ANALISIS ALGORITMA KRIPTOGRAFI RC4 PADA ENKRIPSI CITRA DIGITAL

Galuh Adjeng Sekarsari[1], Bowo Nurhadiyono[2], Yuniarsi Rahayu[3]
[1,2,3]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jalan Nakula 1 No.5-11 Semarang
E-mail : galuhadjengsekarsari@gmail.com[1], bowo.nurhadiono@dsn.dinus.ac.id[2],
yuniarsi.rahayu@dsn.dinus.ac.id[3]

Abstrak

Keamanan dan kerahasian merupakan aspek penting dari suatu pesan, data maupun informasi baik berupa data teks, gambar maupun video. Salah satu cara untuk melindungi data citra digital tersebut dengan cara dekripsi dan enkripsi. RC4 merupakan salah satu algoritma kriptografi yang terkenal dengan kecepatannya dan sederhana sehingga dapat diimplementasikan baik pada perangkat keras maupun perangkat lunak dan digunakan sebagai standar protokol keamanan pengiriman data. Berdasarkan latar belakang tersebut maka pada penelitian ini dilakukan pengujian untuk mengetahui kemampuan maksimal dari algoritma RC4 yang ditinjau dari waktu pemrosesan baik pada enkripsi maupun dekripsi citra. Hasil pengujian meunjukkan waktu tercepat diperoleh dari citra berformat JPEG baik pada enkripsi maupun dekripsi citra untuk citra berukuran 256x256 pixel maupun 512x512 pixel.

Kata Kunci: *citra digital, enkripsi, dekripsi, algoritma RC4.*

Abstract

Safety and secrecy are important aspect of a message, data as well as information on text, image or video. One of the best ways to protect digital image data is by decryption and encryption. RC4 is one of famous cryptograph algorithm by speed and simplicity so it could be implemented either on hardware or software and it is used as standard security protocol on sending data. Based on the background above, so this research has done a test to know maximum capability of algorithm RC4 in terms of processing time either on encryption or image decryption. The result shows that the fastest time is earned by image in JPEG format either in encryption or image decryption for picture sized 256x256 pixel or 512x512 pixel.

Keywords: *digital image, encryption, decryption, RC4 algorithm.*

1. PENDAHULUAN

Semakin berkembangnya ilmu pengetahuan dan teknologi menjadikan keamanan informasi dalam penyimpanan serta transmisi data yang terdapat pada suatu sistem perlu diperhatikan. Algoritma kriptografi yang banyak digunakan adalah RC4 yang populer dengan kecepatan dan sederhana sehingga mudah untuk dikembangkan dan diimplementasikan secara efisien dalam perangkat keras maupun perangkat lunak [1]. Salah satu bentuk informasi yang banyak digunakan secara luas yaitu citra digital. Citra Digital sebagai salah satu bentuk data digital yang banyak digunakan untuk menyimpan foto, gambar, ataupun hasil karya dalam format digital. Citra yang bersifat pribadi atau citra yang mengandung informasi perlu dilindungi dari pengaksesan oleh pihak yang tidak memiliki otoritas [2].

Data citra pada umumnya memiliki ukuran yang relatif besar dibandingkan dengan data teks, maka proses enkripsi menggunakan algoritma yang tidak sesuai akan memerlukan waktu yang cukup lama [2]. Karena dikenal dengan kecepatan pemrosesan dan

keamananannya maka dapat digunakan algortima RC4 untuk penyandian pada citra digital. Pada proses penyandiannya algoritma RC4 beroperasi dari byte ke byte sehingga menghasilkan suatu rangkaian byte yang dapat diimplementasikan pada citra digital dengan menggunakan nilai pixel untuk proses penyandiannya.

Sedangkan keamanan yang dihasilkan dari penyandian citra digital diperoleh dari kunci yang dilakukan dengan menggunakan algoritma RC4 yang dapat menghasilkan suatu aliran kunci acak dan tidak adanya perulangan kunci sehingga menjadikan keamananan informasi pada citra digital dapat terjaga.

Tujuan penelitian ini yaitu menganalisa kemampuan maksimal yang dilakukan oleh algoritma RC4 terhadap waktu enkripsi dan dekripsi citra digital pada format citra BMP, JPEG dan PNG serta dengan ukuran masing-masing citra 256x256 pixel dan 512x512 pixel.

2. METODE

2.1 Kriptografi

Kriptografi merupakan salah satu bagian dari ilmu matematika yang disebut Cryptology yang bertujuan untuk menjaga kerahasiaan informasi yang terdapat pada data maupun citra sehingga informasi tidak dapat diketahui oleh pihak yang tidak berwenang [3]. Kriptografi adalah salah satu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integrasi data dan otentikasi.

