Jurnal Computech & Bisnis, Vol. 6, No. 2, Desember 2012, 82-95
ISSN 2442-4943

KRIPTOGRAFI ALGORITMA DES, AES/RIJNDAEL, BLOWFISH UNTUK KEAMANAN CITRA DIGITAL DENGAN MENGGUNAKAN METODE DISCRETE WAVELET TRANSFORMATION (DWT)

Rohmat Nur Ibrahim
STMIK Mardira Indonesia, Bandung
rohmat_nur@stmik-mi.ac.id

Abstract

In the community of information technology users often occur several crimes either consciously or unconsciously, intentionally or unintentionally done. Way to secure data in the form of digital images can use cryptographic technique; cryptography is one of the techniques used to enhance the security aspect of information. Cryptography is the study of science and art to keep a message or data information so that the data is safe. Cryptographic support the needs of the two aspects of information security, namely secrecy (protection of the confidentiality of data information) and authenticity (protection against counterfeiting and alteration of information that is undesirable).
Along with the development of computer technology, the world of information technology requires a stronger cryptographic algorithm and secure. Currently, AES / Rijndael (Advanced Encryption Standard) is used as the newest standard cryptographic algorithms. AES / Rijndael replace the DES (Data Encryption Standard), which in 2002 was over its service life. DES is also considered to be no longer able to answer the challenges of the development of communication technology very quickly. AES / Rijndael itself is a cryptographic algorithm using the algorithm AES / Rijndael to encrypt and decrypt the data block along with a 128-bit key length of 128 bits, 192 bits, or 256 bits. Blowfish is an algorithm that uses a block size of 64 bits of data along with the key length of 448 bits. To produce a digital image pixel values randomly needed a method transpormasi Discrete Wavelet (DWT) to generate a random pixel values before the encryption process. So from this comparison produces research in the form of computation time (Computation Time), average shape error (Mean Squared Error), Total changes in pixel values, Level Number of Pixel Change (NPCR), peak signal to noise ratio (PSNR (dB)).

Keywords: *Digital imagery, Rijndeal, blowfish, Computation Time, Mean Squared Error, Number of Changing Pixel Rate, Peak signal to Noise Ratio*

Abstrak

Dalam masyarakat pengguna teknologi informasi sering terjadi beberapa tindak kejahatan baik yang disadari maupun tidak disadari, disengaja atau tidak sengaja dilakukan. Cara untuk mengamankan data berupa citra digital dapat menggunakan teknik kriptografi, Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu informasi. Kriptografi merupakan kajian ilmu dan seni untuk menjaga suatu pesan atau data informasi agar data tersebut aman. Kriptografi mendukung kebutuhan dari dua aspek keamanan informasi, yaitu *secrecy* (perlindungan terhadap

kerahasiaan data informasi) dan *authenticity* (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan).
Seiring dengan perkembangan teknologi komputer maka dunia teknologi informasi membutuhkan algoritma kriptografi yang lebih kuat dan aman. Saat ini, AES/Rijndael (*Advanced Encryption Standard*) digunakan sebagai standar algoritma kriptografi yang terbaru. AES/Rijndael menggantikan DES (*Data Encryption Standar*) yang pada tahun 2002 sudah berakhir masa penggunaannya. DES juga dianggap tidak mampu lagi untuk menjawab tantangan perkembangan teknologi komunikasi yang sangat cepat. AES/Rijndael sendiri adalah algoritma kriptografi dengan menggunakan algoritma AES/Rijndael yang dapat mengenkripsi dan mendekripsi blok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, atau 256 bit. *Blowfish* adalah algoritma yang menggunakan ukuran blok data sepanjang 64 bit dengan panjang kunci 448 bit. Untuk menghasilkan citra digital yang nilai pixelnya acak dibutuhkan suatu metode Transpormasi Wavelet Diskrit (DWT) untuk menghasilkan nilai pixel yang acak sebelum proses enkripsi. Sehingga dari perbandingan tersebut menghasilkan penelitian berupa Perhitungan waktu (*Computation Time)*, Rata-rata bentuk kesalahan (*Mean Squared Error)*, Jumlah perubahan nilai piksel, Tingkat Jumlah Mengubah Pixel(*NPCR)*, Ratio Puncak sinyal untuk Noise (*PSNR (dB))*.

Kata Kunci: Citra Digital, *Rijndeal, blowfish, Computation Time, Mean Squared Error, Number Of Changing Pixel Rate, Peak signal to Noise Ratio*

1. PENDAHULUAN

Latar Belakang

Citra Digital sering digunakan dalam menyajikan berbagai informasi didalamnya, oleh karena itu citra digital dapat menjadi hal yang penting apabila citra digital tersebut memiliki informasi yang berharga, dan dapat menjadi bersifat pribadi, karena pada dasarnya data informasi berupa citra digital sangat dibutuhkan dibandingkan dari data yang sifatnya teks dan digunakan dalam berbagai bidang seperti keamanan, medis, ilmu, teknik, seni, hiburan, iklan, pendidikan serta pelatihan. Dengan bertambahnya penggunaan teknik digital bagi transmisi dan penyimpanan citra digital, masalah mendasar untuk melindungi kerahasiaan, keutuhan dan keaslian citra digital memang perlu diperhatikan. Hal ini dikarenakan kerahasiaan suatu informasi sangatlah penting dan bersifat pribadi, karena pencurian data, dan serangan terhadap data berupa citra digital yang secara langsung ataupun tidak langsung dapat menimbulkan berbagai permasalahan yang dapat menimbulkan dampak serius terhadap permasalahan ilegal, sosial, dan ekonomi, karena tidak semua informasi yang ada dibuat untuk konsumsi secara umum. Kasus yang sering terjadi adalah rekayasa photo atau pun penyebaran photo secara illegal tentunya hal ini merugikan pemiliknya, sehingga diperlukan suatu pengamanan dari sumber-sumber yang berkepentingan tentunya yang menghasilkan suatu produk berupa citra digital.

