PROGRAM APLIKASI KEAMANAN CITRA DENGAN ALGORITMA *DES* DAN TRANSFORMASI *WAVELET* DISKRIT

Tesis

untuk memenuhi sebagian persyaratan

mencapai derajat sarjana S-2

Program Studi Magister Sistem Informasi

Oleh:

Solichin Zaki

J4F008028

PROGRAM PASCA SARJANA

UNIVERSITAS DIPONEGORO

SEMARANG

2011

Tesis

PROGRAM APLIKASI KEAMANAN CITRA DENGAN
ALGORITMA DES DAN TRANSFORMASI WAVELET DISKRIT

Oleh:

Solichin Zaki

J4F008028

telah dipertahankan di depan Dewan Penguji pada tanggal :

Penguji I	Penguji II
Prof. Drs. Mustafid, M.Eng, Ph.D	Drs. Suhartono, M.Kom
NIP. 195505281980031002	NIP. 195504071983031003
Pembimbing I	**Pembimbing II**
Drs. Bayu Surarso, M.Sc,Ph.D	**Drs. Eko Adi Sarwoko, M.Kom**
NIP. 196311051988031001	**NIP. 196511071992031003**

Mengetahui :

Ketua Program Studi

Magister Sistem Informasi

Prof. Drs. Mustafid, M.Eng, Ph.D

NIP. 19550528198003100

PERNYATAAN

Dengan ini saya menyatakan bahwa, dalam tesis ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan pada sebuah perguruan tinggi dan sepanjang pengetahuan saya, tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Semarang, 20 Juni 2011

Penulis

Solichin Zaki

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang telah memberikan rahmat dan hidayahNya, sehingga tesis yang berjudul Program Aplikasi Keamanan Citra Dengan Algoritma *DES* dan Transformasi *Wavelet* Diskrit ini dapat diselesaikan. Tesis ini disusun sebagai syarat untuk menyelesaikan studi dan memperoleh gelar kesarjanaan S2 Program Magister Sistem Informasi pada Fakultas Pasca Sarjana Universitas Diponegoro. Pada kempatan ini penulis mengucapkan terima kasih kepada:

1. Prof. Drs. Mustafid, M.Eng, Ph.D selaku Ketua Program Studi Magister Sistem Informasi Fakultas Pasca Sarjana UNDIP.
2. Drs. Bayu Surarso, M.Sc, Ph.D selaku dosen pembimbing I yang telah membimbing dan mengarahkan penulis sehingga selesainya tesis ini.
3. Drs. Eko Adi Sarwoko, M.Kom selaku dosen pembimbing II yang telah membimbing dan mengarahkan penulis sehingga selesainya tesis ini.
4. Para Dosen Penguji Tesis ini dan Semua Dosen Pengajar Program Studi Magister Sistem Informasi Fakultas Pasca Sarjana UNDIP.
5. Semua tenaga administrasi Program Studi Magister Sistem Informasi Fakultas Pasca Sarjana UNDIP dan teman-teman yang telah membantu sehingga terselesaikannya tesis ini.

Semarang, Juni 2011

Penulis

DAFTAR ISI

Daftar Gambar

Daftar Tabel

ABSTRAK

Pada saat ini teknologi informasi telah menyediakan layanan seperti *Multimedia Messaging Service* bagi pengguna Internet untuk melakukan pertukaran informasi. Pertukaran Informasi melalui internet tidak hanya berupa teks, tetapi dapat juga berupa gambar , *audio* dan *video.* Dampak negatif yang timbul dari pesatnya perkembangan teknologi informasi, yaitu kejahatan komputer antara lain pencurian, penipuan pemerasan dan lainya yang menimbulkan pertukaran informasi tidak aman. Salah satu cara untuk melindungi informasi dari kejahatan adalah dengan menggunakan kriptografi.

Tesis ini membuat program aplikasi keamanan citra dengan ekstensi **.jpg, *.png, *.tif* dan **.bmp* menggunakan Matlab 7.1. Langkah-langkah yang dilakukan: pertama, citra ditransformasikan kebentuk citra terkompresi dengan menggunakan transformasi wavelet diskrit dan filter Haar, kedua dengan kunci tertentu melakukan enkripsi citra hasil transfomasi menggunakan algoritma *DES.* Citra hasil enkripsi berupa informasi yang berbentuk *chipertext* yang secara kasat mata tidak jelas objeknya, aman untuk disimpan maupun dipertukarkan. Selanjutnya untuk mengembalikan chipertext kebentuk citra awal, dengan langkah-langkah: pertama, dengan kunci yang sama melakukan dekripsi *chipertext* citra hasil enkripsi menggunakan algoritma *DES,* kedua mengembalikan citra hasil dekripsi kebentuk citra awal dengan menggunakan trasformasi *wavelet* balikan. Selanjutnya dari proses *DWT*, enkripsi, dekripsi, *IDWT* dan rekontruksi dibentuk satu rangkaian dengan hasil akhir berupa program aplikasi keamanan citra.

Kata-kunci: Citra, *Wavelet*, Kriptografi, *DES*

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi pada saat ini, mengubah cara masyarakat dalam berkomunikasi atau pertukaran informasi satu sama lainya. Pertukaran Informasi saat ini tidak hanya berupa teks, tetapi dapat juga berupa gambar , *audio* dan *video*. Pada saat ini teknologi informasi telah menyediakan layanan seperti *SMS*(*Short Message Service*) bagi pengguna handphone dan *MMS* (*Multimedia Messaging Service*) bagi pengguna Internet untuk melakukan pertukaran informasi berupa teks, gambar, audio dan video.

Perkembangan informasi melalui jaringan internet membuat pertukaran informasi semakin cepat dan akurat serta terbuka melewati batas-batas negara dan budaya. Perkembangan ini akan menimbulkan tidak hanya dampak positif yang menguntungkan bagi dunia komunikasi dan pertukaran informasi saja tetapi juga berdampak negative yaitu kejahatan komputer antara lain pencurian, penipuan pemerasan dan lainnya. Pada saat ini masalah keamanan komputer dan kerahasiaan informasi merupakan hal yang sangat penting. Keamanan informasia pada komputer tidak hanya ber f*irewall* dan diteksi sistem intruksi saja tetapi juga keamanan informasi dari informasi itu sendiri.

Kriptografi memegang peran penting dalam membangun keamanan informasi. Kriptografi bertujuan agar pesan informasi tidak dapat dibaca oleh orang yang tidak berhak sehingga informasi baik yang disimpan dalam computer aman maupun yang dikirim melalui jaringan komputer aman dan bisa dipertanggung jawabkan oleh

sipengirim. Tiga fungsi dasar algoritma kriptografi modern adalah enkripsi, dekripsi dan *key*. Berdasarkan *key*, algoritma kriptografi digolongkan menjadi tiga bagian yaitu simetri, asimetri dan fungsi *Hash*. Algoritma *DES*(*Data Encryption Standard*) merupakan algoritma simetris yang paling umum digunakan saat ini (Budi Raharjo).

DES merupakan algoritma standar yang sampai saat ini masih banyak digunakan dan masih dianggap aman untuk menjawab tantangan perkembangan teknologi komunikasi yang sangat cepat.

