Perancangan Perangkat Lunak Kriptografi Citra Digital dengan FFT Kunci Chaos

Linna Oktaviana Sari
Jurusan Elektro Fakultas Teknik Universitas Riau
Kampus Bina Widya KM 12,5 Simpang Baru Pekanbaru 28293, Telepon (0761) 66595
e-mail: linna.osari@gmail.com

Abstrak

Kriptografi dapat dilakukan pada citra. Citra merupakan jenis media digital yang paling rentan terhadap tindakan illegal. Untuk mengamankan citra digital yang ditransmisikan, citra digital harus dienkripsi menjadi gambar yang tidak memiliki arti. Namun, tidak semua metode enkripsi untuk teks dapat diterapkan pada enkripsi citra karena proses yang lambat. Hal tersebut dapat diatasi dengan menerapkan metode enkripsi khusus untuk citra digital. Pada penelitian ini telah dirancang perangkat lunak kriptografi untuk mengamankan citra digital menggunakan FFT (Fast Fourier Transform) sebagai algoritma enkripsi, Invers FFT (IFFT) sebagai agoritma dekripsi dan persamaan logistic dari chaos sebagai kunci. Perangkat lunak dirancang menggunakan GUI (Graphical User Interface) Matlab R2010a. Hasil penelitian menunjukkan bahwa perangkat lunak kriptografi yang dirancang dapat melakukan enkripsi dan dekripsi pada citra digital dengan menggunakan Algoritma FFT, IFFT dan kunci chaos dengan waktu enkripsi dan dekripsi kurang dari 1 detik.

Kata kunci: *Kriptografi, Citra Digital, FFT, Chaos.*

Abstract

Cryptography can be performed on the image. The image is a type of digital media is most vulnerable to illegal actions. To secure the transmitted digital image, digital image must be encrypted into an image that has no meaning. However, not all encryption methods used in the text can be applied to image encryption because a slow process. This can be solved by applying a special encryption method for digital images. In this study, cryptographic software has been designed to secure the digital image using FFT as the encryption algorithm, inverse FFT as the decryption algorithm and the logistic equation of chaos as the key. The software designed to use GUI Matlab R2010a. The results showed that the cryptographic software has been designed, can make the process of encryption and decryption on digital images using algorithms FFT, IFFT and chaos as the key, with less than 1 second.

Keywords*: Cryptography, digital Image, FFT, Chaos*.

1.Pendahuluan

Seiring dengan sangat pesatnya perkembangan jaringan data dan kemajuan teknologi informasi dibidang komputer memungkinkan ribuan orang dapat berkomunikasi dan saling bertukar informasi jarak jauh dalam dunia maya. Pertukaran informasi melalui dunia maya dikenal dengan *cyberspace* atau istilah awam Internet [1]. Dalam dunia maya ini, hampir segala jenis informasi dapat diperoleh, yang dibutuhkan hanyalah sebuah komputer yang terhubung dengan dunia maya ini [2]. Informasi yang diperoleh dalam dunia maya dapat disajikan dalam berbagai format seperti: teks, citra, audio, maupun video [3]. Seiring dengan kemajuan teknologi tersebut, ancaman-ancaman terhadap informasi seperti modifikasi dan duplikasi menyebabkan dibutuhkannya keamanan informasi. Pengamanan informasi tersebut sangat dibutuhkan untuk menjaga kerahasiaan/privasi (*confidentiality*) informasi, memastikan identitas/otentikasi (*authentication*), menjaga keutuhan/integritas (*integrity*) informasi , dan menjamin ketersediaan (*availability*)[4]. Oleh karena itu dibutuhkan sistem pengamanan data yang dapat menyesuaikan dengan perkembangan teknologi sehingga data yang dikirimkan melalui jaringan tidak jatuh pada orang yang tidak berhak dan tidak dimodifikasi. Telah dikembangkan dalam bidang teknologi informasi cabang ilmu yang mempelajari tentang cara-cara pengamanan data, yaitu, kriptografi, steganografi dan watermarking [5]. Kriptografi adalah suatu seni untuk menyembunyikan informasi dari sebuah pesan, sehingga pesan tersebut terlihat tidak memiliki arti [5]. Kriptografi berasal dari bahasa yunani, yang berarti ilmu tentang penulisan rahasia [6]. Berdasarkan namanya, kriptografi digunakan untuk mengaburkan informasi rahasia sehingga tidak bisa dimengerti oleh orang lain yang tidak berhak [7]. Selain itu, kriptografi juga digunakan untuk otentikasi pesan [8].