Cara untuk mengamankan data berupa citra digital tersebut dapat menggunakan teknik kriptografi, Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu informasi. Kriptografi merupakan kajian ilmu dan seni untuk menjaga suatu pesan atau data informasi agar data tersebut aman. Kriptografi mendukung kebutuhan dari dua aspek keamanan informasi, yaitu *secrecy* (perlindungan terhadap kerahasiaan data informasi) dan *authenticity* (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan).

Algoritma kriptografi yang baik akan memerlukan waktu yang lama untuk memecahkan data yang telah disandikan. Seiring dengan perkembangan teknologi komputer maka dunia teknologi informasi membutuhkan algoritma kriptografi yang lebih kuat dan aman. Saat ini, AES/Rijndael (*Advanced Encryption Standard*) digunakan sebagai standar algoritma kriptografi yang terbaru. AES/Rijndael menggantikan DES (*Data Encryption Standar*) yang pada tahun 2002 sudah berakhir masa penggunaannya. DES juga dianggap tidak mampu lagi untuk menjawab tantangan perkembangan teknologi komunikasi yang sangat cepat. AES/Rijndael sendiri adalah algoritma kriptografi dengan menggunakan algoritma AES/Rijndael yang dapat mengenkripsi dan mendekripsi blok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, atau 256 bit. *Blowfish* adalah algoritma yang menggunakan ukuran blok data sepanjang 64 bit dengan panjang kunci 448 bit. Ketiga model algoritma tersebut yang akan coba penulis ungkap dalam penelitian ini. Sedangkan algoritma yang baik tidak ditentukan oleh kerumitan dalam mengolah data atau pesan yang akan disampaikan.

Untuk menghasilkan citra digital yang nilai pixelnya acak dibutuhkan suatu metode Transpormasi Wavelet Diskrit (DWT) untuk menghasilkan nilai pixel yang acak sebelum proses enkripsi. Transpormasi Wavelet Diskrit (DWT) yang mudah diaplikasikan dan hasilnya akan lebih bagus. Transformasi wavelet diskrit secara umum merupakan dekomposisi citra pada frekuensi subband citra itu sendiri.

Rumusan Masalah

Berdasarkan latar belakang yang ada maka dapat dirumuskan beberapa permasalahan sebagai kajian tesis, diantaranya sebagai berikut :

1. Bagaimana karakteristik Citra Digital yang dapat diterima oleh algoritma DES, AES/Rijndeal dan Blowfish.
2. Bagaimana kinerja masing-masing algoritma DES, AES/Rijndeal dan Blowfish untuk proses enkripsi dan dekripsinya.
3. Bagaimana Transformasi wavelet diskrit yang merupakan dekomposisi citra pada frekuensi subband citra itu sendiri.

Batasan Masalah

Dengan melihat permasalahan di atas maka dengan mempertimbangkan efisiensi penajaman kajian atau fokusnya penelitian pada tesis ini serta keterbatasan waktu yang ada, maka penulis lebih menitik beratkan pada kajian pada :

1. Akan diperoleh berbagai macam karakteristik Citra Digital, sehingga dapat diterima oleh ketiga algoritma (*DES, AES/Rijndael dan Blowfish*).
2. Memperoleh hasil kinerja dari masing-masing algoritma *DES, AES/Rijndeal* dan *Blowfish* untuk proses enkripsi dan dekripsinya sehingga menghasilkan gambaran sesuai harapan.
3. Diharapkan dapat menghasilkan suatu perbandingan kecepatan dan keamanannya sehingga diperoleh perbandingan dari sisi **MSE, NPCR, dan PSNR (dB)**
4. Dengan metode transformasi wavelet diskrit diharapkan proses pengolahan citra digital akan lebih baik dan cepat.
5. Proses pengujian menggunakan perangkat lunak MATLAB7.

Tujuan dan Manfaat Penelitian

Tujuan dari penelitian ini adalah melakukan sebuah kajian dengan membandingkan tiga algoritma des, AES/rijndeal dan blowfish pada proses

enkripsi dan dekripsi terhadap citra digital dengan disertakan proses transpormasi wavelet diskrit untuk mempercepat proses tansformasi citra digital.

Kajian ini diharapkan dapat memberikan informasi secara terinci kepada para pembaca akan peran/fungsi enkripsi citra digital menggunakan tiga algoritma (*DES, AES/ Rijndeal*, dan *Blowfish*) sehingga diketahui keamanan, kecepatan dari masing-masing algoritma tersebut serta ditambahkan tranformasi wavelet diskrit untuk memproses pengolahan citra digital.

Metodologi Penelitian

Metodologi penelitian yang akan diterapkan pada tesis ini terdiri dari dua yaitu metode Deskriptif Analitik yang melakukan pengumpulan data dengan mempelajari, mengamati, studi literatur serta didukung dengan metoda transformasi wavelet diskrit untuk menguji dan menemukan gambaran dari keamanan sistem serta melakukan proses pengujian keamanan dari sisi enkripsi dan dekripsi dari ke tiga algoritma sehingga diharapkan kualitas dari citra digital akan lebih aman.

Metode Pengumpulan Data dan Metode Transformasi

Adapun metode dan langkah-langkah penelitian yang diambil adalah sebagai berikut :

a) Indentifikasi dan perumusan masalah
b) *Theoritical Framework*
c) Observasi
d) Penulisan laporan

Metode Transformasi Wavelet Diskrit

Transformasi *Wavelet* merupakan sebuah fungsi variabel riil t yang digunakan untuk melokalisasi suatu fungsi dalam ruang dan skala *L2(R)*, diberi notasi *ψ(t) sebagai mother wavelet*. Untuk memproses metode tersebut maka tidak terlepas dari 3(tiga) komponen berikut: 1. Transformasi *Wavelet* Diskrit Maju (*Forward DWT*), 2. Transformasi *Wavelet* Diskrit Balik (*Invers DWT*), 3. Pemilihan Filter Wavelet

2. TINJAUAN PUSTAKA

2.1 Citra Digital

Warna adalah respon persepsi dari mata dan otak manusia terhadap pancaran energi berbagai panjang gelombang dan intensitasnya. Pancaran energi tersebut diserap oleh mata dan dipersepsikan oleh otak sebagai warna. Ilmu tentang warna pada dasrnya merupakan karakteristik sensor dari mata. *Citra* adalah kumpulan dari beberapa warna yang diatur sedemikian rupa yang bertujuan untuk menyampaikan suatu informasi. Oleh karena itu warna merupakan komponen yang penting dari suatu *Citra*.

