Perbandingan Efisiensi, Efektifitas dan Kualitas Algoritma Rijndael dengan Algoritma Camellia pada Citra Digital

A Comparison of the Efficiency, Effectiveness, Quality of Rijndael Algorithm with Camellia Algorithm at Digital Image

Bagus Satrio Waluyo Poetro*[1], Retantyo Wardoyo[2]
[1,2] Program Pascasarjana Ilmu Komputer, FMIPA, UGM, Yogyakarta
e-mail: ***[1]bagusswp@gmail.com**, [2]**rw@ugm.ac.id**

Abstrak

Algoritma kriptografi harus dirancang agar pada satu sisi dapat digunakan oleh pengguna yang sah, dan pada sisi lain sulit dipecahkan oleh penyerang. Kriteria penting untuk algoritma kriptografi yang baik adalah bahwa ia harus praktis efisien bagi pengguna yang sah. Sebuah algoritma juga umumnya diharapkan efektif yang artinya semua operasi yang akan dilakukan dalam algoritma harus cukup dasar bahwa secara prinsip dapat dikerjakan tepat dan dalam panjang waktu yang terbatas. Citra digital dapat dengan cepat disalin, dipindahkan, dan digandakan tanpa kehilangan informasi atau kualitas gambar. Inspeksi visual tidak cukup untuk menentukan kualitas dari citra terenkripsi.

Dalam penelitian ini dilakukan perbandingan terhadap citra digital menggunakan algoritma Rijndael dan algoritma Camellia. Perbandingan dilakukan terhadap tiga format citra digital yaitu .bmp, .jpg, .png dengan ukuran citra uji 32x32 piksel. Penelitian ini menggunakan parameter Big O, Avalanche Effect, deviasi maksimum, koefisien korelasi, deviasi ketidakteraturan, waktu proses dan PSNR citra untuk menentukan efisensi, efektifitas, kualitas algoritma Rijndael dengan algoritma Camellia terhadap citra digital.

Berdasarkan hasil pengujian yang dilakukan, didapatkan beberapa kesimpulan yaitu algoritma Rijndael lebih efisien dibandingkan algoritma Camellia, algoritma Camellia lebih efektif dibandingkan algoritma Rijndael dan dari segi kualitas algoritma Rijndael lebih unggul dibandingkan dengan algoritma Camellia.

Kata kunci: Efisien, efektif, kualitas, citra digital, kriptografi, algoritma Rijndael, algoritma Camellia

Abstract

Cryptographic algorithm should be designed in such a way that on the one hand can be used by legitimate users, and on the other hand is a difficult by the attacker. An important criterion for a good cryptographic algorithm is that it must be practically efficient for legitimate users. An algorithm is also generally expected to be effective which means that all operations must be done in a fairly basic algorithm that can in principle be done right and in a limited length of time. Digital images can be quickly copied, transferred and duplicated with no loss of information or image quality. Visual inspection is not enough to determine the quality of the encrypted image.

In this study conducted a comparison of the digital image using the Rijndael algorithm and Camellia algorithm. Comparisons were made on three digital image format .bmp, .jpg, .png with size 32x32 pixels test images. This study uses parameters such as Big O, Avalanche Effect, maximum deviation, correlation coefficient, irregular deviation, time and image PSNR to determine the efficiency, effectiveness, quality of Rijndael algorithm with Camellia algorithm at digital image.

Based on the results of tests performed some conclusions are obtained, Rijndael algorithm is more efficient than the Camellia algorithm, Camellia algorithmis more effective than the Rijndael algorithm and in terms of the quality Rijndael algorithm is superior compared to Camellia algorithm.

Keywords: Efficient, effective, quality, digital image, cryptography, Rijndael algorithm, Camellia algorithm

1. Pendahuluan

Kriptografi mendukung kebutuhan dari dua aspek keamanan informasi, yaitu perlindungan terhadap kerahasiaan data informasi (*secrecy*) dan perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan (*authenticity*) (Wibowo, 2004).

Saat ini, AES (*Advanced Encryption Standard*) digunakan sebagai standar algoritma kriptografi yang terbaru. AES sendiri adalah algoritma kriptografi dengan menggunakan algoritma Rijndael. Rijndael adalah sebuah iterasi cipher blok dengan sebuah blok dan kunci dengan panjang yang bervariasi. Panjang blok dan kuncinya bisa dispesifikasikan secara independen kedalam 128, 192 atau 256 bit (Daemen dan Rijmen, 2001).