2.2 Citra Digital

Citra digital merupakan baris dan kolom yang terdapat pada suatu matriks, dimana untuk setiap pasangan indeks baris dan kolom dapat menyatakan titik pada citra. Nilai dari matriks tersebut dapat menyatakan nilai kecerahan titik dari suatu citra. Titik-titik yang terdapat pada citra disebut sebagai elemen citra atau pixel (picture element) yang memiliki koordinat (x,y) dan menunjukan intensitas dari citra tersebut.

2.3 Algoritma RC4

Pada tahun 1987 di Laboratorim Rsa, Ron Rivest menemukan suatu algoritma yang diberi nama RC4. RC itu sendiri merupakan singkatan dari Ron's Code. Karena algoritma RC4 dapat diimplementasikan secara efisien pada perangkat lunak maka menjadikan algritma RC4 populer untuk aplikasi internet antara lain digunakan sebagai standar WEP (Wired Equivalent Privacy), WPA (Wifi Protected Acces) dan TLS (Transport Layer Protocol) [4][5]. RC4 juga diimplementasikan pada protokol SSL (Source Socket Layer) yaitu sebuah protokol untuk memproteksi trafik internet [6][7].

Terdapat dua tahapan untuk membangkitkan aliran kunci algoritma RC4 yaitu Key Scheduling Algorithm (KSA) dan Pseudo-Random Generator Algorithm (PRGA).

Key Scheduling Algorithm (KSA) merupakan tahapan pemberian nilai awal berdasarkan kunci enkripsi. State dari nilai awal tersebut berupa array dengan representasi permutasi 256 byte (dengan indeks 0 sampai dengan 255) dinamakan array S. Menggunakan rentang tersebut karena RC4 mengenkripsi pada mode byte (255 =2^8 dan 8 bit = 1 byte). Artinya maksimal panjang kunci yang dapat tersimpan pada array U adalah 256 karakter. Permutasi terhadap nilai array S dilakukan dengan pseudo-code berikut :

```
j = 0
```

```
for i = 0 to 255
        S[i] = i
for i = 0 to 255
        j = ( j + S[i] + U[i] ) mod
        256  swap ( S[i], S[j] )
        (*pertukaran nilai S[i]
        dan S[j] *)
```

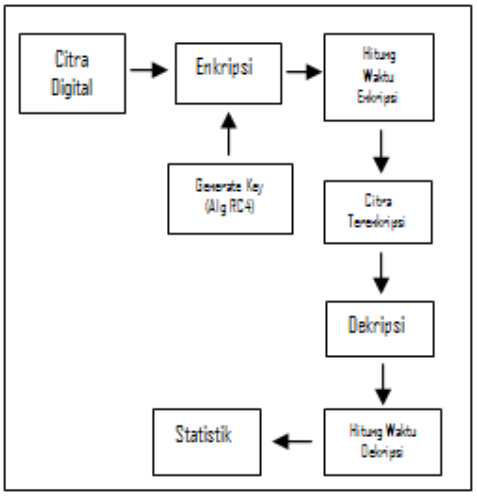
Tahap selanjutnya hasil dari array S yang telah melalui KSA akan diproses kembali pada PRGA (Pseudo-Random Generator Algorithm). Pada tahap PRGA terjadi modifikasi state dan output sebuah byte dari aliran kunci, dimana array S beroperasi dengan array U yang selanjutnya akan menghasilkan keystream. Nilai S[i] dan S[j] diambil dan dijumlahkan dengan modulo 256 untuk memembangkitkan aliran kunci. Hasil dari perhitungan tersebut akan menjadi indeks S[indeks] yang menjadi aliran kunci K yang kemudian digunakan untuk mengenkripsi plainteks ke-aliran kunci K yang kemudian digunakan untuk mengenkripsi plainteks ke-idx.

Setiap putaran bagian keystream sebesar 1 byte (dengan nilai antara 0sampai dengan 255) dioutputkan oleh PRGA berdasarkan state S. Berikut adalah PRGA dalam bentuk pseudo-code:

```
i = o
j = 0
for idx = 0 toPanjangPlainteks –
1 do
        i = ( i + 1 ) mod 256
        j = ( j + S[i] )mod 256
        swap ( S[i], S[j] ) (*
        penukaran nilai S[i] dan
        S[j] *)
        K = ( S[i] + S[j]) mod
        256
Endfor
```

Setelah keystream terbentuk, kemudian keystream tersebut dimasukkan dalam operasi XOR dengan plaintext.

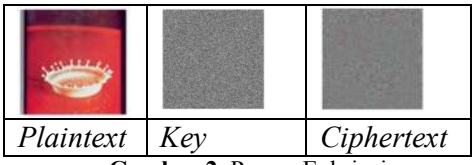
Alur Penelitian algoritma RC4 pada format citra digital adalah sebagai berikut.