Istilah citra, digunakan untuk menyatakan intensitas cahaya dua dimensi dalam fungsi $f(x,y)$, dimana (x,y) menyatakan koordinat spasial dan nilai dari f pada titik (x,y) menyatakan tingkat kecerahan citra pada titik tersebut. Fungsi $f(x,y)$, dipengaruhi oleh banyaknya sumber cahaya yang jatuh pada daerah yang diamati dan banyaknya sumber cahaya yang dipantulkan oleh objek pada daerah tersebut (refleksi). Hal ini dapat ditulis secara matematis sebagai :

$f(x,y) = i\ (x,y).r\ (x,y)$

dimana :

$0 < i\ (x,y) < 8\ 0 < r\ (x,y) < 1$

jika r (x,y) = 0, maka semua cahaya diserap, sedangkan jika r (x,y) = 1, maka semua cahaya dipantulkan. Bila nilai r (x,y) berada diantara kedua nilai tersebut, makan akan dihasilkan warna yang berbeda.

Citra $f(x,y)$ yang kontinu, dapat dinyatakan sebagai nilai-nilai sampel yang dipisahkan pada jarak sama dan disusun dalam betuk matriks NxM dimana tiap elemen dari matriks menunjukan entitas diskrit. Level keabuan dalam bentuk diskrit terpisah dalam range 0 sampai dengan 225. Suatu citra digital dapat dipandang sebagai array dua dimensi seperti berikut :

Citra digital dapat dipandang

sebagai sebuah matrik yang indeks baris dan kolomnya menyatakan titik pada citra dan elemen matriknya menyatakan level keabuan pada titik tersebut.

Secara prinsip ada 2 jenis metode untuk merepresentasikan *Citra Digital*, yaitu:

1. BitMap/*Raster*
   Sebuah *citra* dibagi menjadi kotak-kotak kecil dimana setiap kotak berisi informasi tentang nilai intensitas yang menunjuk kepada index table warna (*palettes*), kotak-kotak ini disebut sebagi pixel. Posisi dari kotak (*bit*) yang dipresentasikan mrupakan pemetaan sebagian dari citra pada posisi tersebut, oleh karena itu disebut bitmap.
2. *Vektor*
   Sebuah *citra* didekripsikan sebagai sekumpulan garis atau bentuk.

2.2 Konsep Dasar Cryptosystem

Cryptosystem digunakan untuk menjamin privasi dan autentik data dalam sistem komputer dan komunikasi. Message yang tidak diproteksi disebut plaintext. Proses plaintext dibentuk dalam ciphertext dari suatu bentuk yang tidak dapat dipahami yang disebut enkripsi atau *enchiperment*. Sebuah algoritma *dechipering* digunakan untuk dekripsi atau decipherment agar mengembalikan plaintext aslinya. Dalam cryptosystem, sekumpulan parameter yang memilih sebuah transformasi chipering khusus yang disebut sekumpulan key. Enkripsi dan dekripsi dikontrol oleh sebuah key atau beberapa key.

Operasi enkripsi dan dekripsi dijelaskan secara umum sebagai berikut :

$$Y = E_{K_E}(X) \quad \text{(enkripsi)}$$

$$X = D_{K_D}(Y) \quad \text{(dekripsi)}$$

dimana: X = plaintext, Y = chipertext

K_E = key enkripsi, K_D = key dekripsi

2.2 Algoritma Simetrik

Model enkripsi konvensional yang juga disebut algoritma simetrik. Proses enkripsi terdiri dari sebuah algoritma dan sebuah key (kunci). Key adalah sebuah nilai yang bebas dari plaintext yang mengontrol algoritma tersebut. Algoritma akan menghasilkan output yang berbeda tergantung pada key khusus yang digunakan pada waktu tersebut. Merubah key akan merubah output algoritma. Untuk menghasilkan kembali plaintext yang aslinya, kita menggunakan algoritma dekripsi dengan kunci yang sama dengan enkripsi. (Rhee, 1994) Pada gambar 2.1, K_E adalah sama dengan K_D.

2.3 Algoritma Public-Key

Algoritma public-key juga disebut algoritma asymmetric yang dirancang sehingga key yang digunakan untuk enkripsi berbeda dengan key yang digunakan untuk dekripsi. Selanjutnya key dekripsi tidak dapat dihitung dari key enkripsi. Algoritma tersebut disebut public-key karena key enkripsi dapat dibuat secara public. Orang asing dapat menggunakan key enkripsi tersebut untuk mengenkripsi sebuah message, tetapi hanya seorang tertentu dengan key dekripsi sepadan dapat mendekripsi message tersebut. Dalam sistem ini key enkripsi sering disebut public key dan key dekripsi disebut private key.

Enkripsi dengan public key (K) dinotasikan dengan :

$E_K(M) = C$

Dan didekripsi dengan private key dengan notasi sebagai berikut:

$D_K(C) = M$

Kadang-kadang message akan dienkripsi dengan private key dan didekripsi dengan public key, seperti yang digunakan dalam digital signatures. (Rhee, 1994)

2.4 Algoritma Data Encryption Standard (DES)

DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis *cipher* blok. DES beroperasi pada

ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (*internal key*) atau up-kunci (*subkey*). Kunci internal dibangkitkan dari kunci eksternal (*external key*) yang panjangnya 64 bit. Skema global dari algoritma DES adalah sebagai berikut:

1. Blok plainteks dipermutasi dengan matriks permutasi awal (*initial permutation* atau IP).
2. Hasil permutasi awal kemudian di-*enciphering*- sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
3. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (*invers initial permutation* atau IP^{-1}) menjadi blok cipherteks.