Algoritma Camellia dikembangkan secara bersama oleh NTT (*Nippon Telegraph and Telephone Corporation*) dan Mitsubishi Electric Corporation pada tahun 2000. Camelia mendukung ukuran blok 128-bit dengan kunci berukuran 128, 192 dan 256 bit sama seperti spesifikasi antarmuka AES (*Advanced Encryption Standard*) (Aoki dkk, 2000). Algoritma Camellia juga dikenal dengan kesesuaiannya dalam implementasi baik segi perangkat lunak maupun perangkat keras serta tingkat keamanannya yang tinggi (Matsui dkk, 2004).

Kriteria penting untuk algoritma kriptografi yang baik adalah bahwa harus praktis efisien bagi pengguna yang sah (Mao, 2003). Untuk mendapatkan algoritma yang efisien serta mendapatkan rumusan matematika sebagai ukuran kerumitan (kompleksitas) maka analisis algoritma dihitung dengan menggunakan teori kompleksitas waktu asimptotik Big O.

Kompleksitas algoritma terbagi menjadi 2, yaitu kompleksitas waktu dan kompleksitas ruang. Kompleksitas waktu diukur dari jumlah tahapan komputasi yang dibutuhkan untuk menjalankan algoritma sebagai fungsi dari ukuran masukan n (Koshy, 2004). Kompleksitas ruang menunjukan seberapa banyak ruang penyimpanan atau memori yang diperlukan oleh algoritma (Levitin, 2007).

Sebuah algoritma juga umumnya diharapkan efektif. Artinya semua operasi yang akan dilakukan dalam algoritma harus cukup dasar bahwa secara prinsip dapat dikerjakan tepat dan dalam panjang waktu yang terbatas (Knuth, 1997).

Ada dua konsentrasi utama dalam istilah efektifitas yaitu kemanjuran dan efisien atau dengan kata lain fokusnya pada kekuatan dan kecepatan (Nazaruk dan Ruzakov, 2010). Salah satu pertimbangan penting untuk mengukur kekuatan dari setiap algoritma kriptografi adalah *Avalanche Effect* nya.

Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek. Citra terbagi 2 yaitu ada citra yang bersifat analog dan ada citra yang bersifat digital (Sutoyo dkk, 2009). Citra digital adalah suatu citra f(x,y) yang memiliki koordinat spasial, dan tingkat kecerahan yang diskrit. Citra yang terlihat merupakan cahaya yang direfleksikan dari sebuah objek (Nugroho, 2004).

Tidak seperti pesan teks, data citra memiliki fitur spesial seperti redudansi tinggi dan korelasi yang tinggi diantara piksel-pikselnya. Selain itu, citra juga biasanya besar dalam ukuran, yang mana membuat metode enkripsi tradisional susah untuk diaplikasikan (El-Ashry, 2010).

Citra digital dapat dengan cepat disalin, dipindahkan, dan digandakan tanpa kehilangan informasi atau kualitas gambar (Anderson, 2001). Inspeksi visual tidak cukup untuk menentukan kualitas dari citra terenkripsi. Jadi, faktor pengukuran lainnya dianggap berdasarkan : pengukuran deviasi maksimum diantara citra asli dan citra terenkripsi, pengukuran koefisien korelasi diantara citra asli dan citra terenkripsi, perbedaan antara nilai piksel dari citra asli dan nilai piksel yang sesuai dari citra terenkripsi atau deviasi ketidakteraturan (*irregular*), waktu enkripsi dan *throughput* (El-Fishawy dan Zaid, 2007).

Kualitas sebuah citra selalu dikaitkan dengan resolusi kedalam intensitas warna. Resolusi citra menyatakan ukuran panjang kali lebar dari sebuah citra yang dinyatakan dalam satuan piksel. Semakin tinggi resolusi sebuah citra berarti semakin banyak jumlah piksel dan semakin tinggi kedalam intensitas berarti semakin banyak jumlah bit/pikselnya, hal ini mengakibatkan semakin baik kualitas citra tersebut (Sukirman dan Subali, 2008). Meskipun banyak parameter untuk mengkuantifikasi kualitas citra, PSNR (*peak signal to noise ratio*) dianggap merupakan salah satu parameter yang umum untuk melakukannya (Sianipar, 2010).