Salah satu komponen multimedia yang berperan sangat penting dalam bentuk informasi visual adalah Gambar atau Citra. Informasi yang bebentuk citra mempunyai karakteristik yang berbeda dengan teks dan citra memberikan informasi yang lebih banyak dibanding dengan informasi berbentuk teks. Ada dua macam citra yaitu citra diam(*still images*) yaitu citra tunggal yang tidak bergerak dan citra bergerak(*moving images*) yaitu rangkaian citra diam yang ditampilkan secara beruntun(sekuensial). Selanjutnya sebutan citra diam akan disebut citra saja. (Munir,2004)

Pada umumnya untuk melakukan pengkodean suatu citra, harus mengubah citra tersebut dari suatu domain kedomain yang lain, proses ini disebut transformasi. Disamping itu juga bahwa transformasi menghasilkan domain yang lebih sesuai untuk proses pengkuantisasian. Metode yang banyak digunakan dalam transformasi ini antara lain Transformasi *Cosinus diskrit*, Transformasi *Fourier* dan Transformasi *Wavelet*. Dari ketiga jenis tranformasi tersebut, transformasi *wavelet* dianggap paling baik hasilnya, hal ini dikarenakan *wavelet* memberikan informasi tentang kombinasi skala dan frekuensi serta membutuhkan memori yang kecil. (Krisnawati,2006).

1.2 Perumusan Masalah

Dari latar belakang tersebut diatas, muncul masalah-masalah :

Dengan transformasi yang bagaimana membuat aplikasi sistem keamanan agar informasi yang berbentuk citra dapat disimpan dengan aman dan informasi yang dikirim melalui jaringan komunikasi internet sampai pada tujuan yang berhak dengan aman sehingga dapat dipertanggung jawabkan.

1.3 Batasan Masalah

Permasalahan sistem keamanan informasi pada tesis ini, akan dibatasi:

a. Sistem keamanan informasi dibatasi pada keamanan informasi itu sendiri menggunakan Algoritma *DES.*

b. Informasi yang dibahas dibatasi pada informasi berbentuk citra (citra diam).

c. Transformasi yang digunakan adalah transformasi *wavelet* diskrit dengan *filter Haar.*

1.4 Keaslian Penelitian

Penelitian-penelitian yang berhubungan dengan citra, aplikasi transformasi wavelet maupun sistem keamanan informasi yang menggunakan algoritma *DES* telah banyak dilakukan, antara lain: Penerapan Algoritma *DES* Dalam Sistem Keamanan Data Dengan penambahan *Password* Terjadwal oleh Saleh Sadikin, Desain Implementasi Teknik Kriptografi Pengamanan Basis data Perusahaan oleh Chitra Hapasari dkk, Simulasi Aplikasi Algoritma *DES* pada Transfer Data Uang Bank oleh Fitria dan Faiz

Sungkar, Implementasi Algoritma Kriptografi *DES* Dan *Watermark* Dengan Metode *LSB* pada Data Citra oleh Sulidar Fitri, Sistem Transfer Data Nirkabel Antar Stasiun Cuaca oleh R. Budiarianto Suryo Kusumo dkk, Transformasi *Fourier* Dan Trasfomasi *Wavelet* Pada Citra oleh Krisnawati, Sistem Keamanan Data Menggunakan *Spread Spectrum Image Steganography(SSIS)* Dan Algoritma Kriptografi *DES* oleh Chaeriah Bin Ali Waell, Penanganan Atribut Citra Dengan *Wavelet* Untuk Pengembangan Algoritma *C4.5* oleh Veronica S. Moertini.

Atas dasar penelitian-penelitian tersebut diatas, maka pada Tesis ini, hanya difokuskan pada pembahasan algoritma *DES* dan aplikasi transformasi *wavelet* diskrit yang digunakan untuk keamanan informasi berbentuk citra.

1.5 Manfaat Penelitian

Aplikasi hasil penelitian ini, diharapkan mempunyai manfaat :

a. Informasi citra dapat disimpan dengan aman.

b. Informasi citra yang dikirim melalui jaringan komunikasi internet, sampai pada tujuan yang berhak dengan aman sehingga dapat dipertanggung jawabkan.

c. Sebagai bahan pertimbangan bagi pengguna atau peneliti lain.

1.6 Tujuan Penelitian

Penelitian ini bertujuan:

a. Melakukan teknik pemrosesan sinyal citra digital dengan menggunakan transformasi *wavelet* diskrit dengan *filter Haar.*

b. Melakukan enkripsi dan dekripsi sinyal citra digital dengan algoritma *DES.*

c. Membuat program aplikasi keamanan citra dengan algoritma *DES.*

d. Menganalisis keamanan citra dengan algoritma *DES.*

BAB II

TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Implementasikan suatu cabang ilmu matematika yang digunakan pengamanan informasi disebut dengan *"Cryptography"* (kriptografi). Dengan kriptografi, data dapat diubah menjadi sandi-sandi yang tidak dimengerti yang disebut enkripsi, serta mengembalikannya kembali ke data semula yang disebut dekripsi data. *DES* merupakan standar proses enkripsi yang dikeluarkan oleh *Federal Information Processing Standard (FIPS)* pada tahun 1977. Dalam metoda *DES*, kunci yang digunakan dalam proses enkripsi dan dekripsi adalah sama (simetris) dan proses dekripsi merupakan kebalikan dari proses enkripsi. (Sadikin,2006).

Pengiriman data-data penting melalui akses internet pada masa sekarang sudah menjadi hal yang biasa. Hal ini menimbulkan semakin berkembangnya dunia kejahatan melalui jaringan internet, seperti penyadapan, pencurian, dan pemalsuan data informasi yang dikirim melalui internet terutama dalam sektor bisnis, perbankan, perdagangan, sampai sektor pemerintahan. Karena itulah kriptografi menjadi pilihan untuk melindungi data. *RSA(Rivers Shamir Adleman)* merupakan algoritma kriptografi yang dianggap aman, karena *RSA* memiliki pemfaktoran bilangan prima yang sangat besar. Sedangkan *DES(Data Encryption Standard)* merupakan algoritma yang menjadi pilihan untuk menjaga keamanan data. Misalnya digunakan dalam kartu chip yang dimiliki oleh para nasabah bank. *DES* menggunakan kunci yang sama untuk menyandi (enkripsi) maupun untuk menterjemahan (dekripsi), sedangkan *RSA* menggunakan dua kunci yang berbeda.

Istilahnya, *DES* disebut sistem sandi simetris sementara *RSA* disebut sistem sandi asimetris. (Nugroho,2007)

Keamanan pada basis data telah menjadi kebutuhan yang penting pada suatu perusahaan. Kebutuhan ini timbul dari semakin banyaknya ancaman terhadap data sensitif yang terdapat pada basis data. Teknik kriptografi merupakan salah satu alternatif solusi yang dapat digunakan dalam pengamanan basis data. Akan tetapi, pengembangan strategi kriptografi pada basis data membutuhkan banyak pertimbangan. Makalah ini memaparkan langkah-langkah implementasi teknik kriptografi dalam basis data, mencakup analisis lingkungan, desain solusi, dan persoalan-persoalan yang ditemui dalam menentukan desain pengamanan basis data. (Hapsari; dkk, 2010)

Simulation Application Algorithm of DES at Transfer Of Bank Data Money represent to protect data in process of bank money data tansfer. The application is not security program of Bank money data as a whole. Security Technique which is used in this research is Technique or Algorithm of DES (Data of Encryption Standard). And for the method of its research, writer use Fourth Generation Language. DES represent Symmetrical Algorithm which the including category of Block Cipher dividing every block as long as 64 bits. In its usage, DES require key with length 64 bit but also which is used only 56 bit. In development, writer used software Microsoft Visual Basic 6.0 with addition Object Library of MSWNSCK.OCX. (Fitria ; Sungkar,2009)