Di dalam proses *enciphering*, blok plainteks terbagi menjadi dua bagian, kiri (*L*) dan kanan (*R*), yang masing-masing panjangnya 32 bit. Kedua bagian ini masuk ke dalam 16 putaran DES. Pada setiap putaran *i*, blok *R* merupakan masukan untuk fungsi transformasi yang disebut *f*. Pada fungsi *f*, blok *R* dikombinasikan dengan kunci internal K_i. Keluaran dai fungsi *f* di-XOR-kan dengan blok *L* untuk mendapatkan blok *R* yang baru. Sedangkan blok *L* yang baru langsung diambil dari blok *R* sebelumnya. Ini adalah satu putaran DES.

a. Enciphering

Proses *enciphering* terhadap blok plainteks dilakukan setelah permutasi awal (lihat Gambar 2.2). Setiap blok plainteks mengalami 16 kali putaran *enciphering*. Setiap putaran *enciphering* merupakan jaringan Feistel yang secara matematis dinyatakan sebagai:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

E adalah fungsi ekspansi yang memperluas blok R_{i-1} yang panjangnya 32-bit menjadi blok 48 bit. Fungsi ekspansi direalisasikan dengan matriks permutasi ekspansi sebagai berikut:

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Selanjutnya, hasil ekpansi, yaitu $E(R_{i-1})$, yang panjangnya 48 bit di-XOR-kan dengan K_i yang panjangnya 48 bit menghasilkan vektor *A* yang panjangnya 48-bit:

$$E(R_{i-1}) \oplus K_i = A$$

Vektor *A* dikelompokkan menjadi 8 kelompok, masing-masing 6 bit, dan menjadi masukan bagi proses substitusi. Proses substitusi dilakukan dengan menggunakan delapan buah kotak-S (*S-box*), S_1 sampai S_8. Setiap kotak-S menerima masukan 6 bit dan menghasilkan keluaran 4 bit. Kelompok 6-bit pertama menggunakan S_1, kelompok 6-bit kedua menggunakan S_2, dan seterusnya.

b. Dekripsi

Proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah $K_1, K_2, \ldots, K_{16}$, maka pada proses dekripsi urutan kunci yang digunakan adalah $K_{16}, K_{15}, \ldots, K_1$. Untuk tiap putaran 16, 15, …, 1, keluaran pada setiap putaran *deciphering* adalah :

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

Dalam hal ini, (R_{16}, L_{16}) adalah blok masukan awal untuk deciphering. Blok (R_{16}, L_{16}) diperoleh dengan mempermutasikan cipherteks dengan matriks permutasi IP^{-1}. Pra-keluaran dari *deciphering* adalah adalah (L_0, R_0). Dengan permutasi awal IP akan didapatkan kembali blok plainteks

semula. Tinjau kembali proses pembangkitan kunci internal. Selama *deciphering*, K_{16} dihasilkan dari (C_{16}, D_{16}) dengan permutasi PC-2. Tentu saja (C_{16}, D_{16}) tidak dapat diperoleh langsung pada permulaan *deciphering*. Tetapi karena (C_{16}, D_{16}) = (C_0, D_0), maka K_{16} dapat dihasilkan dari (C_0, D_0) tanpa perlu lagi melakukan pergeseran bit. Catatlah bahwa (C_0, D_0) yang merupakan bit-bit dari kunci eksternal *K* yang diberikan pengguna pada waktu dekripsi. Selanjutnya, K_{15} dihasilkan dari (C_{15}, D_{15}) yang mana (C_{15}, D_{15}) diperoleh dengan menggeser C_{16} (yang sama dengan C_0) dan D_{16} (yang sama dengan C_0) satu bit ke kanan. Sisanya, K_{14} sampai K_1 dihasilkan dari (C_{14}, D_{14}) sampai (C_1, D_1). Catatlah bahwa (C_{i-1}, D_{i-1}) diperoleh dengan menggeser C_i dan D_i dengan cara yang sama, tetapi pergeseran kiri (*left shift*) diganti menjadi pergeseran kanan (*right shift*).

2.5 Algoritma Blowfish

2.6.1 Enkripsi Algoritma Blowfish

Blowfish adalah cipher blok 64-bit yang memiliki sebuah kunci yang panjangnya variabel. Algoritma blowfish terdiri dari dua bagian yaitu key expansion dan enkripsi data. Key expansion mengkonversikan sebuah kunci sampai 448 bit ke dalam beberapa array subkey dengan total 4168 byte.

2.6.2 Dekripsi Algoritma Blowfish

Dekripsi sama persis dengan enkripsi (Ariyus, 2008), kecuali bahwa P_1, P_2,…, P_{18} digunakan pada urutan yang berbalik (*reverse*). (Schneier, 1996) Dengan membalikkan 18 subkey untuk medekripsi metode algoritma Blowfish. Pertama, masalah ini nampak tidak dapat dipercaya, karena ada dua XOR operasi yang mengikuti pemakaian f-fungsi yang sebelumnya, dan hanya satu yang sebelumnya pemakaian pertama f-fungsi. Meskipun jika kita memodifikasi algoritma tersebut sehingga pemakaian subkey 2 sampai 17 menempatkan sebelum output f-fungsi yang di-XOR-kan ke sebelah kanan blok dan dilakukan ke data yang sama sebelum XOR itu, walaupun itu berarti ia sekarang berada di sebelah kanan blok, karena XOR subkey tersebut telah dipindahkan sebelum swap (tukar) kedua belah blok tersebut (tukar separuh blok kiri dan separuh blok kanan). Kita tidak merubah suatu apapun karena informasi yang sama di-XOR-kan ke separuh blok kiri antara setiap waktu, informasi ini digunakan sebagai input f-fungsi. Kenyataannya, kita mempunyai kebalikan yang pasti dari barisan dekripsi. (William, 2003)

2.6.3 Membangkitkan Subkey (Generating the Subkeys)

Subkey dihitung menggunakan algoritma Blowfish. Metode (Ariyus, 2008) yang pasti sebagai berikut (Johansson, 2001) :

1. Pertama inisial P-array dan kemudian S-boxes, agar mempunyai string yang tetap. String ini terdiri dari digit hexadesimal pi (kurang inisial 3). Contoh :
   P1 = 0x243f6a88
   P2 = 0x85a308d3
   P3 = 0x13198a2e
   P4 = 0x03707344
2. XOR P1 dengan 32 bit key pertama, XOR P2 dengan 32 - bit key yang kedua dan seterusnya untuk semua bit key (mungkin sampai P14). Siklus yang berulang melalui key bit sampai semua P-array yang telah di-XOR-kan dengan key bit. (Untuk setiap key yang pendek, maka ada paling sedikit satu key ekivalen yang panjang; contoh jika A adalah 64-bit key maka kemudian AA, AAA, dan lain-lain adalah key yang ekivalen).
3. Enkripsikan string all-zero dengan algoritma blowfish menggunakan subkey yang dijelaskan pada langkah 1 dan langkah 2.
4. Gantikan P1 dan P2 dengan output langkah 3.