2. Metode Penelitian

2.1 Algoritma yang digunakan

Algoritma Rijndael

Tahap – tahap penyandian dalam algoritma Rijndael untuk proses enkripsi dan dekripsi secara urut didalam penelitian ini dapat dijelaskan sebagai berikut :

Proses Enkripsi

1. Memisahkan tiap *layer* citra asli menjdai *Red*, *Green*, *Blue*.
2. Menginisialisasi panjang baris dan kolom dari citra asli tiap *layer*.
3. Menginisialisasi kunci sebesar 128 bit (16 karakter).
4. Merubah bentuk kunci menjadi blok berukuran 4x4.
5. Melakukan proses *key scheduling* dari kunci sehingga menghasilkan sebuah nilai yang akan digunakan saat proses enkripsi.
6. Menginisialisasi blok data dari citra asli setiap 16 piksel (4x4).
7. Mengenkripsi blok data dari citra asli setiap sebesar 128 bit (16 piksel) sampai dengan ukuran maksimum dari citra asli tersebut.
8. Menggabungkan 3 *layer* yang kemudian disebut citra terenkripsi.

Proses Dekripsi

1. Memisahkan tiap *layer* citra terenkripsi menjadi *Red*, *Green*, *Blue*.
2. Menginisialisasi panjang baris dan kolom dari citra terenkripsi tiap *layer*.
3. Menginisialisasi kunci sebesar 128 bit (16 karakter).
4. Merubah bentuk kunci menjadi blok berukuran 4x4.
5. Melakukan proses *key scheduling* dari kunci sehingga menghasilkan sebuah nilai yang akan digunakan saat proses dekripsi.
6. Menginisialisasi blok data dari citra asli setiap 16 piksel (4x4).

7. Mendekripsi blok data dari citra asli setiap sebesar 128 bit (16 piksel) sampai dengan ukuran maksimum dari citra asli tersebut.
8. Menggabungkan 3 *layer* menjadi satu yang kemudian disebut citra asli.

Algoritma Camellia

Tahap – tahap penyandian dalam algoritma Camellia untuk proses enkripsi dan dekripsi secara urut dalam penelitian ini dijelaskan sebagai berikut :

Proses Enkripsi

1. Memisahkan tiap layer citra asli menjadi *Red*, *Green*, *Blue*.
2. Menginisialisasi panjang baris dan kolom dari citra asli tiap *layer*.
3. Menginisialisasi kunci sebesar 128 bit (16 karakter).
4. Melakukan proses *key scheduling* dari kunci sehingga menghasilkan 26 subkunci yang akan digunakan saat proses enkripsi.
5. Menginisialisasi blok data dari citra asli setiap 16 piksel (4x4).
6. Merubah bentuk blok data menjadi bentuk larik (*array*).
7. Mengenkripsi blok data dari citra asli setiap sebesar 128 bit (16 pikssel) sampai dengan ukuran maksimum dari citra asli tersebut.
8. Merubah setiap hasil proses enkripsi menjadi berbentuk blok kembali (4x4) sehingga membentuk sebuah citra yang berukuran seperti saat proses inisialisasi.
9. Mengulangi langkah 5 sampai dengan langkah 8 pada setiap *layer* yang belum terproses.
10. Menggabungkan 3 *layer* menjadu satu yang kemudian disebut dengan citra terenkripsi.

Proses Dekripsi

1. Memisahkan tiap *layer* citra terenkripsi menjadi *Red*, *Green*, *Blue*.
2. Menginisialisasi panjang baris dan kolom dari citra terenkrispsi tiap *layer*.
3. Menginisialisasi kunci sebesar 128 bit (16 karakter).
4. Melakukan proses *key scheduling* dari kunci sehingga menghasilkan 26 subkunci yang berkebalikan saat proses enkripsi. Contoh: kw1 -> kw3, kw2 -> kw4, dsb.
5. Menginisialisasi blok data dari citra asli setiap 16 piksel (4x4).
6. Merubah bentuk blok data menjadi bentuk larik (*array*).
7. Mendekripsi blok data dari citra hasil setiap sebesar 128 bit (16 piksel) sampai dengan ukuran maksimum dari citra terenkripsi tersebut.
8. Merubah setiap hasil proses dekripsi menjadi berbentuk blok kembali (4x4) sehingga membentuk sebuah citra yang berukuran seperti saat proses inisialisasi.
9. Mengulangi langkah 5 sampai dengan langkah 8 pada setiap *layer* yang belum terproses.
10. Menggabungkan 3 *layer* menjadi satu yang kemudian disebut citra asli.