Dalam kriptografi, enkripsi merupakan hal yang sangat penting. Enkripsi dapat diartikan *chiper* atau kode, dimana pesan asli (*plaintext*) dirubah menjadi kode-kode yang tidak dimengerti (*ciphertext*)[4]. Dalam proses enkripsi terdapat dua hal yang perlu untuk diperhatikan yaitu algoritma dan kunci. Algoritma dapat dibuat untuk diketahui umum akan tetapi kunci harus dirahasiakan. Untuk beberapa mekanisme enkripsi, kunci yang sama digunakan baik untuk enkripsi dan dekripsi disebut *kunci simetri*; untuk

mekanisme yang lain, kunci yang digunakan untuk enkripsi dan dekripsi berbeda disebut *kunci asimetri.*[9].

Kriptografi tidak hanya dilakukan pada data yang berupa teks (pesan), melainkan juga berupa gambar (citra). Diantara jenis-jenis digital media yang ada, citra atau gambar adalah yang paling rentan terhadap operasi-operasi illegal berupa duplikasi, modifikasi, dan pemalsuan, karena data berupa citra dapat dengan mudah ditangkap oleh mata manusia. Sehingga banyak citra digital menjadi informasi yang sangat penting untuk diamankan dan dijaga kerahasiannya agar tidak akses oleh orang yang tidak berhak dan dirubah kebenaran isi informasi dari citra digital tersebut, sebagai contoh foto digital, sertifikat digital, tanda tangan digital (digital signature), dan lain sebagainya. Hal tersebut menyebabkan kebutuhan akan program-program aplikasi kriptografi yang dapat membantu pemakai untuk menjamin keamanan data berupa citra digital pada saat ditransmisikan juga semakin besar. Untuk menjamin keamanan data berupa citra digital yang ditransmisikan, maka citra digital harus dienkripsi menjadi *cipher image* atau gambar yang tidak memiliki arti. Setelah sampai di tujuan, maka *cipher image* didekripsikan kembali menjadi citra yang serupa dengan citra asli (*decipher image*) yang diterima oleh penerima. Namun, tidak semua metode enkripsi untuk teks dapat diterapkan pada enkripsi citra dikarenakan kesulitan implementasi dan proses yang lambat. Hal tersebut dapat diatasi dengan menerapkan metode enkripsi khusus untuk citra digital.

Telah dikembangkan metode untuk mengenkripsi gambar, metode ini mengkonversi gambar 2D ke dalam daftar 1D, dan mempekerjakan *scan* bahasa untuk menjelaskan hasil yang dikonversi. Namun tidak efisien untuk mengenkripsi atau mendekripsi gambar ukuran besar secara langsung. [10]. Kuo pada tahun 1993 mengembangkan metode enkripsi mengacu pada distorsi citra, dimana citra yang terenkripsi diperoleh dengan menambahkan spectral fase dari citra asli, enkripsi ini cukup aman, tetapi tidak memperhatikan teknik kompresi[11].