5. Enkripsikan output langkah 3 menggunakan algoritma Blowfish dengan subkey yang termodifikasi.
6. Gantikan P3 dan P4 dengan output langkah 5.
7. Teruskan proses tersebut, gantikan semua entry P-array, dan kemudian semua empat S-boxes supaya mempunyai output algoritma Blowfish secara kontinyu berubah (*continuously-changing*).

Total iterasi 521 dibutuhkan untu membangkitkan semua subkey yang diinginkan dari pada mengeksekusi proses turunan ini beberapa kali. (Kurniawan, 2004)

2.7 Algoritma AES (*Advanced Encryption Standard*)/Rijndael

a. *Representasi Data*

Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau *plaintext* yang nantinya akan dienkripsi menjadi *ciphertext*. *Cipher key* dari AES terdiri dari *key* dengan panjang 128 bit, 192 bit, atau 256 bit. Urutan bit diberi nomor urut dari 0 sampai dengan n-1 dimana n adalah nomor urutan. Urutan data 8 bit secara berurutan disebut sebagai byte dimana byte ini adalah unit dasar dari operasi yang akan dilakukan pada blok data.

b. Enkripsi

Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dikopikan ke dalam *state* akan mengalami transformasi byte AddRoundKey. Setelah itu, *state* akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak *Nr*. Proses ini dalam algoritma AES disebut sebagai *round function*. *Round* yang terakhir agak berbeda dengan *round-round* sebelumnya dimana pada *round* terakhir, *state* tidak mengalami transformasi MixColumns.

c. Dekripsi

Transformasi *cipher* dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers *cipher* adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Algoritma dekripsi dapat dilihat pada skema berikut ini :

2.8 Metode Wavelet Diskrit

Realisasi fusi citra digunakan untuk mengekstrak informasi (*detail*) dari setiap sumber citra dan memperoleh demonstrasi efektif dalam fusi citra akhir. Menurut teori umum pengolahan citra, informasi citra (detail) dapat disimpulkan dalam citra komponen frekuensi tinggi, oleh karena itu, titik kunci dari penelitian fusi citra adalah untuk mencari metode pengolahan informasi yang sesuai untuk menggabungkan detail sumber citra masing-masing, yaitu, bagaimana informasi yang akan menyatu diproses secara efektif dalam pita frekuensi yang sesuai.

Transformasi wavelet diskrit (*DWT*) dekomposisi di mana filter dirancang khusus sehingga lapisan berturut-turut piramida hanya mencakup rincian yang belum tersedia di tingkat sebelumnya. *DWT* menggunakan *low-pass* dan *high-pass filter* bertingkat khusus dan *sub-sampling* operasi.

Berikut adalah contoh integrasi dua citra dan perpaduan beberapa citra yang dapat disimpulkan. A dan B adalah citra asli yang harus diproses, F adalah citra hasil fusi. Proses umum adalah sebagai berikut:

1. Melakukan transformasi wavelet diskrit pada citra masing-masing untuk menciptakan dekomposisi wavelet.
2. Gabungkan setiap tingkat dekomposisi secara individual dengan

menggunakan operator yang berbeda untuk berbagai fusi komponen frekuensi dan akhirnya mendapatkan wavelet piramida setelah proses penggabungan.

3. Melakukan invers transformasi wavelet diskrit pada wavelet piramida, yang dilakukan untuk merekonstruksi citra, yang mana citra yang direkonstruksi merupakan citra fusi F.

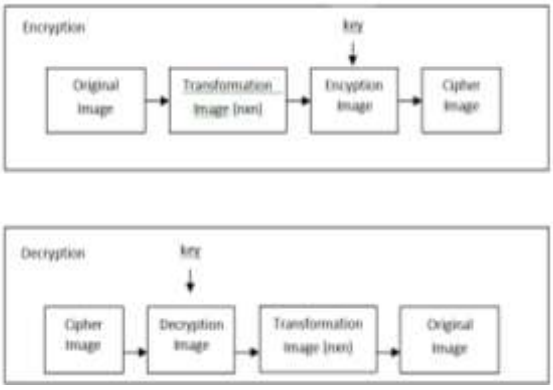
2.9 Kerangka Pemikiran

1. (Soni, Agrawal, & Sharma, 2012), masing-masing algoritma mempunyai kekuatan sendiri dan kelemahan, sehingga hasil perbandingan algoritma tersebut bahwa algoritma DES dari sisi keamanan 'terbukti tidak memadai' , perlawanan kiptaanalisis 'rentan terhadap diferensial dan linier pada saat pembacaan sandi, table substitusi lemah' sedang untuk algoritma AES dari sisi keamanan 'dianggap aman' dan perlawanan kriptaanalisis 'kuat terhadap diferensial, diferensial terpotong, linear, interpolasi. Serta menghasilkan a. Perhitungan Waktu, Rata-rata bentuk kesalahan, NPCR(*Number Of Changing Pixel Rate)*, PSNR dB(*Peak Signal to Noise to NoiseRatio, UNAIC(Unified Average Changed Intensity*).

2. "*Comparison Of Data Encryption Algorithms*" (Singh & Maini, 2011), apabila disimpulkan yang bisa diambil dari jurnal internasional tersebut adalah algoritma enkripsi kriptografi AES, DES, Blowfish dan TripleDES dimana ditujukan untuk menangani keamanan dari pencurian data sehingga dihasilkan kecepatan baik dari sisi enkripsi dan dekripsinya, kemudian dihitung dengan membagi total plaintext dalam Megabyte dengan mempertimbangkan berbagai ukuran blok data.