DES(Data Encryption Standard) merupakan algoritma yang pernah menjadi sangat terkenal di Amerika dan pernah menjadi keamanan dasar yang digunakan di seluruh dunia. Teknologi *Watermark* juga merupakan suatu solusi didalam melindungi kerahasiaan dari tanda kepemilikan. *Watermark* metode *LSB(Least Significant Bit)* dapat menyamarkan pesan ke dalam suatu media tanpa orang lain menyadari bahwa media tersebut telah disisipi suatu pesan. Penelitian ini dibagi menjadi 3 tahap. Pertama adalah

implementasi dari algoritma *DES* dan *Watermark LSB* dalam bahasa pemrograma java. Dilanjutkan dengan mengamati perbedaan media citra antara sebelum dan sesudah disisipkan pesan yang terenkripsi dengan *DES*. Media citra yang merupakan tempat penyisipan pesan menggunakan ekstensi file gambar *jpeg*, *gif*, dan *png*. Tahap terakhir adalah mengukur seberapa cepat kinerja dari proses dalam satuan detik pada beberapa ekstensi file gambar yang berbeda. Dari hasil pengujian, didapat bahwa implementasi yang dilakukan di sistem operasi *Windows* berhasil. Kualitas gambar sebelum dan sesudah disisipi tidak dapat dibedakan dengan hanya dilihat mata manusia secara langsung. Tetapi bisa dibedakan dengan melihat informasi dari histogram. Kinerja proses yang didapat dengan memproses 100 karakter, rata-rata kurang dari sama dengan 1 detik. (Fitri,2009)

Pengamanan komunikasi antar piranti keras sangat diperlukan, baik dari sisi jalur komunikasi maupun dari paket data yang dikirimkan dengan menggunakan protokol *SSL* dapet memberi keamanan dalam 3 hal; 1. Menjadikan kanal sebagai kanal private. dengan algoritma *DES* atau *RC4*; 2. Kanal diotentifikasi; 3. Setiap pengubahan data yang sedang dalam perjalanan oleh pihak yang tidak berwenang akan mudah di deteksi dengan penggunaan *message integrity (authentication) check (MAC).* Fungsi hash yang aman *(MD2,MD5,SHA)* digunakan untuk perhitungan *MAC.* Sehingga paket data yang dikirimkan pun merupakan paket data yang utuh dan asli. Output yang dicapai adalah memperoleh prototip sistem keamanan komunikasi data terintegrasi di dalam *SBC* yang handal dan efisien, proses enkripsi dan deskripsi data dilakukan secara otomatis oleh *SBC* melalui jaringan nirkabel dan dikembangkan berbasis open source sehingga dapat mereduksi tingkat ketergantungan Indonesia terhadap piranti lunak berlisensi. (Kusumo; dkk, 2010)

Algoritma *C4.5* adalah algoritma klasifikasi data bertipe pohon keputusan yang terkenal. Saat ini, algoritma ini dapat mengkonstruksi pohon keputusan dari set data atau tabel yang berisi rekord-rekord yang memiliki atribut kontinyu dan diskret. Penelitian ini dilakukan untuk mengembangkan *C4.5* agar dapat menangani atribut citra. Wavelet dipilih sebagai teknik analisis citra untuk membangkitkan vektor fitur citra. Makalah ini akan membahas prinsip-prinsip algoritma *C4.5*, analisis citra dengan *wavelet*, konsep awal pendekatan penanganan atribut citra dengan wavelet, dan eksperimen awal untuk mendukung konsep tersebut. Ada dua pendekatan yang diajukan untuk menangani atribut citra, yaitu dengan mentransformasi atribut citra menjadi atribut kontinu dan diskrit. Transformasi ke atribut kontinu dilakukan mengubah citra menjadi angka tingkat kemiripan terhadap sebuah citra referensi, ke atribut diskrit dilakukan dengan mengelompokkan dan mengklasifikasi citra lalu memberi label yang sesuai. Transformasi ini memanfaatkan algoritma *image retrieval* dengan *wavelet*, yaitu *Windsurf*.(Moertini, 2004)

Tranformasi *wavelet* merupakan perbaikan dari transformasi *Fourier*. Transformasi *Fourier* hanya dapat menangkap informasi apakah suatu sinyal memiliki frekuensi tertentu ataukah tidak, tapi tidak dapat menangkap dimana frekuensi itu terjadi. Jika Transformasi *Fourier* hanya memberikan informasi tentang frekuensi suatu sinyal, maka transformasi *wavelet* memberikan informasi tentang kombinasi skala dan frekuensi. (Krisnawati, 2006)

Steganography menyembunyikan keberadaan informasi, kriptografi hanya menyembunyikan arti atau isi dari sebuah informasi. Kedua teknik ini dapat digabungkan sehingga menghasilkan informasi yang semakin sulit dilacak. Sistem yang akan dirancang ini meggunakan teknik image steganography dengan data digital yang disisipkan pada citra cover berupa teks (.txt) yang telah dienkripsi terlebih dahulu

menggunakan algoritma kriptografi *DES*. *SSIS* menggunakan metode spread spectrum, dimana informasi yang akan disisipkan ke citra cover disebar ke dalam noise yang memiliki band frekuensi yang lebar. *Noise* inilah yang ditambahkan ke dalam citra *cover*. Sebagai antisipasi terjadi *error* selama proses transmisi, digunakan teknik *Error Control Coding (ECC)* yang terdiri dari enkoder konvolusi di *transmitter* dan *dekoder* yang menggunakan algoritma *viterbi* di *receiver*. Dari simulasi yang dilakukan, diketahui bahwa tingkat *imperceptibility* citra *stego* yang dihasilkan pada simulasi I (hanya untuk disimpan) tidak dipengaruhi oleh kriteria citra *cover* (low detail, medium detail, high detail) tapi dipengaruhi oleh jumlah bit yang disisipkan per tiap píksel citra *cover*. Kapasitas maksimum citra cover pada simulasi II, selain dibatasi oleh ukuran citra cover itu sendiri, juga dibatasi oleh jumlah code rate dari kode konvolusi yang digunakan dan level kuantisasi. Tingkat *imperceptibility* citra *stego* pada simulasi II dipengaruhi oleh kriteria citra *cover (low detail, médium detail, high detail)*, ukuran *file* teks, dan jumlah bit yang disisipkan pada tiap piksel citra *cover*. Rata-rata penilai *MOS* dari sampel 30 orang didapatkan bahwa citra stego memiliki penilaian *fine* pada kanal dengan *SNR* diatas 22 dB.(Chaeriah, 2006)

Kompresi citra digital telah diimplemetasikan menggunakan *wavelet Daubechies* dan diuji berdasarkan parameter laju bit dan *PSNR*. Kinerja tiga jenis *wavelet Daubechies db2*, *db3* dan *db4* dibandingkan untuk mengkompresi beberapa citra uji: citra Lenna, citra *Daubechies* dan citra *Fingerprint*. Hasil empirik menunjukkan bahwa *wavelet* ini mampu mengkompresi sedikitnya sampai 2/5 kapasitas semula. *Wavelet db4*, yang memiliki derajat kehalusan tertinggi, membuktikan bahwa dia mampu menjadi algoritma kompresi yang sangat memuaskan dan menghasilkan laju bit yang lebih rendah dari *wavelet* lainnya. Parameter *PSNR* menunjukkan bahwa *wavelet db4* menjadi yang terbaik kecuali untuk citra uji *Daubechies*. (Sianipar, 2003).