Kunci yang digunakan

Kunci merupakan bagian penting dalam proses kriptografi. Panjang kunci untuk proses kriptografi dapat bervariasi. Kunci yang digunakan dalam penelitian ini memiliki panjang 16 karakter atau 128 bit. Kuncinya adalah ‘123456789abcdefg
’

Mode operasi yang digunakan

Mode operasi yang digunakan dalam penelitian ini adalah ECB (*Electronic Codebook*). Mode ini digunakan karena data yang diujicoba yaitu citra digital akan dibagi menjadi beberapa blok yang sama sebesar 128 bit dan memiliki kunci yang sama sebesar 128 bit. Mode ini juga memiliki kelebihan yaitu blok mana yang akan diproses terlebih dahulu tidak menjadi masalah, apakah blok yang tengah terlebih dahulu atau yang terakhir sekalipun.

2.2 Parameter yang digunakan

Perbandingan terhadap dua algoritma kriptografi yaitu algoritma Rijndael dan algoritma Camellia membutuhkan parameter – parameter tertentu untuk dapat menghasilkan kesimpulan yang baik. Parameter yang digunakan dalam penelitian ini adalah Big O, *Avalanche Effect*, maksimum deviasi, koefisien korelasi, deviasi ketidakteraturan (*irregular*) dan PSNR citra.

Parameter Big O

Kecanggihan suatu program bukan dilihat dari tampilan program, melainkan berdasarkan efisiensi algoritma yang terdapat didalam program tersebut (Levitin, 2007). Efisiensi berarti algoritma tersebut dapat dijalankan untuk ukuran masukan tertentu dengan waktu yang diperlukannya tumbuh dengan tidak drastis. Ukuran efisiensi waktu eksekusi dihitung dari *source code* program menggunakan nilai kompleksitas waktu asimptotik Big O.

Parameter Avalanche Effect

Menurut Raden (2010) *Avalanche Effect* merupakan salah satu cara untuk mengetahui tingkat efektifitas algoritma kriptografi dari file yang telah terenkripsi. Sebuah algoritma yang baik memiliki *Avalanche Effect* tinggi (Ramanjuma dan Karuppiah, 2011).

Parameter Deviasi Maksimum

Dengan implementasi dari sebuah algoritma enkripsi citra, terdapat perubahan dalam nilai piksel di citra terenkripsi terhadap citra aslinya. Sebuah ukuran untuk kualitas enkripsi mungkin dinyatakan sebagai berapa banyak deviasi (perubahan) disebabkan nilai piksel di setiap lokasi pada citra terenkripsi (El-Wahed dkk, 2008).

Pengukuran dilakukan dengan menghitung jumlah piksel dari setiap nilai keabuan dalam jarak dari 0 sampai dengan 255 dan menampilkannya dengan hasil grafis (seperti histogram distribusi), kemudian menghitung perbedaan mutlak (absolut) atau deviasi diantara dua kurva. Langkah terakhir adalah menghitung curva perbedaan absolut, dimana adalah jumlah total deviasi (D) dan ini merepresentasikan kualitas enkripsi (El-Fishawy dan Zaid, 2007).

Parameter Koefisien Korelasi

Analisis statistik seperti faktor koefisien korelasi digunakan untuk mengukur hubungan antara dua variabel, yaitu citra asli dan citra terenkripsi. Faktor ini menunjukkan sejauh mana algoritma enkripsi yang diusulkan melawan serangan statistik. Oleh karena itu, citra terenkripsi harus benar-benar berbeda dari citra asli (Chen, 2004). Persamaan (1) menunjukkan perhitungan koefisien korelasi.

$$Koefisien\ Korelasi = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \quad (1)$$

Dengan E ditunjukkan dengan persamaan (2)

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (2)$$

Dimana x dan y adalah nilai piksel keabuan dari citra asli dan citra terenkripsi.

