Teori Grup Pada Algoritma *DES* Dan Transformasi *Wavelet* Diskrit Dalam Program Aplikasi Keamanan Citra Digital

Miftah Sigit Rahmawati[1], Rendra Soekarta[2]

Program Studi Teknik Informatika
Universitas Muhammadiyah Sorong

Abstract
Chryptography or Chriptology plays an important role in building data and information security. Chryptography aims to not read unauthorized people, so information can be safely maintained. Some research about Chryptography and algorithms related to data security have been done by practitioner of informatics and mathematic, one of which is DES algorithms and wavelet transform. *DES* algorithm is symmetrical standart algorithm which is widely used and is still considered safe to answer th challenges of the rapid development of information technology.
This paper have discussed about application of Algebra in DES algorithms and discrete Wavelet Transform On Digital Image Security Application, i.e. *XOR* operation, permutation, and permutation group or siklik group which is used in DES algorithms on digital image security application. Then, as Group it found (x+b)-group in discrete wavelet transform on digital image security application

***Key words** : digital image, chryptography, XOR algebra, DES algorithm, discrete wavelet transform.*

Abstrak
Kriptografi atau kriptologi memegang peran penting dalam membangun keamanan data dan informasi. Kriptografi bertujuan agar data dan informasi tidak dapat dibaca oleh orang yang tidak berhak, sehingga informasi dapat terjaga dengan aman. Beberapa penelitian tentang kriptografi dan algoritma yang berkaitan dengan keamanan data telah dilakukan oleh banyak orang baik dari praktisi ilmu informasi dan ilmu matematika, salah satunya adalah Algoritma *DES*. Algoritma *DES* merupakan algoritma standar simetris yang masih banyak digunakan dan masih dianggap aman untuk menjawab tantangan perkembangan teknologi informasi yang sangat cepat.
Penelitian ini menghasilkan pembahasan tentang penerapan aljabar pada algoritma *DES* dan transformasi *wavelet* diskrit dalam program aplikasi keamanan citra digital yaitu operasi *XOR*, permutasi, dan grup permutasi dapat digunakan pada algoritma *DES* dalam program aplikasi keamanan citra digital. Dipandang dari teori grup ditemukan grup-(x+b) pada transformasi *wavelet* diskrit dalam program aplikasi keamanan citra digital.

***Kata kunci** : Citra Digital, Kriptografi, Aljabar XOR, Algoritma DES, Transformasi Wavelet Diskrit*

1. Pendahuluan

Perkembangan teknologi informasi pada saat ini mengubah cara masyarakat dalam berkomunikasi atau bertukar data dan informasi satu sama lain. Pertukaran data dan informasi saat ini tidak hanya berupa teks, melainkan juga dapat berupa gambar, audio, dan video dan dapat disimpan secara digital. Data dan informasi yang dimiliki termasuk salah satu barang berharga yang perlu dijaga dan diamankan. Upaya untuk mengamankan informasi atau data tersebut dilakukan karena maraknya kasus pencurian dan penyalahgunaan informasi atau data oleh pihak-pihak yang tidak bertanggung jawab untuk kepentingan tertentu seperti penculikan, pencemaran nama baik dan lain-lain. Citra atau gambar merupakan salah satu bentuk data dan informasi digital yang sering disalahgunakan. Bentuk penyalahgunaan citra digital yang sering terjadi adalah rekayasa foto dan penyebaran foto pribadi secara ilegal. Tentunya hal ini dapat merugikan pemilik foto tersebut. Oleh karena itu perlu adanya pengamanan terhadap data dan informasi pribadi yang dimiliki sesuai apa yang telah ditulis oleh Solichin Zaki (2011) yaitu tentang Program Aplikasi Keamanan Citra dengan Algoritma *DES* dan Transformasi *Wavelet* Diskrit.

Kriptografi atau kriptologi memegang peran penting dalam membangun keamanan data dan informasi. Kriptografi atau kriptologi merupakan salah satu teori matematika yang sering digunakan dalam teknologi informasi. Kriptografi bertujuan agar data dan informasi tidak dapat dibaca oleh orang yang tidak berhak, sehingga informasi dapat terjaga dengan aman. Tiga fungsi dasar kriptografi modern adalah enkripsi, *des*kripsi, dan *key*. Kriptografi digolongkan menjadi tiga bagian yaitu simetris, asimetris, dan fungsi *Hash*. Algoritma *DES* merupakan algoritma standar simetris yang masih banyak digunakan dan masih dianggap aman untuk menjawab tantangan perkembangan teknologi informasi yang sangat cepat.