3. METODE PENELITIAN

Metode yang dilakukan dengan kaidah proses penelitian yang lazim digunakan misalnya metodologi penelitian yang meliputi langkah-langkah penelitian, pengumpulan data dan hasil terpokus pada pokok permasalahan yang ada, metode tersebut meliputi pengelompokkan data dan kelayakan, sehingga menghasilkan pembahasan dengan pemecahan masalah, serta kesulitan-kesulitan apa yang didapatkan selama melakukan tahapan-tahapan penelitian tersebut. Proses umum dari proses enkripsi dan dekripsi gambar pada penelitian ini akan dijelaskan secara garis besar pada Gambar 1.



Gambar 1 Proses Umum Enkripsi dan Dekripsi

Gambar 1 dijelaskan bagaimana alur proses yang berjalan dan algoritma yang digunakan untuk mengenkripsi dan dekripsi gambar. Proses enkripsi dimulai dari memasukkan *original image* ke dalam sistem kemudian masuk ke proses berikutnya yaitu proses *transformation image*. Proses ini membagi dan memecah-mecah gambar menjadi beberapa blok yang berukuran n (n x n). Nilai dari n ditentukan sesuai dengan inputan sistem. Semakin kecil ukuran blok atau ukuran n, maka akan semakin acak nilai hasil enkripsinya. Setelah dibagi menjadi beberapa blok langkah berikutnya adalah proses menyandikan nilai dari setiap blok melalui proses enkripsi dengan nilai *key* yang ditentukan sebelumnya oleh *user*. Nilai *key* untuk proses enkripsi pada setiap blok menggunakan *key* yang sama. Nilai akhir dari proses enkripsi menghasilkan dokumen *cipher image.* Dokumen ini berupa file gambar yang terenkripsi. Gambar yang telah di enkripsi agar dapat kembali menjadi gambar

asli/*original image* harus melalui proses dekripsi. Langkah pertama dari proses dekripsi yaitu memasukkan *cipher image* ke dalam sistem. Setelah itu *cipher image* di bagi ke dalam beberapa blok dan setiap blok di dekripsi menggunakan kunci yang sama dengan proses enkripsi. Hasil akhir dari proses dekripsi akan menghasilkan dokumen yang baru atau *original image*.

Analisis Proses Enkripsi

Enkripsi merupakan proses untuk menyandikan plain cirta digital menjadi cipher citra digital. Gambaran proses enkripsi dapt dilihat pada gambar dibawah ini:

Gambar 2 : Proses Enkripsi

4. PEMBAHASAN DAN EVALUASI KINERJA

Pembahasan

Kriprografi algoritma DES, AES/RIJNDAEL dan BLOWFISH merupakan tahap awal pemilihan algoritma yang memiliki perbandingan, karakteristik dan proses citra digital pada algoritma DES, AES/RIJNDAEL dan BLOWFISH sebagai berikut:

Perbandingan Antara Des, AES/Rijndael dan Blowfish

Pada tabel di bawah merupakan studi banding antara Des, Aes/Rijndael dan Blowfish disajikan dalam sembilan faktor diantaranya: Panjang Kunci, Jenis Chiper, Ukuran Blok, Dikembangkan, Resistensi Pembacaan Sandi, Keamanan, Kunci Kemungkinan, Kemungkinan Kunci Karakter yang dapat dicetak kode ASCII, Waktu yang diperlukan untuk memeriksa semua kunci yang mungkin.

Tabel 1 : PERBANDINGAN ANTARA AES/RIJNDEAL, DES dan BLOWFISH **(Rinaldi, 2006) dan (Soni, Agrawal, & Sharma, 2012)**

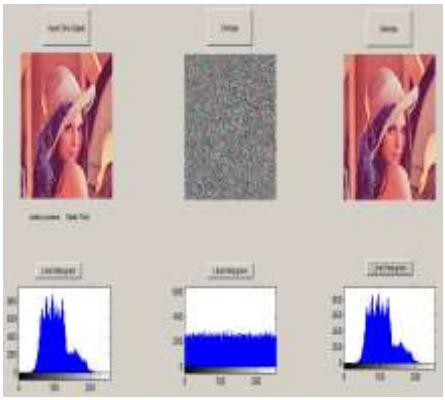
Faktor	DES	AES/RIJNDEAL	BLOWFISH
Panjang Kunci	Menggunakan 56 *bits* Kunci	Menggunakan 128, 192, atau 256 *bits* Kunci	Menggunakan 448 *bit* Kunci
Panjang Blok	64 bits Kunci	128, 192, atau 256 *bits* Kunci	64 bits Kunci
Chiper Teks	Simetrik Blok Chiper	Simetrik Blok Chiper	Simetrik Blok Chiper
Pengembang	1977	2000	2008
Keamanan	Terbukti tidak memadai	Dianggap Aman	Dianggap Paling Aman
Perlawanan Kriptaanalisis	Rentan terhadap diferensial dan linier pembacaan sandi, table substitusi lemah	Kuat terhadap diferensial, diferensial terpotong, linier, interpolasi dan serangan persegi	Blowfish dapat diandalkan keamanannya karena belum dapat dibongkar (*broken*) oleh *Cryptoanalyst* manapun sampai saat ini karena tidak mempunyai kelemahan yang berarti untuk dapat dibongkar sehingga pesan yang ada dalam ciphertextnya sangat aman
Kemungkinan Kunci	2^{56}	2^{128}, 2^{192}, and 2^{256}	2^{448}
Kemungkinan cetak karakter kunci ASCII	957	95^{16}, 95^{24}, or 95^{32}	2^{56}

Mengapa peneliti memilih algoritma DES, AES/RIJNDAEL dan BLOWFISH disesuikan dengan hasil tabel 1 diatas, adapun penelitian yang akan penulis kembangkan yaitu dengan penambahan pada citra digitalnya dengan pengamanan kuncinya menggunakan ketiga algoritma tersebut di atas.