Parameter Deviasi Ketidakteraturan

Faktor pengukuran kualitas didasarkan pada seberapa banyak deviasi ketidakteraturan (penyimpangan / perubahan) yang disebabkan oleh proses enkripsi pada citra terenkripsi (Elkamchouchi dan Makar, 2005). Menghitung matriks 'D' yang merepresentasikan nilai absolut dari perbedaan diantara nilai piksel citra asli dan citra terenkripsi. Selanjutnya menyajikan dengan distribusi histogram. Langkah berikutnya adalah mengambil rata-rata dari banyaknya piksel yang menyimpang pada setiap nilai deviasi (seperti jumlah piksel pada histogram jika distribusi statistic dari matriks deviasi adalah distribusi keseluruhan). Selanjutnya kurangi rata-rata dari histogram deviasi, kemudian ambil nilai absolut dari hasilnya. Langkah terakhir adalah menghitung area dibawah nilai kurva 'AC' yang mana hasil dari jumlah variasi penyimpangan dari histogram rerata (El-Fishawy dan Zaid, 2007).

Parameter PSNR

PSNR (*Peak Signal to Noise Ratio*) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut (Male dkk, 2012). PSNR menggunakan satuan decibel (dB) dalam pengukuran kualitas, dimana dalam penelitian ini akan dicari nilai PSNR terbesar. Semakin besar nilai PSNR maka kualitas citra hasil rekonstruksi mendekati kualitas citra aslinya (Sukirman dan Subali, 2008).

Data yang digunakan

Data yang dimaksudkan dalam penelitian ini adalah 10 citra diam dengan format .bmp,.png dan .jpg. Ukuran citra yang digunakan bersifat square yaitu panjang dan lebar citra harus sama, contoh 32x32 piksel. Citra yang digunakan adalah citra berfrekuensi tinggi seperti citra Barbara (Elkamchouchi, 2005), citra mengandung area yang besar dari sebuah warna tunggal seperti citra Nike (El-Fishawy dan Zaid, 2007), citra yang mengandung daerah berkualitas tinggi maupun rendah seperti citra Bridge (Larson dan Chandler, 2010), citra yang rumit seperti citra Mandrill (Dung, 1998), citra dengan detail rendah seperti citra Medis (El-Ashry, 2010) dan sisanya citra yang dipilih secara acak dari koleksi pribadi peneliti. Gambar 1 menunjukan 10 citra yang digunakan dalam penelitian ini.


Barbara


Nike


Bridge

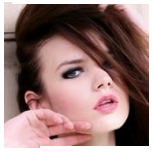

Mandrill


Medis


Fatma


Monica


Nadira


Olga


Xeniya

Gambar 1 Citra yang digunakan

2.3 Perancangan Sistem

Gambaran umum proses enkripsi maupun dekripsi yang digunakan pada penelitian ini seperti pada Gambar 2 dan Gambar 3.

Penentuan algoritma yang terbaik

Berikut adalah penjelasan bagaimana cara mengukur perbandingan berdasarkan masing – masing parameter :

- Big O

[1] Penentuan algoritma terbaik dengan parameter Big O adalah apabila nilai kompleksitasnya berada diurutan atas pada Tabel 1, karena semakin ke bawah urutan algoritma semakin tidak mangkus (efisien).

- Avalanche Effect

[2] Sebuah algoritma yang baik memiliki *Avalanche Effect* tinggi (Ramanjuma dan Karuppiah, 2011).

- Deviasi Maksimum

[3] Semakin besar nilai deviasi maksimumnya maka semakin menyimpang citra terenkripsi dari citra asli.

- Koefisien Korelasi

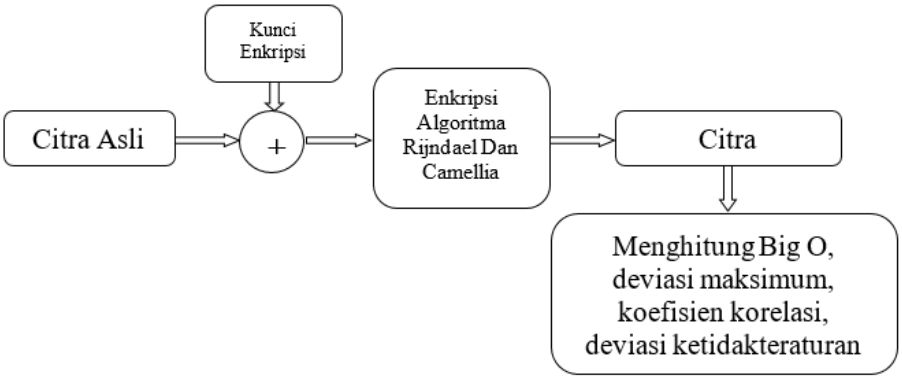
[4] Kesuksesan proses enkripsi berarti mengahasilkan koefisien korelasi yang kecil (El-Fishawy dan Zaid, 2007).