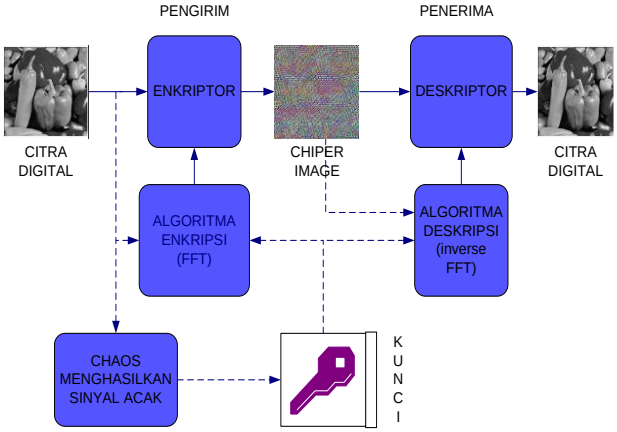
Kemudian telah dikembangkan *chaotic Kolmogrov-flowbased image encryption technique*, dimana citra dianggap sebagai suatu blok tunggal dan dipermutasikan melalui pengontrolan system kunci chaotic [12]. Pada tahun 1999 Yen dan Guo mengembangkan metode enkripsi yang disebut *BRIE,* berdasarkan logistic map chaos. Dimana kunci rahasia terdiri dari dua integer dan kondisi awal pemetaan logistic[13].

Selain itu telah dikembangkan teknik kriptogarafi citra menggunakan teknik kompresi citra dan vector kuantisasi untuk merancang kriptosystem yang efisien [14]. Prasanna telah mengembangkan metode enkripsi dengan FFT, dimana kunci dihasilkan dari citra pembawa (*Carrier Image*) [5].

Pada penelitian ini telah dirancang perangkat lunak kriptografi untuk mengamankan citra digital menggunakan FFT (*Fast Fourier Transform*) sebagai algoritma enkripsi dan *Inverse* FFT sebagai algoritma dekripsi dan persamaan *logistic* dari *chaos* sebagai kunci. Perangkat lunak dirancang dengan menggunakan GUI (*Graphical User Interface*) Matlab R2010a. Hasil penelitian menunjukkan algoritma FFT dan kunci *chaos* yang digunakan pada perancangan perangkat lunak kriptografi citra digital telah berhasil melakukan proses enkripsi dan dekripsi pada citra digital. Proses enkripsi dan dekripsi pada citra digital yang dilakukan perangkat lunak kriptografi yang dirancang yaitu kurang dari 1 detik.

2. Metode Penelitian

Perancangan perangkat lunak ini menerapkan metode yang mengintegrasikan teknologi pengolahan citra digital dengan teknologi informasi. Sistem pengamanan citra digital terdiri dari dua bagian yaitu *Enkriptor* pada bagian pengirim/sumber citra digital untuk mengenkripsi citra digital dan *Deskrtiptor* pada bagian penerima untuk mendekripsikan atau mengembalikan citra digital asli. Algoritma untuk enkripsi dan dekripsi dirancang dengan menggunakan FFT (*Fast Fourier Transform*). Sedangkan Kunci yang digunakan adalah kunci simetris yang acak dihasilkan dengan *Logistic* Map dari *Chaos.* Semua sistem dibuat dengan menggunakan GUI (*Graphical User Interface*) Matlab 2010a. Proses kerja perangkat lunak dapat ditunjukkan pada blok diagram (Gambar 1). Pada blok diagram tersebut, dapat dijelaskan bahwa *citra digital asli* yang akan *diamankan* pada bagian pengirim akan *dienkripsi* dengan menggunakan *enkriptor*. *Enkriptor* akan mengenkripsi citra digital dengan menggunakan *algoritma enkripsi (FFT).* Algoritma enkripsi akan menggunakan *kunci* dalam proses enkripsinya. Kunci dihasilkan dari sinyal acak menggunakan *teori logistic map chaos*. Hasil keluaran enkriptor berupa *cipher image* yang tidak dimengerti. Cipher image pada bagian penerima akan masuk ke *dekriptor* untuk didekripsi menggunakan *algoritma deskripsi (Inverse FFT)*. Algoritma deskripsi juga menggunakan kunci yang sama dengan algoritma enkripsi. Sehingga kunci tersebut dikatakan *kunci simetris*. Keluaran descriptor berupa citra digital asli.