Pada penelitan ini menggunakan citra digital yaitu citra 8 bit (28= 256 warna), dari warna hitam yang bernilai 0 hingga warna putih.yang bernilai 255, yang artinya setiap nilai piksel akan dikodekan menjadi 8 bit yakni : 00000000 = 0 (hitam) hingga 11111111 = 255 (hitam) Contoh. Suatu citra grayscale 4 bit (24=16 warna) dengan size 5x5 piksel. Penelitian ini akan meneliti tentang unjuk kerja dari proses

enkripsi dan dekripsi citra digital dengan menggunakan transformasi wavelet diskrit (DWT) untuk menghasilkan subband-subband dekomposisi, kemudian citra rekontruksi didapat dari proses transformasi balik (IDWT). Citra rekontruksi dapat disimpan atau dapat itransmisikan. Parameter yang banyak digunakan dalam penelitian ini adalah ditinjau dari proses enkripsi dan dekripsi, PSNR (*Peak Signal to Noise Ratio*), dan MSE (*Mean Square Error*) pada citra digital, dari hasil program Matlab 7.0.

a. Karakteristik Citra Digital algoritma DES



Gambar 3 : Citra Lena.jpg

Hasil pengujian dari algoritma DES

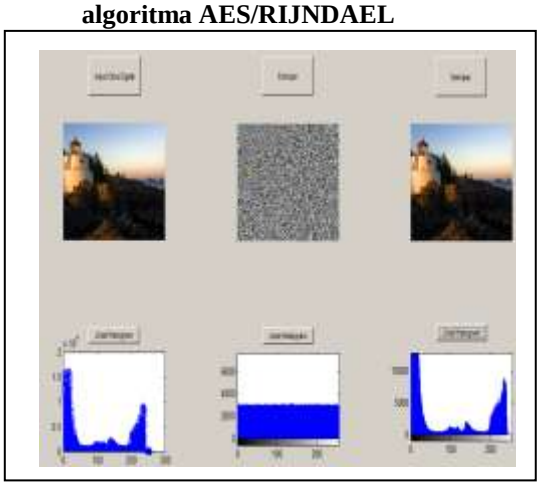
1. Besar file Lena.Jpg : 19.9 KB (20,401 Byte)
2. Waktu Awal Proses : 0.8147
3. Waktu Akhir Proses : 0.9058
4. MSE : 8.8394e+03
5. PSNR(dB) : 8.6666

Tabel 2 : Hasil Enkripsi dan Dekripsi Algoritma DES

Nama Gambar	Waktu Awal Proses	Waktu Akhir Proses	MSE	PSNR (dB)
Lena.JPG 19.9 KB (20,401 Byte)	0.1576	0.9706	8.8394e+03	8.6666
Koala.JPG 762 KB (780,831 bytes)	0.8003	0.1419	9.4562e+03	8.3737
JellyFish.JPG	0.4218	0.5469	1.4471e+04	6.5259
19.9 KB (20,401 Byte)				
Lighthouse.JPG 548KB(561,276bytes)	0.7922	0.9649	1.4752e+04	6.4423

Untuk ukuran citra Jenis gambar **Lena.JPG** dan **Koala.JPG** mempunyai kecepatan waktu awal proses=0.8147

b. Karakteristik Citra Digital algoritma AES/RIJNDAEL



Gambar 4 : Lighthouse.jpg

Nama Gambar	Waktu Awal Proses	Waktu Akhir Proses	MSE	PSNR (dB)
Lena.JPG 19.9 KB (20,401 Byte)	0.1576	0.9706	8.8394e+03	8.6666
Koala.JPG 762 KB (780,831 bytes)	0.8003	0.1419	9.4562e+03	8.3737
JellyFish.JPG 19.9 KB (20,401 Byte)	0.4218	0.5469	1.4471e+04	6.5259
Lighthouse.JPG 548KB(561,276bytes)	0.7922	0.9649	1.4752e+04	6.4423

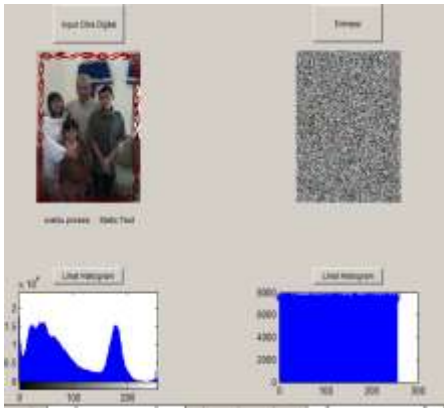
Waktu akhir proses= 0.9058 sama, yang membedakan untuk nilai **MSE** dan ***PSNR(dB)***, sedangkan untuk gambar **JellyFish.JPG** dan **Lighthouse.JPG** masing-masing mempunyai kecepatan yang relatif berbeda untuk (Waktu Proses, Waktu Akhir Proses, MSE dan PSNR(dB).

Hasil pengujian dari algoritma AES/RIJNDAEL

1. Besar file Ligtthouse.Jpg :548KB(561,276bytes
2. Waktu Awal Proses : 0.7922
3. Waktu Akhir Proses : 0.9649
4. MSE : 1.4752e+04
5. PSNR(dB) : 6.4423

Pada Gambar 5 untuk hasil proses Algoritma AES/RIJNDAEL menghasilkan pengujian untuk masing-masing gambar yang terangkum dalam tabel berikut:

c. Karakteristik Citra Digital algoritma BLOWFISH



Hasil pengujian dari algoritma BLOWFISH

1. Besar file Rohmat.Jpg : 420 KB (430,386 bytes)
2. Waktu Awal Proses : 0.6787
3. Waktu Akhir Proses : 0.7577
4. MSE : 1.0937e+04
5. PSNR(dB) : 7.7417

Pada Gambar untuk hasil proses Algoritma **BLOWFISH** menghasilkan pengujian untuk masing-masing gambar yang terangkum dalam tabel berikut:

Tabel 4 Hasil Enkripsi dan Dekripsi Algoritma BLOWFISH

Nama Gambar	Waktu Awal Proses	Waktu Akhir Proses	MSE	PSNR (dB)
Rohmat.Jpg: 420 KB (430,386 bytes)	0.6787	0.7577	1.0937 e+04	7.7417
Tulip.Jpg : 762 KB (780,831 bytes)	0.6555	0.1712	1.3923 e+04	6.6934
JellyFish.JPG :19.9 KB (20,401 Byte)	0.4218	0.5469	1.4471 e+04	6.5259
Lighthouse.JPG : 548KB(561,276 bytes)	0.7922	0.9649	1.4752 e+04	6.4423

Untuk ukuran citra Jenis gambar 4 **Rohmat.JPG**, **Tulip.JPG, JellyFish.JPG,** dan **Lighthouse.JPG** masing-masing mempunyai kecepatan yang relatif berbeda untuk (Waktu Proses, Waktu Akhir Proses, MSE dan PSNR(dB)).