Pada umumnya untuk melakukan pengkodean suatu citra, harus mengubah citra tersebut dari suatu domain ke domain yang lain, proses ini disebut transformasi. Metode yang banyak digunakan dalam transformasi ini antara lain Transformasi *Cosinus Diskrit*, Transformasi *Fourier*, Dan transformasi *Wavelet*. Dari Ketiga jenis transformasi tersebut, transformasi *Wavelet* memberikan hasil yang paling baik, hal ini dikarenakan *Wavelet* memberikan informasi tentang kombinasi skala dan frekuensi serta membutuhkan memori yang kecil (Krisnawati, 2006). Selanjutnya, *Wavelet* diteliti dalam pemampatan citra dengan menggunakan transformasi *MP-Wavelet* tipe B oleh Fahim dkk. (2016).

Pada algoritma *DES* dan transformasi *Wavelet Diskrit* menggunakan beberapa konsep aljabar. penelitian ini mempunyai tujuan untuk menyelidiki adanya konsep dasar aljabar pada Algoritma *DES* dan Transformasi *Wavelet* Diskrit dalam keamanan citra digital. Dalam penelitian ini akan dibahas konsep dasar mengenai Algoritma *DES* dan Transformasi *Wavelet Diskrit* dalam keamanan citra digital.

2. Metode Penelitian

Penelitian ini dilakukan berdasarkan studi literatur berupa buku-buku dan jurnal-jurnal ilmiah khususnya yang berhubungan dengan Kriptografi, Algoritma *DES*, dan Transformasi *Wavelet* Diskrit. Penelitian ini mempunyai tujuan untuk menyelidiki adanya konsep dasar aljabar pada Algoritma *DES* dan Transformasi *Wavelet* Diskrit dalam keamanan citra digital.

3. Hasil Dan Pembahasan

Hasil penelitian dibagi menjadi dua yaitu penerapan aljabar pada *DES* dan penerapan aljabar pada transformasi *wavelet*. Masing-masing dijabarkan sebagai berikut:

3.1. Teori Grup Pada *DES*

DES adalah *chipper* blok yang mengenkripsi data dalam blok 64-bit. Sebuah blok 64-bit dari plaintext sebagai input ke dalam algoritma tersebut akan menghasilkan blok 64-bit *ciphertext*. Untuk proses enkripsi dan dekripsi menggunakan algoritma yang sama kecuali dalam pengaturan kunci. Panjang kunci yang digunakan adalah 56-bit, namun panjang kunci sebenarnya yang dimasukkan adalah 64-bit karena setiap bit kelipatan 8 tidak digunakan dalam algoritma namun hanya digunakan untuk *parity check*. Kunci dapat berupa angka 56-bit pa saja dan dapat dubah sewaktu waktu.

Pada level yang paling sederhana, algoritma *DES* dapat dikatakan hanya berupa kombinasi dari 2 teknik dasar enkripsi, konfusi, dan difusi. Dasar dari pembentukan blok dari *DES* adalah kombinasi tunggal dari teknik teknik ini yang berupa sebuah substutusi yang diikuti oleh sebuah permutasi terhadap plaintext yang didasarkan pada kunci. Ini dikenal sebagai sebuah round. Sebuah *DES* memiliki 16 *round*, yang melakukan kombinasi teknik yang sama terhadap plaintext selama 16kali.

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 di kombinasikan dengan kunci internal Ki. Keluaran dari fungsi *f* di -*XOR*-kan dengan blok L untuk mendapatkan blok R yang baru. Sedangkan blok L yang baru langsung diambil dari blok R sebelunya. Ini adalah satu putaran *DES*. Secara matematis satu putaran *DES* dapat dinyatakan sebagai:

$$L^{i-1} = R^i \oplus f(L^i, K^i)$$

$$R^{i-1} = L^i$$

Pada penjabaran di atas terdapat operasi aljabar yaitu operasi "*XOR*" dengan dilambangkan $\oplus$ yang merupakan aljabar Boolean.

Operasi aljabar *XOR* ditemukan dalam algoritma *DES* yang merupakan hasil dari $(a'b)+(ab')$

Tabel !. Operasi *XOR*

a	b	$(a'b)+(ab')$	
0	0	0+0	0
0	1	0+1	1
1	0	1+0	1
1	1	1+1	0

Sehingga bisa dituliskan, jika salah satu ada yang bernilai 1 maka hasilnya adalah 1 dan jika keduanya bernilai 1 atau 0 maka hasilnya 0.