2.2 Landasan Teori

2.2.1 Pengolahan Citra digital

Pengolahan citra adalah pemrosesan citra, khususnya dengan menggunakan computer, menjadi citra yang kualitasnya lebih baik. Proses ini dilakukan karena seringkali citra yang dimiliki sering mengalami penurunan mutu (degradasi), misalnya mengandung cacat atau derau(*noice*), warnanya terlalu kontras, kurang tajam, kabur(*blurring*) dan sebagainya. Umumnya, operasi-operasi pada pengolahan citra diterapkan pada citra bila [*JAI89*]: (Munir,2004,h.3)

1. perbaikan atau memodifikasi citra perlu dilakukan untuk meningkatkan kualitas penampakan atau untuk menonjolkan beberapa aspek informasi yang terkandung di dalam citra,

2. elemen di dalam citra perlu dikelompokkan, dicocokkan, atau diukur,

3. sebagian citra perlu digabung dengan bagian citra yang lain.

Pengolahan Citra bertujuan memperbaiki kualitas citra agar mudah diinterpretasi oleh manusia atau mesin (dalam hal ini komputer). Teknik-teknik pengolahan citra mentransformasikan citra menjadi citra lain. Jadi, masukannya adalah citra dan keluarannya juga citra, namun citra keluaran mempunyai kualitas lebih baik daripada citra masukan. Termasuk ke dalam bidang ini juga adalah pemampatan citra (*image compression*), pengubahan kontras citra , penghilangan derau (*noise*) pada citra dengan operasi penapisan (*filtering*). (Munir,2004,h.5)

2.2.2 **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*. *Doughter wavelet* $\psi_{a,b}(t)$ dihasilkan oleh parameter dilatasi a dan translasi/kontraksi b, yang dinyatakan dalam persamaan :

$$\psi_{a,b}(t) = a^{-1/2}\psi\left(\frac{t-b}{a}\right); a>0, b\in R$$

dengan :

a = parameter dilatasi atau kontraksi, b = parameter translasi

R = mengkondisikan nilai a dan b dalam nilai *integer*

selanjutnya $W_{\psi}(f)(a,b) = \frac{1}{\sqrt{a}}\int_{-\infty}^{\infty} f(t)\,\psi\left(\frac{t-b}{a}\right)\mathrm{dt}$

dan formula *Calderon* memberikan:

$$f(t) = C_{\psi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\langle f, \psi_{a,b}\rangle\,\psi_{a,b}(t)a^{-2}\,dadb$$

Wavelet yang sering digunakan didefinisikan dengan fungsi *Haar* :

$$\psi(t) = \begin{cases} 1 & , \quad 0 \le t \le \frac{1}{2} \\ -1 & , \quad \frac{1}{2} \le t \le 1 \\ 0 & \quad otherwise \end{cases} \qquad \text{dan}$$

$$\psi_{j,k}(t) = a^{j/2}\psi\left(2^{j}t - k\right);\ j,k \in Z$$

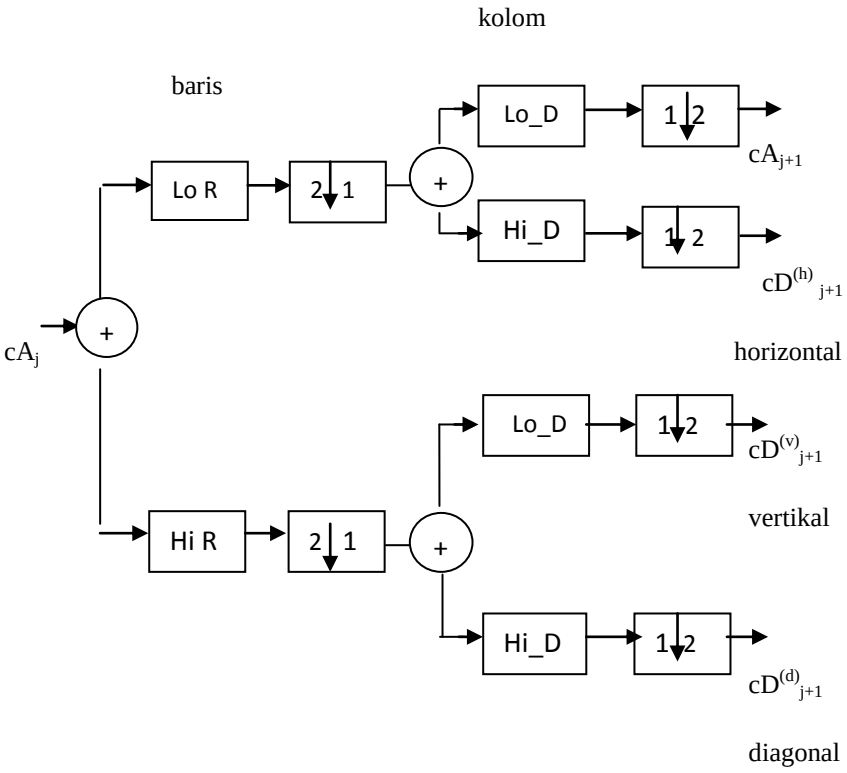
dengan: j *integer nonnegative*, $0 \le k \le 2^{j-1}$, 2^j = parameter dilatasi (parameter frekuensi atau skala), k = parameter waktu atau lokasi ruang dan Z = mengkondisikan nilai j dan k dalam nilai integer. Fungsi -fungsi diatas harus memenuhi kondisi $\int_{-\infty}^{\infty} \psi(t)\ dt = 0$, yang menjamin terpenuhinya sifat ortogonalitas vektor (Krisnawati,2006). Pada dasarnya, transformasi *wavelet* dapat dibedakan menjadi dua tipe berdasarkan nilai parameter translasi dan dilatasinya, yaitu *Continue Wavelet Transform (CWT)* dan *Discrete Wavelet Transform (DWT)*. Transformasi *wavelet* kontinu ditentukan oleh nilai parameter dilatasi *(a)* dan translasi *(b)* yang bervariasi secara kontinu, dimana $a,b \in R$ dan $a \neq 0$. *Continue Wavelet Transform* (CWT) menganalisis sinyal dengan perubahan skala pada *window* yang dianalisis, pergeseran *window* dalam waktu dan perkalian sinyal serta mengintegral semuanya sepanjang waktu. Secara matematis dirumuskan sebagai :

$$CWT(a,b) = \int f(t)\psi^{*}_{a,b}(t)dt$$

Transformasi *wavelet* diskrit bertujuan untuk mengurangi redundansi yang terjadi pada transformasi *wavelet* kontinu dengan cara mengambil nilai diskrit dari parameter *a* dan *b*. Transformasi *wavelet* diskrit menganalisa suatu sinyal dengan skala yang berbeda dan merepresentasikannya ke dalam skala waktu dengan menggunakan teknik *filtering* dimana sinyal dalam domain waktu dilewatkan ke dalam *High Pass Filter* dan *Low Pass Filter* untuk memisahkan komponen frekuensi tinggi dan frekuensi rendah , yakni menggunakan *filter* yang berbeda frekuensi *cut-off*-nya. (Siregar,2008)

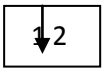
2.2.2.1 Transformasi *Wavelet* Diskrit Maju (*Forward DWT*)