Gambar 1. Blok Diagram Proses kerja Pengaman Citra Digital

Algoritma untuk enkripsi dirancang dengan menggunakan FFT dan dekripsi dengan menggunakan Inverse FFT. Algoritma yang bekerja dengan *Transformasi Fourier* pada komputer biasanya melibatkan suatu bentuk dari transformasi yang dikenal sebagai *Discrete Fourier Transform* (DFT). DFT adalah transformasi yang memiliki nilai input dan output berupa sampel diskrit, sehingga mudah untuk dimanipulasi komputer. Ada dua alasan utama untuk menggunakan bentuk dari transformasi:

- Masukan dan keluaran dari DFT keduanya diskret, yang dapat dimanipulasi komputer.
- Algoritma yang cepat untuk menghitung DFT dikenal sebagai *Fast Fourier Transform* (FFT)

DFT biasanya ditetapkan untuk fungsi diskrit f (m, n) yang hanya nol pada batasan hingga 0 ≤ m ≤ M -1 dan 0 ≤ n ≤ N -1. DFT Dua dimensi M-by-N dan invers DFT M-by-N dapat dinyatakan oleh [15] :

$$F(p,q) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} f(m,n)e^{-j2\pi pm/M}e^{-j2\pi qn/N} \qquad \begin{matrix} p = 0,\ 1,\ ...,\ M-1 \\ q = 0,\ 1,\ ...,\ N-1 \end{matrix} \qquad (1)$$

Dan invers DFT:

$$f(m,n) = \frac{1}{MN}\sum_{p=0}^{M-1}\sum_{q=0}^{N-1} F(p,q)e^{j2\pi pm/M}e^{j2\pi qn/N} \qquad \begin{matrix} m = 0,\ 1,\ ...,\ M-1 \\ n = 0,\ 1,\ ...,\ N-1 \end{matrix} \qquad (2)$$

Dengan melihat persamaan (1) dan (2) jelas bahwa FFT memiliki basis sinyal sinusoda dan merupakan bentuk komplek. Sehingga representasi domain frekuensi yang dihasilkan juga akan memiliki bentuk komplek. Dengan demikian akan dilihat adanya bagian real dan imajiner, dan bisa juga hasil transformasi direpresentasikan dalam bentuk nilai mutlak yang juga dikenal sebagai magnitudo respon frekuensinya dan magnitudo respon fase.

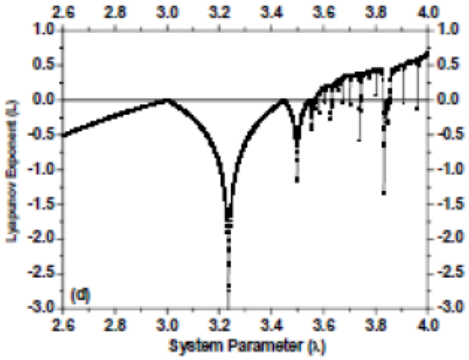
Kunci yang digunakan pada proses enkripsi sama dengan kunci dekripsi, dimana menggunakan kunci chaos berupa persamaan *logistic map*. Persamaan Logistik (*Logistic Map*) adalah salah satu bentuk yang paling sederhana dari proses *chaotic.* [16] menunjukkan bahwa model sederhana ini menunjukkan perilaku yang kompleks. Karena kesederhanaan matematisnya, model ini terus memunculkan ide-ide baru dalam teori chaos serta aplikasi kekacauan dalam kriptografi [16] . Berikut adalah persamaan dari peta logistik :

$$Xn+1 = \lambda\, Xn\, (1 - Xn) \qquad (3)$$

Di mana Xn adalah *variabel state*, yang terletak di interval [0,1] dan λ disebut sebagai parameter sistem yang dapat memiliki nilai antara 1 dan 4. Pada dasarnya, peta ini, seperti peta satu-dimensi lainnya, yaitu aturan untuk mendapatkan sebuah bilangan dari bilangan lain..