- Deviasi Ketidakteraturan

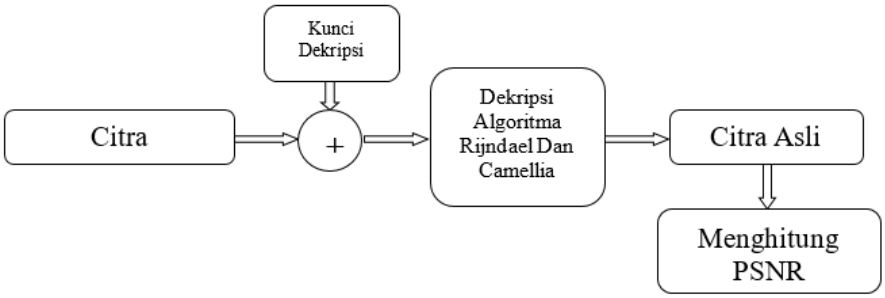
[5] Semakin kecil nilai deviasi ketidakteraturan maka semakin baik algoritma tersebut (El-Fishawy dan Zaid, 2007).

- PSNR

[6] Semakin besar nilai PSNR maka kualitas citra hasil rekonstruksi mendekati kualitas citra aslinya (Sukirman dan Subali, 2008).



Gambar 2 Gambaran umum proses enkripsi



Gambar 3 Gambaran umum proses dekripsi

Tabel 1. Kelompok algoritma berdasarkan kompleksitas waktu asimptotik

Kelompok Algoritma	Nama	Keterangan
O(1)	Konstan	Waktu pelaksanaan algoritma adalah tetap, tidak bergantung pada ukuran masukan
O(log n)	Logaritmik	Algoritma yang termasuk kelompok ini adalah algoritma yang memecahkan persoalan besar dengan mentransformasikannya menjadi beberapa persoalan yang lebih kecil yang berukuran sama
O(n)	Linear	Algoritma yang waktu pelaksanaanya linear. Umumnya terdapat pada kasus yang setipe elemen masukannya dikenai proses yang sama
O(n log n)	n log n	Terdapat pada algoritma yang memecahkan persoalan menjadi beberapa persoalan menjadi yang lebih kecil, menyelesaikan tiap persoalan secara independen dan menggabungkan solusi masing-masing persoalan
$O(n^2)$	Kuadratik	Hanya praktis digunakan untuk persoalan yang berukuran kecil. Umumnya algoritma ini memproses tiap masukan dalam dua buah kalang bersarang
$O(n^3)$	Kubik	Seperti algoritma kuadratik, algoritma kubik memproses setiap masukan dalam tiga buah kalang bersarang
$O(2^n)$	Eksponensial	Algoritma ini mencari solusi persoalan secara “brute force”. Bila n dijadikan dua kali semula, waktu pelaksanaanya menjadi kuadrat kali semula
O(n!)	Faktorial	Algoritma ini memproses setiap masukan dan menghubungkannya dengan n-1 masukan lainnya. Bila n dijadikan dua kali semula, maka waktu pelaksanaan algoritma menjadi faktorial dari 2n

3. Hasil Dan Pembahasan

3.1 Data hasil pengujian proses kriptografi

Pengujian dilakukan berdasarkan metode penelitian yang telah dijelaskan sebelumnya. Berikut adalah hasil pengujian berdasarkan masing – masing parameternya.

Berdasarkan kompleksitas algoritma

Berdasarkan *source code*, maka kompleksitas waktu asimptotik yang terdapat dalam fungsi enkripsi dan dekripsi algoritma Rijndael ditunjukan pada persamaan (3).

$$T(n) = O(1) + O(1) = O(1) \quad (3)$$

Sedangkan kompleksitas waktu asimptotik yang terdapat dalam fungsi enkripsi dan dekripsi algoritma Camellia ditunjukan pada persamaan (4).

$$T(n) = O(n) + O(n) = O(2n) = O(n) \quad (4)$$

Nilai kompleksitas waktu asimptotik Big O pada algoritma Rijndael adalah O(1) dan pada algoritma Camellia adalah O(n). Berdasarkan (Levitin, 2007) maka kedua algoritma adalah konstan, sedangkan algoritma Camellia Linear. Maka algoritma Rijndael lebih efisien dibandingkan algoritma Camellia.