Discrete Wavelet Transform (DWT) dikelompokkan menjadi dua yaitu *DWT* maju dan *DWT* balik. Pada tahap *DWT* maju dilakukan proses dekomposisi data citra, yang dimulai dengan melakukan dekomposisi terhadap baris dari data citra yang diikuti dengan operasi dekomposisi terhadap kolom pada koefisien citra keluaran dari tahap pertama. Cara kerja dari transformasi *wavelet* maju, ditunjukkan pada gambar 2.1 : (Novamizanti, 2008)

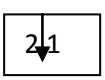


Gambar 2.1 *Gambar Forward DWT Dua Dimensi Skala Satu*

keterangan gambar 2.1: cA_j = citra masukan



= *down sampling* baris



= *down sampling* kolom

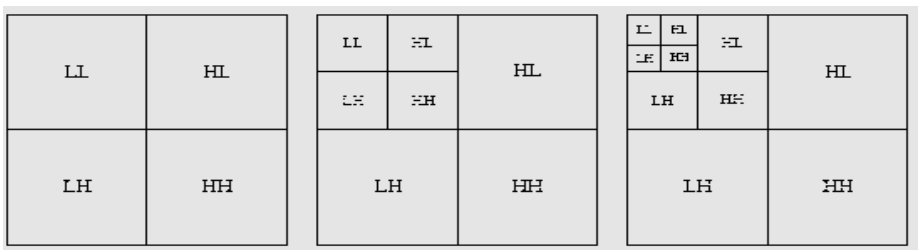
cA_{j+1} = koefisien approksimasi (LL)

$cD^{(h)}_{j+1}$ = koefisien *detail horizontal*(LH)

$cD^{(v)}_{j+1}$ = koefisien *detail vertical*(HL)

$cD^{(d)}_{j+1}$ = koefisien *detail diagonal*(HH)

Citra masukan diinterpretasikan sebagai sinyal, didekomposisi menggunakan *Lo_D* (*Low Pass Filter Decomposition*) dan *Hi_D (High Pass Filter Decomposition)* kemudian dilakukan *downsampling* dua. Keluaran berupa sinyal frekuensi rendah dan frekuensi tinggi. Kedua proses tersebut dilakukan sebanyak dua kali, terhadap baris dan terhadap kolom sehingga diperoleh empat subband keluaran yang berisi informasi frekuensi rendah dan informasi frekuensi tinggi. Koefisien aproksimasi mengandung informasi *background* dan Koefisien detail, yaitu : detail horizontal, detail vertikal, dan detail diagonal yang mengandung informasi tepian. Dekomposisi transfomasi *wavelet*, ditunjukkan pada gambar 2.2 :



a

b

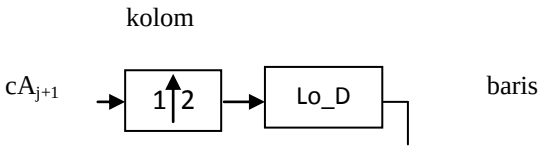
c

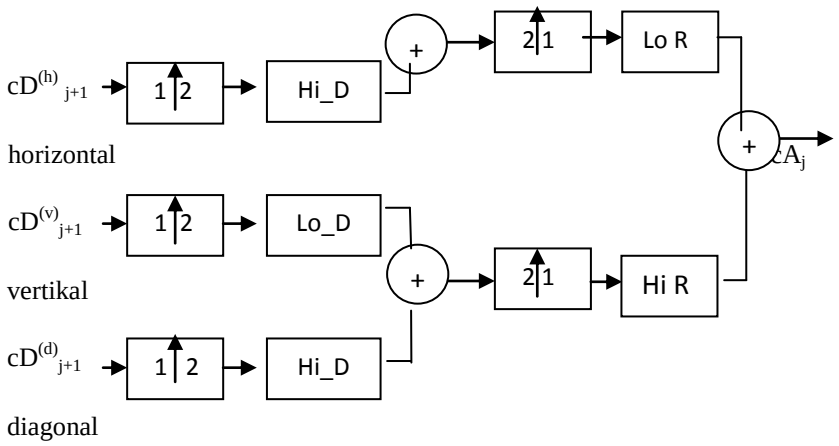
Gambar 2.2 *Gambar a. Transformasi wavelet level 1, b. Transformasi wavelet level 2 dan c. Transformasi wavelet level 3*

Transformasi *wavelet* level 2 didapatkan dengan membagi kembali *subband* residu pelolos rendah dari transformasi *wavelet* level 1 menjadi *subband-subband* yang lebih kecil dan seterusnya. (Siregar,2008)

2.2.2.2 Transformasi *Wavelet* Diskrit Balik (*Invers DWT*)

DWT balik merupakan kebalikan dari *DWT* maju. Pada tahap ini dilakukan proses rekonstruksi dengan arah yang berlawanan dari proses sebelumnya, yaitu dengan proses *up-sampling* dan pem-*filter*-an dengan koefisien-koefisien filter balik. Proses *up-sampling* dilakukan dengan mengembalikan dan menggabungkan sinyal seperti semula. Proses ini dilakukan dengan menyisipkan sebuah kolom berharga nol di antara setiap kolom dan melakukan konvolusi pada setiap baris dengan *filter* satu dimensi. Hal yang sama dilakukan dengan menyisipkan sebuah baris nol di antara setiap baris dan melakukan konvolusi pada setiap kolom dengan *filter* yang lainnya. *Filter* yang digunakan pada transformasi balik (rekonstruksi) ini adalah *filter* yang mempunyai hubungan khusus terhadap *filter* pada sisi dekomposisi yaitu *filter Lo_R* (*Low Pass Filter Reconstruction*) dan *Hi_R (High Pass Filter Reconstruction)*. Cara kerja *DWT* balik, ditunjukkan pada gambar 2.3: (Novamizanti, 2008)





Gambar 2.3 *Gambar Backward DWT Dua Dimensi Skala Satu*

keterangan gambar 3.3:

cA_j = citra keluaran yang sama dengan citra masukan

1 2 = *up sampling* baris

2 1 = *up sampling* kolom

cA_{j+1} = koefisien approksimasi (LL)

$cD^{(h)}_{j+1}$ = koefisien detail *horizontal*(LH)

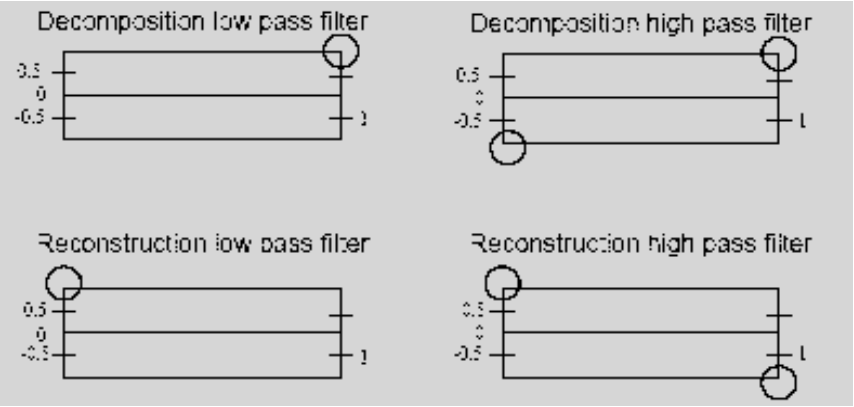
$cD^{(v)}_{j+1}$ = koefisien detail *vertical*(HL)