Dari gambar 2, dapat dilihat bahwa persamaan yang menghasilkan sifat *chaos* terbesar adalah saat λ bernilai sekitar 4. *Logistic Map* tidak akan bersifat chaos saat λ bernilai < 3.559 yang menghasilkan nilai Lypunof negatif. Menurut perhitungan yang telah dilakukan, dapat disimpulkan bahwa logistic map memberikan karakter *chaos* terbaik saat λ bernilai sangat dekat dengan 4. [16].

Persamaan logistik ini dapat diterapkan dalam kriptografi dengan membuat fungsi seperti yang telah dicantumkan diatas. Setelah membuat fungsi tersebut, dilakukan proses perhitungan dengan melakukan iterasi secara berulang, sehingga akan selalu mendapatkan bilangan yang acak.



Gambar 2. Perilaku dari *Logistic Map : Lyapunov exponent* (pengukuran kuantiatif dari sifat *chaos*) sebagai fungsi dari parameter λ.

Pada penelitian ini, yang menjadi objek penelitian adalah citra digital yang dapat dihasilkan dari :

- Kamera digital dengan *memory card*.
- WebCam integrated 1.3 MP atau Webcam 1.3 MP dengan USB
- Image Scanner dengan USB.

Citra Digital disimpan dalam *memory card*, memory internal dan memory eksternal dengan menggunakan format standar citra digital seperti table 1. berikut :

Tabel 1. Format Standar Citra Digital

Format	Deskripsi	Recognized Extension	
TIFF	Tagged Image File Format	.tif	.tiff
JPEG	Join Photographics Expert's Group	.jpg	.jpeg
GIF	Graphics Interchange Format	.gif	
BMP	Windows Bitmap	.bmp	
PNG	Portable Network Graphics	.png	
XWD	X-Window Dump	.xwd	

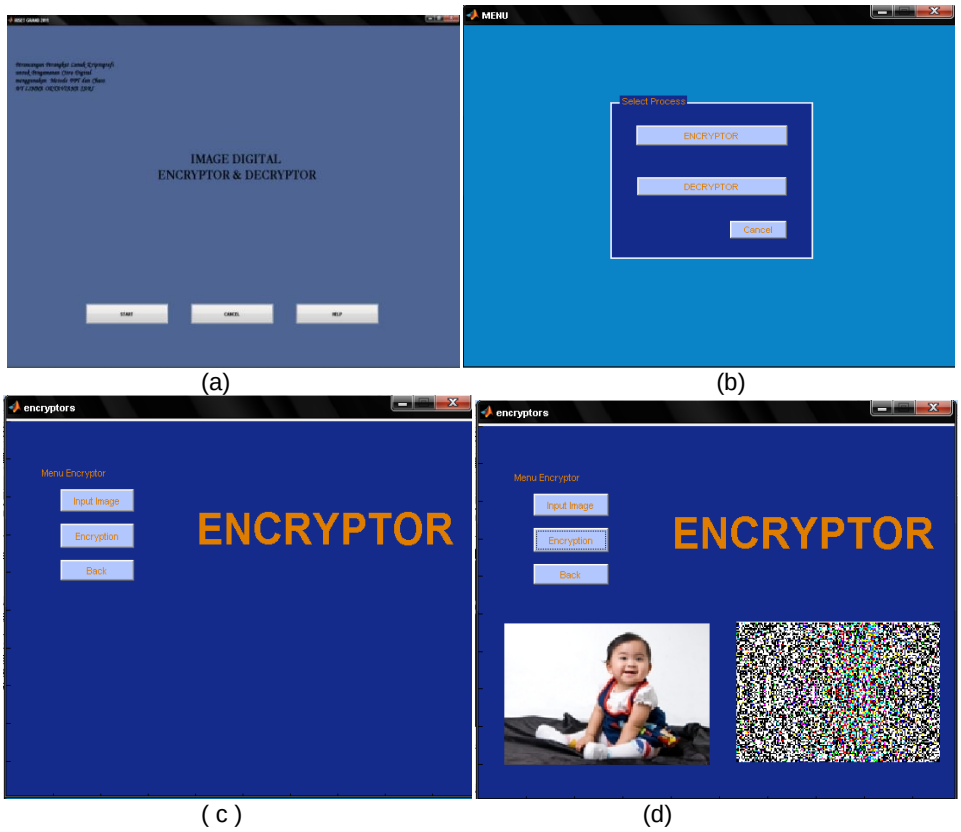
Kemudian citra digital tersebut disesuaikan ukurannya menggunakan *Microsoft Office picture manager* mengikuti kebutuhan di internet.