Berdasarkan Avalanche Effect

Pengujian menunjukan bahwa dari 30 citra yang diujikan menghasilkan 60% (18 dari 30) nilai *Avalanche Effect* algoritma Camellia lebih tinggi daripada algoritma Rijndael. Dari perhitungan yang telah dilakukan maka dapat dinyatakan algoritma Camellia lebih efektif daripada algoritma Rijndael.

Berdasarkan deviasi maksimum

Pengujian menunjukan bahwa dari 30 citra yang diujikan menghasilkan 70% (21 dari 30) nilai deviasi maksimum algoritma Rijndael lebih tinggi daripada algoritma Camellia.

Berdasarkan koefisien korelasi

Pengujian menunjukan bahwa dari 30 citra yang diujikan menghasilkan 53,33% (16 dari 30) nilai koefisien korelasi algoritma Rijndael lebih rendah daripada algoritma Camellia.

Berdasarkan deviasi ketidakteraturan

Pengujian menunjukan bahwa dari 30 citra yang diujikan menghasilkan 56,67% (17 dari 30) nilai deviasi ketidakteraturan algoritma Rijndael lebih rendah daripada algoritma Camellia.

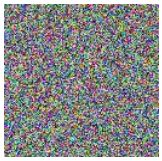
Berdasarkan PSNR

Pengujian menunjukan bahwa dari 30 citra yang diujikan menghasilkan 73,33% (22 dari 30) kemungkinan nilai PSNR algoritma Camellia lebih tinggi daripada algoritma Rijndael.

3.2 Bentuk citra hasil

Citra hasil yang ditunjukan pada proses enkripsi saat pengujian adalah mirip dalam setiap formatnya. Pada Gambar 4 sampai dengan Gambar 6 menunjukan hasil pengujian proses enkripsi dengan algoritma Rijndael dan algoritma Camellia terhadap format .bmp, .jpg , .png.

Gambar 4. Hasil enkripsi untuk format .bmp (kiri algoritma Rijndael, kanan algoritma Camellia)




Gambar 5. Hasil enkripsi untuk format .jpg (kiri algoritma Rijndael, kanan algoritma Camellia)


Gambar 6. Hasil enkripsi untuk format .jpg (kiri algoritma Rijndael, kanan algoritma Camellia)

4. Kesimpulan

Berdasarkan penelitian dan pengujian yang telah dilakukan, maka disimpulkan bahwa: Membandingkan efisiensi, efektifitas dan kualitas algoritma Rijndael dengan algoritma Camellia pada citra digital adalah dengan cara : (a) Menggunakan teori kompleksitas waktu asimptotik Big O sebagai parameter efisiensi; (b) Menggunakan nilai *Avalanche Effect* yang didapat pada saat proses enkripsi kedua algoritma sebagai parameter efektifitas; (c) Menggunakan perhitungan deviasi maksimum, koefisien korelasi, deviasi ketidakteraturan dan PSNR sebagai parameter kualitas.

Hasil perbandingan efisiensi, efektifitas dan kualitasnya adalah : (a) Algoritma Rijndael lebih efisien dibandingkan dengan algoritma Camellia; (b) Algoritma Camellia lebih efektif dibandingkan dengan algoritma Rijndae; (c) Algoritma Rijndael lebih berkualitas dibandingkan dengan algoritma Camellia.

Daftar Pustaka

Anderson, S.D., 2001, Digital Image Analysis : Analytical Framework for Authenticating Digital Images, *Tesis*, University of Colorado Denver.

Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J. dan Tokita, T., 2000, *Specification of Camellia – a 128-bit Block Cipher*, NTT and Mitsubishi Electric Corporation.

Chen, G., Mao, Y. dan Chui, C.K., 2004, A Symmetric image encryption scheme based on 3D chaotic cat maps, *Chaos Solitons and Fractals*, Vol. 21, pp. 749-761.

Daemen, J. dan Rijmen,V., 2001, *AES Proposal : Rijndael*, Katholieke Universiteit Leuven, Belgium.

Dung, L.P., 1998, Perception Based Quality Measure for Image Compression and Transmission, *Thesis*, School of Computer Science and Software Engineering, Monash University, Australia.