Diberikan contoh: 40 *XOR* 8
Penyelesaian:
Mengingat perubahan bilangan *des*imal ke bilangan biner yaitu
40 = (2^5)+(2^3)
8= 2^3
7 6 5 4 3 2 1 0 ~ 1byte = 8bits
0 0 1 0 1 0 0 0 (untuk bilangan biner 40 angka 5 dan 3 diberi nilai 1)
0 0 0 0 1 0 0 0 (untuk bilangan biner 8 angka 3 diberi nilai 1)
Bilangan biner 40 adalah 0 0 1 0 1 0 0 0
Sedangkan bilangan biner 8 adalah 0 0 0 0 0 1 0 0
Untuk 40 *XOR* 8 didapatkan 0 0 1 0 0 0 0 0 = 2^3 = 32

Dalam *DES* dikenal dengan istilah initial permutasi, dibidang aljabar dikenal dengan grup permutasi. Sebelum mengenal lebih lanjut, disini akan diingatkan terlebih dahulu tentang pemetaan. Misalkan diketahui dua himpunan S dan T yang keduanya tak hampa. Pemetaan f dari S ke dalam T dituliskan $f: S \to T$ adalah suatu cara yang mengaitkan setiap unsur $x \in S$ dengan satu unsur di $y \in T$. Pengaitan ini ditandai dengan $f: x \to y$. Pada hakikatnya setiap unsur di S dapat dikaitkan dengan paling sedikit satu unsur di Y. Misalkan unsur $x \in S$ dikaitkan dengan unsur y_1 dan y_2 di T yang berbeda. Hal ini tidak dapat terjadi pada pemetaan $f: S \to T$. Dengan demikian didefinisikan sebagai berikut.

Definisi. Pengaitan semua unsur $x \in S$ akan mendefinisikan pemetaan $f: S \to T$ jika dan hanya jika setiap $x \in S$ dikaitkan dengan satu $y \in T$.

Bayangan atau peta pemetaan $f: S \to T$ adalah himpunan semua unsur $y \in T$ yang merupakan peta suatu unsur $x \in S$. Bayangan (peta) pemetaan di $f: S \to T$ dinotasikan dengan peta(*f*). jadi peta(*f*) didefinisikan sebagai berikut:

$$\text{Peta}(f) = \{y \mid y \in T, y = f(x) \text{ untuk suatu } x \in S\}$$

Definisi. Pemetaan $f: S \to T$ dikatakan satu satu atau injektif , jika untuk setiap unsur x_1 dan x_2 di S yang dipetakan sama oleh *f*, yaitu $f(x_1) = f(x_2)$ berlaku $x_1 = x_2$

Definisi. Pemetaan $f: S \to T$ dikatakan pada atau surjektif , jika untuk setiap unsur $y \in T$ terdapat unsur $x \in S$ yang memenuhi $f(x) = y$

Kedua definisi diatas memberikan definisi bijektif yaitu ketika pemetaan kesatuan $id_s: S \to S$ bersifat satu-satu dan pada.

Selanjutnya dari pemetaan bijektif akan memunculkan grup permutasi. Sebelum mendefinisikan grup permutasi, terlebih dahulu akan dijelaskan tentang permutasi sebagai berikut.

Misalkan $N = \{1, 2, 3, ..., n\}$ himpunana yang memuat *n* bilangan asli. Pemetaan satu satu $\pi: N \to N$ dituliskan dengan $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ x_1 & x_2 & \dots & x_n \end{pmatrix}$, dengan $x_i = \pi(i)$ untuk *i* = 1,2,…,*n*. menurut sifat sebelumnya $\pi: N \to N$ bersifat pada. Untuk selanjutnya, pemetaan satu-satu $\pi: N \to N$ disebut permutasi.

Jika A_n suatu himpunan berhingga dengan n elemen,maka banyaknya permutasi tingkat n pada elemen –elemen A_n adalah n!. Dengan menghimpun semua fungsi-fungsi bijektif dari A_n ke A_n diperoleh himpunan permutasi S_n.