$cD^{(d)}_{j+1}$ = koefisien detail *diagonal*(HH)

2.2.2.3 Pemilihan Filter Wavelet

Pada makalah ini, digunakan *wavelet* dengan *filter Haar* (*Daubechies orde 1*). *Wavelet* dengan *filter Haar* dipilih karena memiliki *low pass filter*

dan *high pass filter* yang tidak memakan biaya komputasi yang besar. Berikut adalah gambar *filter Haar* yang digunakan : (Siregar,2008)



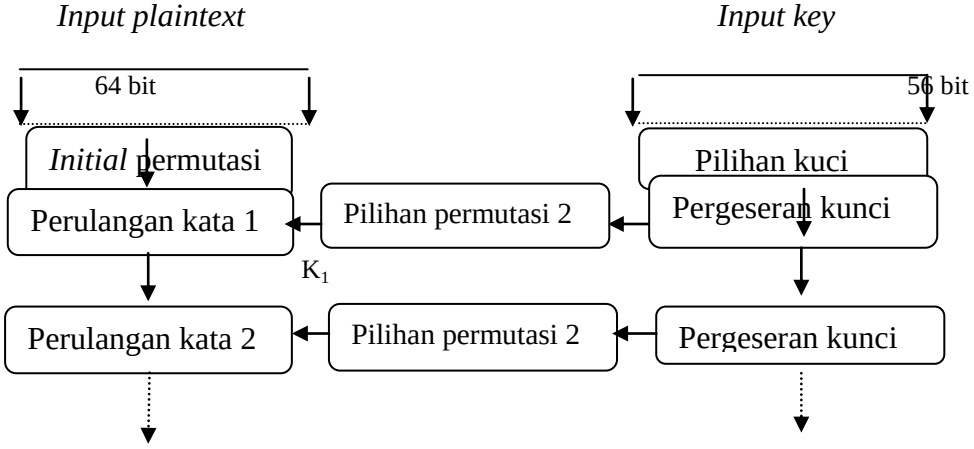
Gambar 2.4 *Gambar Filter Haar*

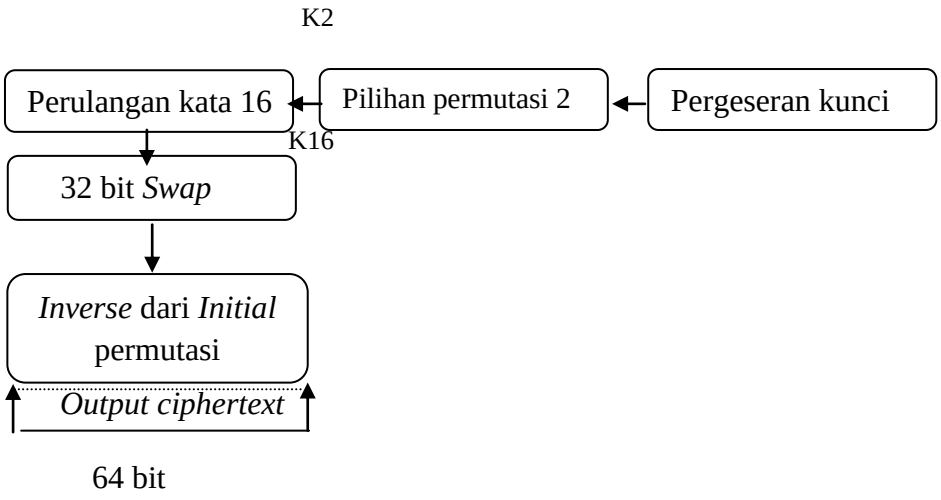
2.2.3 Algoritma *Data Encryption Standard(DES)*

DES termasuk dalam algoritma enkripsi yang sifatnya *cipher block*, yang berarti *DES* mengubah data masukan menjadi blok-blok 64-bit dan kemudian menggunakan kunci enkripsi sebesar 56-bit. Setelah mengalami proses enkripsi maka akan menghasilkan output blok 64-bit. (Ariyus, 2006)

2.2.3.1 Algoritma Enkripsi *DES*

Algoritma Enkripsi *DES*, ditunjukkan pada gambar 2.5:





Gambar 2.5 *Gambar Algoritma Enkripsi DES*

Pada awalya, kunci dilintaskan melewati suatu fungsi permutasi. Kemudian untuk setiap 16 kali iterasi subkunci(K_i) dihasilkan melalui kombinasi pergeseran sirkuler kiri dan permutasi. Fungsi permutasi sama untuk masing-masing iterasi, namun subkunci yang berbeda dihasilkan karena pergeseran ulang dari bit-bit kunci tersebut. Kunci yang digunakan sebagai input untuk algoritma *DES* merupakan subjek pertama permutasi. Kunci 56 bit yang dihasilkan kemudian diperlakukan sebagai dua kuantitas 28 bit, yang diberi label C_0 dan D_0. (Starlling , *2002*)

Proses *Initial* Permutasi(IP):

- Plaintext 64 bit diproses di IP dan menyusun kembali bit untuk menghasilkan permutasi input.
- Langkah untuk melakukan perulangan kata dari plaintext sebanyak 16 dengan melakukan fungsi yang sama, yang menghasilkan fungsi substitusi, dimana output akhir berisisi 64 bit(fungsi dari *plaintext* dan kunci), masuk ke *swap* dan menghasilkan *pre-output*.
- Pre-output diproses dan permutasi di *inverse* dari IP yang akan menghasilkan *ciphertext*. (Ariyus, 2006)

Diberikan input “M” 64 bit, yaitu M1, M2, …,M64.

Jika Mx adalah bilangan biner kemudian dilakukan permutasi X=IP(M) seperti: M58 M50 M12 M31 M18 M10 M12 M60 M52 M44 M36 M28 M20 M12 M4 M62 M54 M46 M38 M20 M22 M14 M6 M64 M48 M40 M32 M24 M16 M8 M57 M49 M41 MM33 M25 M17 M9 M1 M59 M51 M43 M35 M27 M19 M11 M3 M61 M53 M45 M37 M29 M21 M13 M5 M63 M55 M47 M39 M31 M23 M15 M7,maka inversnya $Y=IP^{-1}(X)=IP^{-1}(IP(M))$ akan mengembalikan M kebentuk semula (Ariyus, 2006).

Initial Permutasi, invers permutasi, fungsi permutasi dan expansi permutasi Algoritma *DES*, ditunjukan pada table-tabel:

Tabel 2.1 *Tabel Initial Permutasi(IP) Algoritma DES*

Input Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Output Bit	58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
Input Bit	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Output Bit	62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
Input Bit	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Output Bit	57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
Input Bit	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
Output Bit	61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Tabel 2.2 *Tabel Inverse Initial Permutasi (IP^{-1}) Algoritma DES*

Input Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Output Bit	40	8	48	16	56	24	64	32	39	7	47	15	55	20	63	31
Input Bit	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Output Bit	38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
Input Bit	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Output Bit	36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
Input Bit	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
Output Bit	34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Tabel 2.3 *Tabel Expantion Permutasi(E) Algoritma DES*