El-Ashry, E.I.F., 2010, Digital Image Encryption, *Tesis*, Faculty of Electronic Engineering, Menofia University.

El-Fishawy,N., dan Zaid, O.M.A., 2007, Quality of Encryption Measurement of Bitmap Images with RC6,MRC6 and Rijndael Block Cipher Algorithms, *Int. J. of Network Security*, Vol 5, No.3, PP.241-251.

Elkamchouchi, H. dan Makar, M.A, 2005, Measuring encryption quality of bitmap images encrypted with Rijndael and KAMKAR block ciphers, *Proceedings Twenty second National Radio Science Conference (NRSC 2005)*, pp. C11, Cairo, Egypt.

El-Wahed, M.A., Mesbah, S., dan Shoukry, A., 2008, Efficiency and Security of Some Image Encryption Algorithms, *Proceedings of the World Congress on Engineering*, Vol 1, July 2-4 2008, London.

Engeldrum, P.G., 2000, *Psychometric Sacaling : A Toolkit for Imageing Systems Development*, Imcotek Press, Winchester, USA.

Knuth, D.E., 1997, *The Art of Computer Programming Volume 1: Fundamental Algorithms - Third Edition*, Addison Wesley, USA.

Koshy, T., 2004, *Discrete Mathematics with Applications*, Elsevier Inc, USA.

Larson, E.C. dan Chandler, D.M., 2010, Most Apparent Distortion : Full Reference Image Quality Assesment and the Role of Strategy, *Journal of Electronic Imaging*, Vol 19, No 1.

Levitin, A., 2007, *The Design & Analysis of Algorithm*, Pearson Education Inc, USA.

Male, G.M., Wirawan, dan Setijadi, E., 2012, Analisa Kualitas Citra Pada Steganografi Untuk Aplikasi e-Government, *Prosiding Seminar Nasional Manajemen Teknologi XV*, Institut Teknologi Surabaya, Surabaya.

Mao, W., 2003, *Modern Cryptography : Theory and Practice*, Prentice Hall PTR, New Jersey, USA.

Matsui, M., Nakajima, J. dan Moriai, S., 2004, A Description of the Camellia Encryption Algorithm, *Request For Comments : 3713*.

Nazaruk, V., dan Ruzakov, P., 2010, Implementation of Cryptographic Algorithms in Software: An Analysis of the Effectiveness, *Scientific Journal of Riga Technical University* ,Volume 43, Latvia.

Nugroho, S., 2004, Sistem Pendeteksi Wajah Manusia pada Citra Digital, *Tesis*, Fakultas MIPA, Universitas Gadjah Mada, Yogyakarta.

Raden, B.B.P., 2010, Analisis Penyimpanan Online Dengan Enkripsi Menggunakan Algoritma AES (*Advanced Encryption Standards*), *Skripsi*, Fakultas Elektro dan Telekomunikasi, Institut Teknologi Telkom, Bandung.

Ramanjuma, S., dan Karuppiah, M., 2011, Designing an algorithm with high Avalanche Effect, *International Journal of Computer Science and Network Security*, Vol 11, No 1, India.

Sari, D.M., 2009, Implementasi Enkripsi Dekripsi 128 Bit Menggunakan Algoritma Rijndael Studi Kasus : Aplikasi billing Warung Internet, *Skripsi*, Universitas Kristen Duta Wacana, Yogyakarta.

Sianipar, R.H dan Muliani, S.W.J, 2003, Kompresi Citra Digital Berbasis Wavelet: Tinjauan PSNR Dan Laju Bit, *Jurnal Informatika*, Vol.4.

Sukirman, E., dan Subali, M., 2008, Analisis Perbandingan Kualitas Citra dan Rasio Kompresi Menggunakan Perangkat Lunak JPEG, *Jurnal Matematika dan Komputer*, No. 1, Volume 23, Universitas Diponegoro, Semarang.

Sutoyo, T., Mulyanto, E., Suhartono, V., Nurhayati, O.D. dan Wijanarto, 2009, *Teori Pengolahan Citra Digital*, Penerbit Andi, Yogyakarta.

Wibowo, W.A., 2004, *Advanced Encryption Standard : Algoritma Rijndael*, Tugas akhir Keamanan Sistem Informasi, Institut Teknologi Bandung, Bandung.