Jika himpunana permutasi S_n dengan operasi komposisi fungsi pada S_n memenuhi aksioma grup maka ($S_n, \circ$) disebut grup permutasi

Pada bagian ini bisa dibentuk grup permutasi, perhatikan himpunan hingga $A_3 = \{1, 2, 3\}$, diidentifikasi semua pemetaan bijektif $\pi_i: A_3 \to A_3$. Dalam hal ini hanya dimiliki 6 pemetaan bijektif yaitu

1. $\pi_1 : 1 \to 1 \quad 2 \to 2 \quad 3 \to 3$
2. $\pi_2 : 1 \to 1 \quad 2 \to 3 \quad 3 \to 2$
3. $\pi_3 : 1 \to 2 \quad 2 \to 1 \quad 3 \to 3$
4. $\pi_4 : 1 \to 2 \quad 2 \to 3 \quad 3 \to 1$
5. $\pi_5 : 1 \to 3 \quad 2 \to 1 \quad 3 \to 2$
6. $\pi_6 : 1 \to 3 \quad 2 \to 2 \quad 3 \to 1$

Dapat dituliskan $S_3 = \{\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6\}$

Operasi dalam S_3 didefinisikan sebagai operasi fungsi, yaitu:

Misalkan $\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ dan

$\pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$(\pi_1 \circ \pi_2)(1) = \pi_1(\pi_2(1)) = \pi_1(1) = 1$

$(\pi_1 \circ \pi_2)(2) = \pi_1(\pi_2(2)) = \pi_1(3) = 3$

$(\pi_1 \circ \pi_2)(3) = \pi_1(\pi_2(3)) = \pi_1(2) = 2$

Jadi, $\pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \pi_2$

Berikutnya akan dibentuk tabel untuk memudahkan melihat $(S_n, \circ)$ memenuhi aksioma aksioma grup.

Tabel 2. Hasil dari $(S_n, \circ)$

$\circ$	π_1	π_2	π_3	π_4	π_5	π_6
π_1	π_1	π_2	π_3	π_4	π_5	π_6
π_2	π_2	π_3	π_1	π_6	π_4	π_5
π_3	π_3	π_1	π_2	π_5	π_6	π_4
π_4	π_4	π_5	π_6	π_1	π_2	π_3
π_5	π_5	π_6	π_4	π_3	π_1	π_2
π_6	π_6	π_4	π_5	π_2	π_3	π_1

Akan ditunjukkan bahwa $S_3 = \{\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6\}$ grup

i. Tertutup
$(\forall f, g \in S_3)\, f \circ g \in S_3$
Terlihat dalam tabel bahwa semua elemen merupakan anggota S_3

ii. Assosiatif
$(\forall f, g, h \in S_3)(f \circ g) \circ h = f \circ (g \circ h)$
Ambil sebarang $\pi_3, \pi_4, \pi_5 \in S_3$
$(\pi_3 \circ \pi_4) \circ \pi_5 = \pi_5 \circ \pi_5 = \pi_1$
$\pi_3 \circ (\pi_4 \circ \pi_5) = \pi_3 \circ \pi_2 = \pi_1$
Terlihat bahwa sifat assosiatif terpenuhi

iii. Eksistensi elemen identitas
$(\exists i \in S_3)(\forall f \in S_3) i \circ f = f \circ i = f$
Dari tabel terlihat bahwa terdapat $\pi_1 \in S_3$ sedemikian sehingga untuk setiap $f \in S_3$ memenuhi $\pi_1 \circ f = f \circ \pi_1 = f$, jadi elemen identitas S_3 adalah π_1

iv. Eksistensi elemen invers
$(\forall f \in S_3)(\exists f^{-1} \in S_3)\, f \circ f^{-1} = f^{-1} \circ f = i$

Menurut tabel, terlihat bahwa untuk setiap $f \in S_3$ selalu dapat ditemukan $f^{-1} \in S_3$ sedemikian sehingga $f \circ f^{-1} = f^{-1} \circ f = \pi_1$ yaitu

$\pi_1^{-1} = \pi_1$

$\pi_2^{-1} = \pi_3$

$\pi_3^{-1} = \pi_2$

$\pi_4^{-1} = \pi_4$

$\pi_5^{-1} = \pi_5$

$\pi_6^{-1} = \pi_6$

Dari (i)-(iv) terbukti bahwa $(S_n, \circ)$ merupakan grup, kemudian dikenal dengan Grup Permutasi

