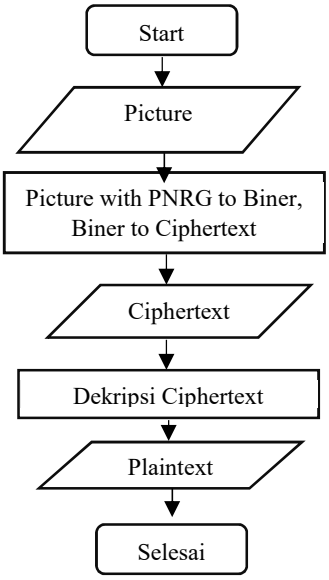


Gambar 2 Flowchart Proses Enkripsi

Berdasarkan diagram alir di atas, Bagian ini mencoba untuk mengenkripsi 100 karakter dengan Algoritma RC4.

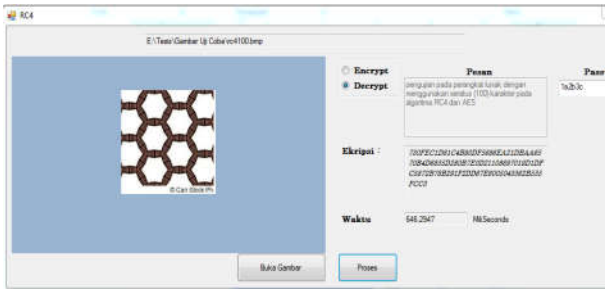


Gambar 3 Proses Enkripsi RC4



Gambar 4 Flowchart Proses Dekripsi

Bagian ini akan menerangkan pendeskripsian 100 karakter dengan Algoritma RC4.

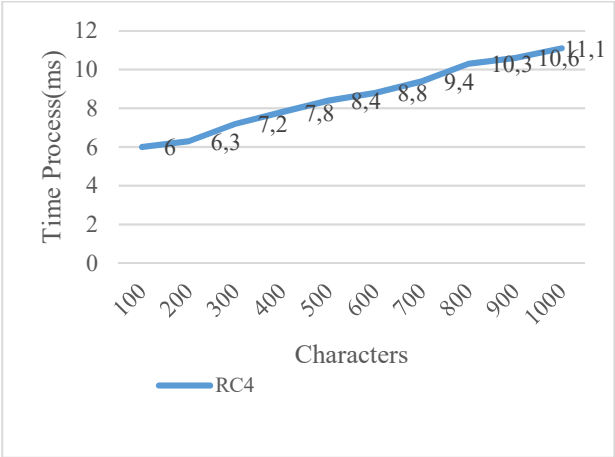


Gambar 5 Proses Dekripsi RC4

Kemudian hasil dari pengujian tersebut akan ditunjukan dalam table dan grafik berdasarkan waktu enkripsi dan waktu dekripsi, algoritma yang digunakan dan nilai MSE serta PSNR berdasarkan gambar yang dihasilkan.

Table 1 Waktu Enkripsi

Characters	Encryption Time (Millisecond)
	RC4
100	6
200	6.3
300	7.2
400	7.8
500	8.4
600	8.8
700	9.4
800	10.3
900	10.6
1000	11.1

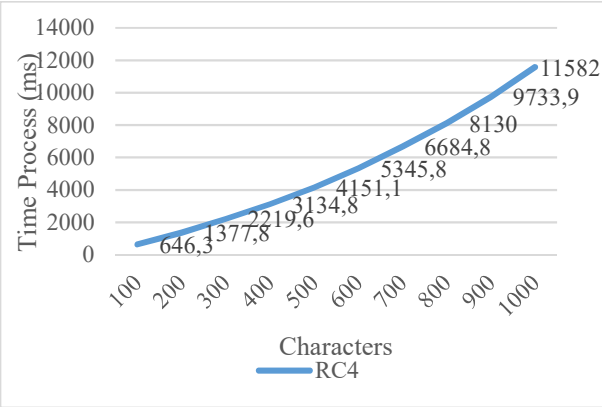


Gambar 6 Grafik Waktu Ekripsi RC4

Hasil grafik diatas menggambarkan lamanya waktu proses enkripsi untuk algoritma RC4 yang diterapkan pada metode LSB. Sumbu x menyatakan jumlah karakter yang dienkripsi dan sumbu y menyatakan lamanya proses enkripsi dalam satuan *millisecond*. Pengujian dilakukan sebanyak 10 kali untuk tiap jumlah karakter, nilai yang dimasukan kedalam grafik merupakan nilai rata-rata. Hal ini dilakukan untuk mendapatkan waktu yang konsisten, mengingat kinerja prosesor yang tidak stabil selama proses pengukuran waktu.