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

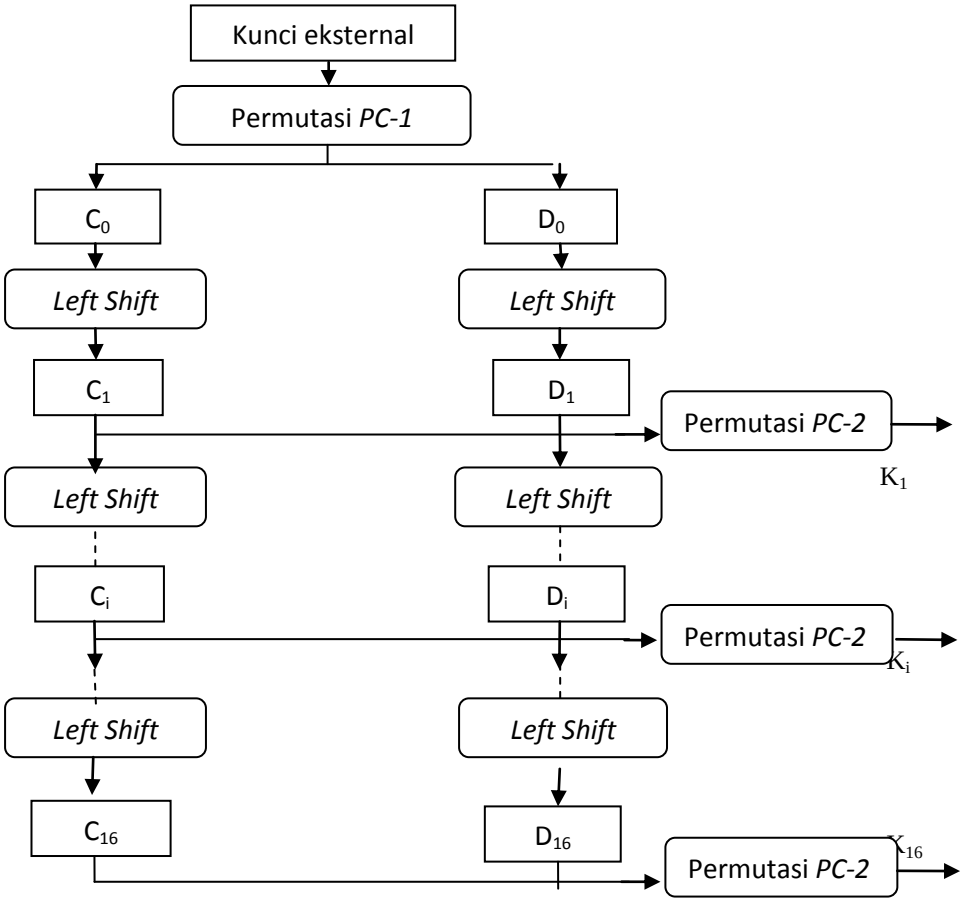
Output Bit	12	13	12	13	14	15	16	17	16	17	18	19	20	21	20	21
Input Bit	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Output Bit	22	23	24	25	24	25	26	27	28	29	28	29	30	31	32	1

Tabel 2.4 *Tabel Fungsi Permutasi(P) Algoritma DES*

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

Pembangkitan Kunci Internal:

Proses pembangkitan kunci internal algoritma *DES*, ditunjukkan pada gambar 2.6 : (Munir, 2006,h.141)



Gambar 2.6 *Gambar Proses Pembangkitan Kunci Internal DES*

Karena ada 16 putaran, maka dibutuhkan kunci internal sebanyak 16 buah, yaitu K_1, K_2, ...,K_{16}. Kunci-kunci internal ini dapat dibangkitkan

sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal panjangnya 64 bit atau 8 karakter. Misalkan kunci eksternal yang tersusun dari 64 bit adalah *K*. Kunci eksternal ini menjadi masukan untuk permutasi dengan menggunakan matriks permutasi kompresi *PC- 1* tabel 2.5. Dalam permutasi ini, tiap bit kedelapan *(parity bit)* dari delapan *byte* kunci diabaikan. Hasil permutasinya adalah sepanjang 56 bit, sehingga dapat dikatakan panjang kunci *DES* adalah 56 bit. Selanjutnya, 56 bit ini dibagi menjadi 2 bagian, kiri dan kanan, yang masing-masing panjangnya 28 bit, yang masing-masing disimpan di dalam C_0 dan D_0*:*

C_O: berisi bit-bit dari *K* pada posisi

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36

Do: berisi bit-bit dari *K* pada posisi

63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Selanjutnya, kedua bagian digeser ke kiri *(left shift)* sepanjang satu atau dua bit bergantung pada tiap putaran sesuai Tabel 2.7. (Munir, 2006, h.140)

Perhitungan Kunci Algoritma *DES*, ditunjukan pada table-tabel dibawah ini. (Ariyus, 2006, h.70)

Tabel 2.5 *Tabel Permutasi Chois One(PC-1) Algoritma DES*

Input Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Output Bit	57	49	41	33	25	17	9	1	58	50	42	34	26	18	10	2
Input Bit	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Output Bit	59	51	43	35	27	19	11	3	60	52	44	36	63	55	47	39
Input Bit	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Output Bit	31	23	15	7	62	54	46	38	30	22	14	6	61	53	45	37
Input Bit	49	50	51	52	53	54	55	56								
Output Bit	29	21	13	5	28	20	12	4								

Tabel 2.6 *Tabel Permutasi Choise Two(PC-2) Algoritma DES*

Input Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Output Bit	14	17	11	24	1	5	3	28	15	6	21	10	23	19	12	4
Input Bit	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Output Bit	26	8	16	7	27	20	13	2	41	52	31	37	47	55	30	40
Input Bit	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Output Bit	51	45	33	48	44	49	39	56	34	53	46	42	50	36	29	32

Tabel 2.7 *Tabel Schedule of Left Shifts Algoritma DES*

Nomor Iterasi	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Perputaran Bit	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