3.2. Teori Grup Pada Transformasi *Wavelet*

Wavelet merupakan pengembangan dari *Fourier*, yang dibentuk dari suatu keluarga fungsi ortogonal di suatu ruang fungsi yang dilengkapi dengan hasil kali dalam tertentu. Salah satu ruang yang dilengkapi dengan hasil kali dalam adalah ruang *Hillbert*. Dalam ruang *Hilbert*, misalkan $L^2(1,0)$ mempunyai basis ortonormal yaitu basis Haar seperti yang telah dijelaskan sebelumnya. Dalam hal ini, ruang Hilbert bekerja di dalam R yaitu $L^2(R)$ yang terdefinisi di R

Definisi. Ruang Hilbert merupakan abstraksi alami dari R^3, yang memiliki struktur linear vektor, hasil kali dalam, dan sifat kelengkapan.

Misalkan H ruang vector atas C. pemetaan $\langle .,. \rangle : HxH \to C$ yang memenuhi

(1) $\langle \alpha x + \beta y, z \rangle = \alpha \langle x, z \rangle + \beta \langle y, z \rangle,$
$\forall \alpha, \beta \in C, \forall x, y, z \in H$

(2) $\overline{\langle x, y \rangle} = \langle y, x \rangle, \forall x, y \in H$

(3) $\langle x, x \rangle \geq 0, \forall x \in H$

(4) $\langle x, x \rangle = 0, \forall x \in H$ jika hanya jika $x = 0$

Disebut hasil kali dalam pada H. Ruang vector H atas C yang dilengkapi dengan hasil kali dalam $\langle .,. \rangle$ disebut ruang hasil kali dalam.

Definisi. Basis Haar adalah himpunan fungsi $H = \{h_0 \cup \{h_{jk} : j \geq 0, 0 \leq k \leq 2^j\}\}$ dengan

$$h_0(x) = \begin{cases} 1, & \text{jika } 0 < x < 1 \\ 0, & \text{jika } x \text{ yang lain} \end{cases}$$

dan

$$h_{jk}(x) = \begin{cases} 2^{j/2}, & \text{jika } 2^{-j}k < x < 2^{-j}(k+1/2) \\ 2^{j/2}, & \text{jika } 2^{-j}(k+1/2) < x < 2^{-j}(k+1) \\ 0, & \text{jika } x \text{ yang lain} \end{cases}$$

Dari kajian pustaka sebelumnya, persamaan fungsi skala dapat dibentuk persamaan *wavelet* yang pertama atau disebut mother *wavelet* dengan definisi sebagai berikut

$$\psi_{a,b}(t) = \frac{1}{\sqrt{|a|}} \psi\left(\frac{t-b}{a}\right), a, b \in R, a \neq 0$$

Dimana *a* merupakan parameter skala yang mengukur derajat skala dan *b* merupakan parameter translasi yang menentukan lokasi waktu dari *wavelet*.

Dipandang dari Teori Grup, *wavelet* $\psi_{a,b}(t)$ merupakan hasil dari operasi $U(a,b)$ dalam fungsi ψ yang kemudian bisa dituliskan sebagai berikut

$$[U(a,b)\psi](x) = \frac{1}{\sqrt{|a|}} \psi\left(\frac{x-b}{a}\right), a, b \in R, a \neq 0$$

Operasi tersebut dikenakan pada seluruh kesatuan di ruang Hilbert $L^2(R)$ yang mendasari representasi dari grup-($ax + b$).

Hal ini diperjelas dengan pembuktian sebagai berikut

Akan ditunjukkan $U(a,b)$ merupakan grup dengan $U(a,b)U(c,d) = U(ac, b + ad)$

i) Bersifat asosiatif

$$\begin{aligned} &(U(a,b)U(c,d))U(e,f) \\ &= (U(ac, b+ad))U(e,f) \\ &= U(ace, (b+ad)+(ac)f) \\ &= U(ace, b+a(d+cf)) \\ &= U(a,b)U(ce, d+cf) \\ &= U(a,b)(U(c,d)U(e,f)) \end{aligned}$$

Terbukti bersifat asosiatif

ii) Memuat elemen identitas

Ambil $U(1,0) = Id$, maka untuk setiap $a, b \in R$ berlaku

$$\begin{aligned} U(1,0)U(a,b) &= U(1a, 0+1b) \\ &= U(a,b) \end{aligned}$$

Terbukti adanya elemen identitas

iii) Setiap elemennya mempunyai invers

Misalkan $U(\frac{1}{a}, -\frac{b}{a}) = U(a,b)^{-1}$ dengan $a \neq 0$ maka untuk setiap $a, b \in R$ berlaku

$$\begin{aligned} U(a,b)[U(a,b)]^{-1} &= U(a,b)U\left(\frac{1}{a}, -\frac{b}{a}\right) \\ &= \left(a.\frac{1}{a}, b + a\left(-\frac{b}{a}\right)\right) \\ &= U(1,0) \\ &= Id \end{aligned}$$

Terbukti setiap elemen nya mempunya invers.