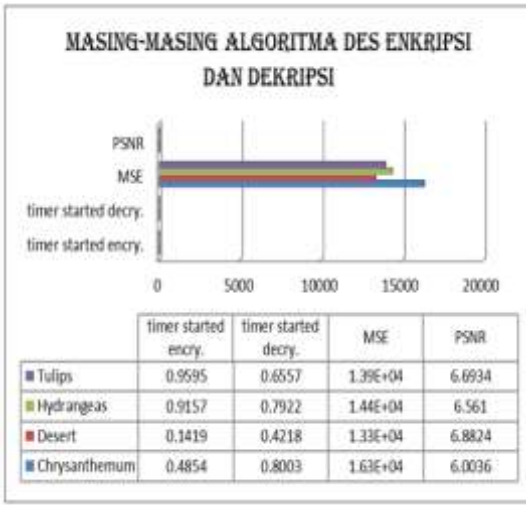
Evaluasi Kinerja

Evaluasi kinerja di sini menunjukkan contoh gambar lain dan grafik dari masing-masing enkripsi dan dekripsi dari mulai algoritma DES, AES/RIJNDAEL dan BLOWFISH dengan menunjukkan formulasi (*timer started encryption, timer starte decryption, MSE and PSNR*) dengan menampilkan tabel dan Gambar berikut:

Tabel 4 Hasil Analisis Enkripsi dan Dekripsi dari Algoritma DES

Tabel 4 Masing-masing Algoritma DES Enkripsi dan Dekripsi

Nama Gambar	timer started encryp.	timer started decry.	MSE	PSNR
Chrysanthemum	0.4854	0.8003	1.63E+04	6.0036
Desert	0.1419	0.4218	1.33E+04	6.8824
Hydrangeas	0.9157	0.7922	1.44E+04	6.561
Tulips	0.9595	0.6557	1.39E+04	6.6934



	timer started encry.	timer started decry.	MSE	PSNR
Tulips	0.9595	0.6557	1.39E+04	6.6934
Hydrangeas	0.9157	0.7922	1.44E+04	6.561
Desert	0.1419	0.4218	1.33E+04	6.8824
Chrysanthemum	0.4854	0.8003	1.63E+04	6.0036

Gambar 7 Menunjukkan Grafik Enkripsi dan Dekripsi dari Algoritma DES

Pada tabel 4 dan gambar 7 diatas menunjukkan bahwa waktu proses enkripsi, dekripsi, *Mean Square Error* dan *Peak Signal to Noise Ratio* menunjukkan perbedaan pada saat awal dan akhir proses.

5. KESIMPULAN

Hasil akhir dari penelitian ini diperoleh beberapa hal yang berkenaan dengan proses penelitian yang terdiri dari, seperti terangkum diantarnya:

1. Sistem yang dibangun untuk pengamanan citra digital menggunakan kriptografi *Algoritma Des, Blowfish dan Rijndael* dapat mengenkripsi dan mendekripsi citra digital, terbukti menghasilkan beberapa karakteristik dari mulai kecepatan proses, MSE, NPCR dan PSNR (dB).
2. Untuk proses pengacakan citra digital dengan menggunakan Metode Transformasi Wavelet Diskrit sehingga proses tersebut menghasilkan pengolahan dan pengacakan dari sisi piksel lebih cepat.
3. Tahapan *processing* Citra Digital yang digunakan dapat menghasilkan proses enkripsi dan dekripsi yang sesuai dengan yang diharapkan baik dari segi *input* maupun *output*, hal ini dikarenakan selain dari variasi kunci yang dimasukan.
4. Sistem pengamanan citra digital yang dibuat belum dapat sepenuhnya memenuhi kebutuhan pengguna sistem dalam merahasiakan *file* berupa *image* secara aman dengan memberikan kombinasi dan variasi kunci yang digunakan. Semakin banyak variasi kunci yang digunakan semakin baik pula hasil dari enkripsi dan dekripsi yang didapatkan.
5. Dukungan aplikasi Matlab mempermudah pada saat melakukan beberapa rumus matematika sehingga tidak menyulitkan bagi pengguna. Walaupun masih banyak aplikasi pendukung lainnya untuk dikembangkan selanjutnya.

REFERENSI

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi, Teori, Analisis dan implementasi.* Yogyakarta: Andi Offset.

Johansson, K. (2001). *A short summary of Blowfish Algoritm: Descryption of a New Variable-Lenght Key, 64/128-Bit Block Cipher (Blowfish) by Bruce Schneier.* Retrieved from http://www.finecrypt.net/bloefish encryption algoritm.html

Kurniawan, Y. (2004). *Kriptografi Keamanan Internet dan Jaringan Telekomunikasi.* Bandung: Informatika.

Rhee, M. Y. (1994). *Cruptography and Secure Communications.*

Singapore: MCGraw-Hill Book Co.

Rinaldi, M. (2006). Retrieved from www.informatika.org/~rinaldi/Kriptografi/2010.../kripto10-11.htm

Schneier, B. (1996). *Applied Cryptoghraphy: Protocols, Algorithms, and Source Code in C.* USA: John Willey & Sons, Inc.

Singh, S. P., & Maini, R. (2011). Comparison of Data Encryption Algorithm. *International Journal of Computer Science and Communication , 2* (1), 125-127.

Soni, S., Agrawal, H., & Sharma, M. (2012). Analysis and Comparison Betwen AES and DES Cryptographic Algorithm. *International Journal of Engineering and Innovative Technolgy , 2* (6).

William, S. (2003). *Cryptography and Network Security*. Principle and Practice.