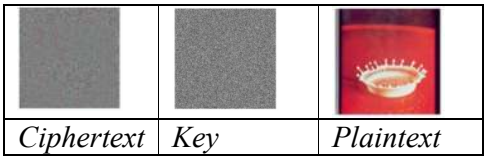
Gambar 1. Alur Penelitian

3. HASIL DAN PEMBAHASAN

Pengujian algoritma RC4 dilakukan pada enkripsi dan dekripsi citra digital ditinjau dari waktu pemrosesannya.



Gambar 2. Proses Enkripsi



Gambar 3. Proses Dekripsi

Dari pengujian yang dilakukan terhadap kecepatan enkripsi dan dekripsi citra digital dengan menggunakan algoritma RC4 diperoleh hasil sebagai berikut:

Tabel 1: Pengujian kecepatan enkripsi pada citra digital dengan ukuran 256x256 *pixel*.

No	File Citra	Rata-rata Kecepatan Enkripsi dalam Detik
1	BMP	7,726269
2	JPEG	6,837388
3	PNG	7,707722

Tabel 2: Pengujian kecepatan enkripsi pada citra digital dengan ukuran 512x512 *pixel*.

No	File Citra	Rata-rata Kecepatan Enkripsi dalam Detik
1	BMP	127,667953
2	JPEG	125,892711
3	PNG	128,062754

Tabel 3: Pengujian kecepatan dekripsi pada citra digital dengan ukuran 256x256 *pixel*.

No	File Citra	Rata-rata Kecepatan Enkripsi dalam Detik
1	BMP	0,001629
2	JPEG	0,001399
3	PNG	0,001728

Tabel 4: Pengujian kecepatan dekripsi pada citra digital dengan ukuran 512x512 *pixel*.

No	File Citra	Rata-rata Kecepatan Enkripsi dalam Detik
1	BMP	0,002664
2	JPEG	0,002613
3	PNG	0,002734

4. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan, maka dapat disimpulkan beberapa hal sebagai berikut:

1. Hasil pengujian untuk mengetahui kecepatan enkripsi pada dataset citra dengan ukuran 256x256 pixel menggunakan algoritma RC4 diperoleh waktu enkripsi lebih cepat terdapat pada citra dengan fomat JPEG. Kecepatan rata-rata enkripsi yang diperlukan yaitu 6,837388 detik.
2. Pada citra berukuran 512x512 pixel, citra dengan format JPEG memerlukan waktu enkripsi lebih cepat dibandingkan dengan citra dengan format BMP dan PNG. Waktu rata-rata yang diperlukan untuk proses enkripsi citra JPEG yang berukuran 512x512 pixel adalah 125,892711 detik.
3. Sedangkan pada proses dekripsi citra berukuran 256x256 pixel menghasilkan waktu yang relatif lebih cepat terdapat pada citra dengan format JPEG. Kecepatan rata-rata yang diperlukan untuk dekripsi citra yaitu 0,001399 detik.
4. Citra dengan ukuran 512x512 pixel diperoleh waktu dekripsi yang lebih cepat pada format citra JPEG. Proses dekripsi yang dilakukan pada citra format JPEG memerlukan waktu dekripsi 0,002613 detik.

DAFTAR PUSTAKA

[1] Yuri Ariyanto, "Algoritma RC4 dalam Proteksi Transmisi dan Hasil Query untuk ORDBMS Postgresql," jurnal informatika, vol. 10, no. 1, pp. 53-39, mei 2009. Rinaldi Munir, Kiptografi. Bandung: Informatika, 2006.

[2] Allam Mousa, Ahmad Hamad, (2006) Evaluation of RC4 Algorithm for Data Encryption. International Journal of Computer Science and Applications, Vol. 3, No.2, pp 44-56.

[3] Ruri Hartika Zain, "Perancangan dan Implementasi Cryptography dengan Metode Algoritma RC4 pad Type File Document Menggunakan Bahasa Pemrograman Visual BAsic 6.0," Jurnal Momentum Vo.12 No. 1 februari 2012, pp. 71-80, 2012.

[4] T. Sutojo, Mulyanto, Edi., Suhartono, Vincent., Nurhayati, O.D., Wijanarto, Teori Pengolahan Citra Digital. Yogyakarta: Andi, 2009.

[5] S. S. Gupta, A. Chattopadhyay, K.Sinha, S. Maitra, B. Sinha, "High Performance Hardware Implementation for RC4 Stream Cipher", Computers, IEEE Transactions on, vol.62, no.4, pp.730,743, April 2013 doi:10.1109/TC.2012.19

[6] Yuri Ariyanto, "Algoritma RC4 dalam Proteksi Transmisi dan Hasil Query untuk ORDBMS Postgresql," jurnal informatika, vol.

10, no. 1, pp. 53-39, mei 2009. Rinaldi Munir, Kiptografi. Bandung: Informatika, 2006.
[7] Prasetyo Andy Wicaksono, "Studi Pemakaian Algoritma RSA dalam Proses Enkripsi dan Aplikasinya".