Dikarenakan grup yang tak tereduksi, maka setiap bilangan tak nol $f \in L^2(R)$ selalu didapatkan penyelesaian untuk semua $U(a,b)f$. Dengan kata lain, $U(a,b)f$ merentang di seluruh ruang. Operasi perkalian tersebut mendefinisikan hasil kali dari pasangan $(a,b),(c,d) \in R/\{0\} \times R$, dengan $(a,b) \circ (c,d) = (ac, b+ad)$. Seperti hal nya operasi $U(a,b)$, pasangan (*a*,*b*) bersama dengan operasi $\circ$ membentuk grup.

Grossmann kemudian mengembangkan algoritma diatas yaitu transformasi *wavelet* menuju pengenalan dengan *wavelet* $\psi_{a,b}(t)$ yang berhubungan dengan perwakilan intgrasi kuadrat dari *grup affine*.

4. Kesimpulan

Kesimpulan yang dapat diambil setelah pembahasan tentang penerapan aljabar pada algoritma *DES* dan transformasi *wavelet* diskrit

dalam program aplikasi keamanan citra digital adalah:

1. Operasi *XOR*, permutasi, dan grup permutasi dapat digunakan pada algoritma *DES* dalam program aplikasi keamanan citra digital
2. Dipandang dari teori grup, ditemukan grup-(x+b) pada transformasi *wavelet* diskrit dalam program aplikasi keamanan citra digital.

5. Referensi

Stalling, William., 2006, *Cryptographi and Network Security Principles and Practises, Fourth Edition*. USA : Prentice Hall. Inc.

Alfiyanih dan Suryadi, 2012, Penggunaan Aljabar pada Algoritma Serpent dalam Pengamanan Citra Digital. *Prosiding Seminar Nasional Aljabar Universitas Diponegoro,* hal 106.

Ariyus, Doni., 2008, *Pengantar Ilmu Kriptografi*. Yogyakarta : Andi Offset.

Ariyus, Doni., 2006, *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta : Graha Ilmu.

Bronshtein,I.N., Semendyayev, K.A., Musiol, G., muehlig, H., 2005, *HANDBOOK OF MATHEMATICS fifth edition*. New York : Springer-Verlag.Inc.

Fresly, dkk., 2015. Implementasi Kriptografi Pengamanan Data pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standart. *Jurnal Informatika Mulawarman*, Vol.10, No 1. 20-31.

Herstein, I.N., 1995. *Abstrack Algebra*. USA : Prentice Hall. Inc.

Krisnawati., 2006. Transformasi Fourier dan Transformasi *Wavelet* pada Citra. *Dasi*. Vol 7. No 4

Munir, Rinaldi., 2012, Algoritma Enkripsi Selektif Citra Digital dalam Ranah Frekuensi Berbasis Permutasi Chaos, *Jurnal Rekayasa Elektrika*, Vol 10, no 2. 89-95.

Zaki, Solichin., 2011, Program Aplikasi Keamanan citra dengan Algoritma *DES* dan Transformasi *Wavelet* Diskrit, *Tesis*, Program Pasca Sarjana Universitas Diponegoro.

Yunitha, dkk., 2013, Perancangan Sistem Keamanan Pada Mesin ATM Menggunakan Verifikasi Sidik Jari *Life Fingerprit Security*. *Seminar Nasional Informatika UPN "Veteran" Yogyakarta.*

Fahim, dkk., 2016. Transformasi MP-Wavelet Tipe B Dan Aplikasinya Pada Pemampatan Citra. *Math And Its Application Journal*, Vol.13, No.1.hal 49-58.

Lee, D.T.L and Yamamoto, A. 1994. Wavelet Analysis: Theory and Applications. *Hewleet-Packard Journal.*

Gunawan,H. 2014. *Analisis Fourier dan Wavelet (edisi revisi)*. Buku Ajar, Bandung