Table 2 Waktu Dekripsi

Characters	Decryptio Time (Millisecond)
	RC4
100	646.3
200	1377.8
300	2219.6
400	3134.8
500	4151.1
600	5345.8
700	6684.8
800	8130
900	9733.9
1000	11582



Gambar 7 Waktu Proses Dekripsi

Hasil grafik diatas menggambarkan lamanya waktu proses dekripsi untuk algoritma RC4 yang diterapkan pada metode LSB. Sumbu x menyatakan jumlah karakter yang dienkripsi dan sumbu y menyatakan lamanya proses enkripsi dalam satuan *millisecond*. Pengujian dilakukan sebanyak 10 kali untuk tiap jumlah karakter, nilai yang dimasukan kedalam grafik merupakan nilai rata-rata. Hal ini dilakukan untuk mendapatkan waktu yang konsisten, mengingat kinerja prosesor yang tidak stabil selama proses pengukuran waktu.

Table 3 Nilai MSE

Characters	RC4
	MSE
100	38.1781
200	38.2248
300	38.3687
400	38.4302
500	38.5769
600	38.7548
700	38.9389
800	39.1587
900	39.2893
1000	39.4443

Hasil grafik diatas menggambarkan nilai Mean Square Error (MSE) dari gambar yang dihasilkan berdasarkan algoritma RC4. Sumbu x menyatakan jumlah karakter yang terenkripsi dalam gambar, sedangkan sumbu y merupakan nilai MSE yang dihasilkan dalam satuan *decibel*. Berdasarkan grafik tersebut, nilai MSE pada gambar yang dihasilkan dari kombinasi algoritma RC4 dan LSB memiliki nilai yang berbeda dari tiap-tiap gambar yang dihasilkan,walaupun nilai tersebut tidak signifikan

Table 4 Nilai PSNR

Characters	RC4
	PSNR
100	32.2944
200	32.2733
300	32.2688
400	32.2635
500	32.2591
600	32.2504
700	32.2491
800	32.2449
900	32.2353
1000	32.2252

Hasil grafik diatas menggambarkan nilai Peak Signal to nnoise Ratio (PSNR) dari gambar yang dihasilkan berdasarkan algoritma RC4. Sumbu x menyatakan banyaknya karakter yang terenkripsi dalam gambar, sedangkan sumbu y merupakan nilai PSNR pada gambar.

V. CONCLUSION

Berdasarkan hasil analisa yang dilakukan dan hasil pengujian dari penelitian yang telah

dilakukan, maka kesimpulan yang diperoleh, yaitu sebagai berikut:

1. Kecepatan proses enkripsi dan dekripsi bergantung pada banyaknya jumlah karakter yang dienkripsi dan dekripsi.
2. Banyaknnya jumlah karakter yang terenkripsi dalam gambar mempengaruhi nilai MSE dan PSNR yang dihasilkan, walaupun tidak significant.
3. Ukuran yang berbeda-beda akan menghasilkan nilai MSE dan PSNR yang berbeda pula. Semakin besar ukuran file pesan maka nilai MSE akan semakin besar dan nilai PSNR semakin kecil, begitu pula sebaliknya semakin kecil ukuran file pesan maka nilai MSE semakin kecil dan nilai PSNR akan semakin besar.

REFERENCES

[1] Aplikasi Keamanan Informasi Menggunakan Teknik Steganografi Metode Least Significant Bit (LSB) Insertion dan RC4, Jamaluddin, UIN Syarif Hidayatullah 2010.

[2] Cheddad, A., Joan, C., Curran, K. & Paul, M.K. 2010, *Digital image steganography: Survey and analysis of current methods Signal Processing 90*

[3] Basri. 2016, *Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi*, Program Studi Teknik Informatika Universitas Al Asyariah Mandar, Jurnal Ilmiah Ilmu Komputer, Vol. 2, No. 2, September 2016

[4] Elka LH., Khairil dan Fery HU. 2014, *APLIKASI ENKRIPSI DAN DESKRIPSI DATA MENGGUNAKAN ALGORITMA RC4 DENGAN MENGGUNAKAN BAHASA PEMROGRAMAN PHP*, Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu, Jurnal Media Infotama Vol. 10 No. 1, Februari 2014

[5] Adetya, K.P. *Pengamanan Data Dengan Metode Advanced Cryption Standard dan Metode Least Significant Bit,* Mahasiswa Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semaran

[6] Utsav S. & Shiva S. 2016, *Image Steganography Using AES Encryption and Least Significant Nible¸* International Conference on Communication and Signal Processing,, India

[7] Nurhayati & Syukuri, S.H. 2014,*Steganography for Inserting Message on Digital Image Using Least Significant Bit and AES Cryptographic Algorithm*, Informatics Engineering Department, Science and Technology Faculty Syarif Hidayatullah State Islamic University (UIN) Jakarta,.

[8] Gede, W.B, & Made, I.W.2015, *Implementasi Algoritma Kriptografi AES 256 dan Metode Steganografi LSB pada Gambar Bitmap,* Jurnal Ilmiah Ilmu Komputer, Universitas Udayana, Vol. 8, No. 2, September 2015

[9] N.P, Indah, F.A. & Awang, H.K. 2015, *Jurnal Implementasi Kriptografi Pengamanan Data Pada File Teks, Isi File Dokumen dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard.* Jurnal Informatika Mulawarman Vol. 10 No.1