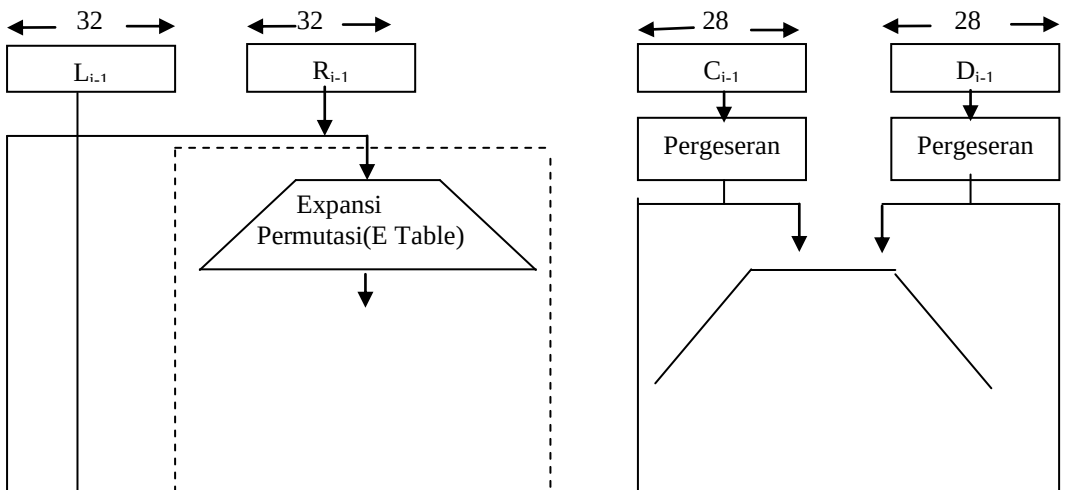
Tabel 2.8 *Tabel S-Box Algoritma DES*

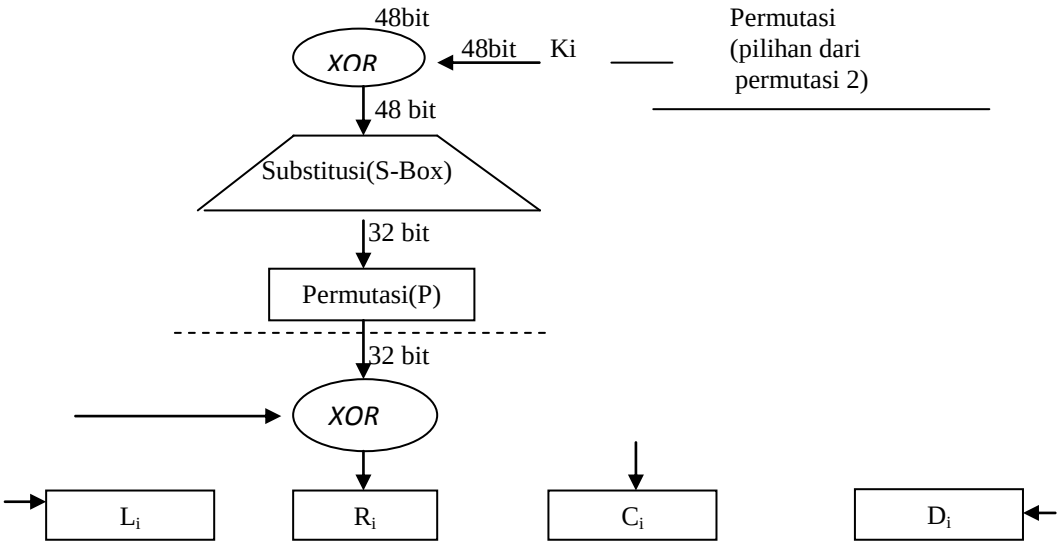
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8

	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S7	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Iterasi Algoritma *DES*

Putaran tunggal Algoritma *DES*, ditunjukkan pada gambar 2.7 : (Starlling , 2002)





Gambar 2.7 *Gambar Putaran Tunggal Algoritma DES*

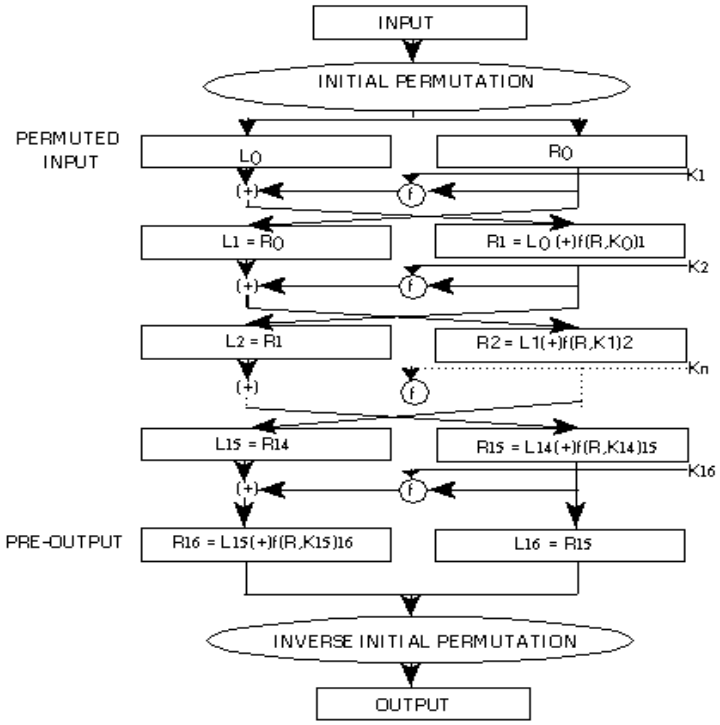
Input yang dipermutasi 64 bit melintasi 16 iterasi, menghasilkan nilai 64 bit lanjutan pada akhir dari masing-masing iterasi. Separuh kiri dan kanan dari setiap nilai iterasi mediate 64 bit diperlakukan terpisah sebagai kuantitas 32 bit, yang diberi label L(*left*) dan R(*right*). Pengolahanya menyeluruh pada masing-masing iterasi dapat diikhtiarkan dalam rumus :

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

Output dari sebelah kiri dari iterasi (L_i) setara dengan input sebelah kanan (R_{i-1}) tersebut. Output sebelah kanan (R_i) merupakan *OR* eklusif dari L_{i-1} dan merupakan fungsi yang kompleks dari R_{i-1} dan L_{i-1}. Fungsi yang kompleks ini beroperasi melibatkan permutasi dan substitusi. Operasi substitusi ditunjukan sebagai mana table Kotak_S (*S-Box*) memetakan setiap kombinasi 48 bit input kedalam suatu pola 32 bit khusus. Pada setiap Iterasi C dan D disubjekan secara terpisah untuk penggeseran sirkuler atau rotasi dari 1 atau 2. Nilai-nilai yang tergeser ini bertindak sebagai input untuk iterasi berikutnya. Keduanya juga bertindak sebagai input untuk fungsi

permutasi lainnya, yang menghasilkan output 48 bit yang bertindak sebagai input untuk fungsi $f(R_{i-1}, K_i)$. *(Starlling , 2002)*

Detail Proses Enkripsi, ditunjukkan pada gambar 2.8: (Astrianto)



Gambar 2.8 *Gambar Detail Proses Algoritma DES*

Initial Permutasi : $x_0 = IP(x) = L_0R_0$, sebagai *plaintext biner*

Prosoes Enkripsi 16 putaran:

$L_i = R_{i-1}$ dengan $1< i <16$, $R_{i-1} = L_{i-1} \oplus f(R_{i-1},K_i)$,

$C_0D_0 = PC1(K)$, $C_i = LS_i(C_{i-1})$, $D_i = LS_i(D_{i-1})$, $K_i = PC2(C_iD_i)$.

Ciphertext biner : $y = IP^{-1}(R_{16}L_{16})$. (Ariyus, 2006)

2.2.3.2 Algoritma Dekripsi *DES*

Proses dekripsi Algoritma *DES*, pada intinya sama seperti pada proses enkripsi, prosesnya balikan dari proses enkripsi. Blok (R_{16},L_{16}) merupakan masukan awal untuk *deciphering*. Blok (R_{16},L_{16}) diperoleh dengan mempermutasikan *ciphertext* dengan matriks permutasi IP^{-1}.

Prakeluaran dari *deciphering* adalah (R_0,L_0). Dengan permutasi awal IP akan didapatkan kembali blok *plaintext* semula. 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. (C_0,D_0) merupakan bit-bit dari kunci ekternal K yang diberikan pada waktu dekripsi. Selanjutnya K_{15} dihasilkan dari (C_{15},D_{15}) yang diperoleh dengan menggeser (C_{16},D_{16}) =(C_0,D_0) satu bit kekanan (sesuai arah kebalikan dari tabel schedule of left). K_{14} dihasilkan dari (C_{14},D_{14}) yang diperoleh dengan menggeser (C_{15},D_{15}) dua bit kekanan(sesuai arah kebalikan dari tabel *schedule of left*), dan seterusnya sampai dengan K_1 yang dihasilkan dari (C_1,D_1) . secara umum (C_{i-1},D_{i-1}) diperoleh dengan menggeser (C_i,D_i) satu atau dua bit kekanan (sesuai arah kebalikan dari tabel *schedule of left*) . (Munir, 2006,h.145-146).