3.Hasil dan Analisa

Hasil dari perancangan perangkat lunak kriptografi citra digital dengan FFT dan kunci Chaos berupa perangkat lunak yang dapat dijalankan melalui Matlab R2010a. Adapun tahapan untuk menjalankan perangkat lunak tersebut sebagai berikut :

1. Jalankan program matlab.
2. Jalankan aplikasi kriptografi dengan mengetikan "start" pada command window.
3. Maka akan muncul tampilan utama aplikasi seperti Gambar 3(a), kemudian klik "START" untuk masuk ke menu, klik "CANCEL" untuk membatalkan dan keluar dari aplikasi, dan klik "HELP" untuk bantuan.
4. Untuk masuk ke Menu, klik "START", sehingga tampil halaman MENU, seperti Gambar 3(b).Pada halaman MENU terdapat pilihan proses yang akan dilakukan yaitu ENCRYPTOR untuk melakukan proses enkripsi atau DECRYPTOR untuk melakukan proses dekripsi. Sedangkan "CANCEL untuk keluar dari aplikasi.
5. Untuk melakukan proses enkripsi maka klik "ENCRYPTOR", kemudian akan masuk ke halaman encryptors seperti Gambar 3(c).
6. Untuk melakukan proses enkripsi pada citral digital maka klik "Input Image".
7. Kemudian pada halaman encryptors akan muncul citra digital seperti Gambar 3(d), Kemudian klik "Encryption" untuk melakukan proses enkripsi pada citra yang telah diinputkan. Sehingga hasil citra hasil enkripsi menjadi seperti pada bagian kanan Gambar 3(d). Hasil enkripsi image secara otomatis tersimpan dengan nama "ImageEnkripsi.jpg" . Citra dengan nama "ImageEnkripsi.jpg" inilah yang nantinya dikirimkan ke tujuan sehingga aman untuk tidak dilihat atau dibaca oleh orang lain yang tidak berhak mengakses.
8. Disisi penerima "ImageEnkripsi.jpg" ini nantinya akan dilakukan proses dekripsi sehingga akan mengembalikan ke citra digital semula yang dipahami informasinya.

9. Pada aplikasi ini untuk melakukan proses dekripsi maka masuk kebagian MENU, dan klik "DECRYPTOR", setelah itu akan masuk ke halaman decryptors, seperti gambar 4(a), Pada halaman ini untuk melakukan proses dekripsi pada citra yang telah dienkripsi maka klik "Input, kemudian pilih data "ImageEnkripsi.jpg", maka akan muncul citra yang terenkripsi, seperti Gambar 4(b), kemudian klik "Decryption" untuk mendekripsikan citra sehingga menghasilkan citra asli.



Gambar 3.(a) Tampilan utama (splash) aplikasi, (b) Halaman Menu. (c) Halaman Encryptor. (d) Input Citra dan Hasil Enkripsi

Gambar 4(a). Halaman decryptors.(b). Proses Dekripsi.

Setelah dilakukan pengujian pada perangkat lunak, maka dapat dianalisa bahwa Matlab R2010a dapat digunakan untuk memprogramkan algoritma FFT dan Kunci *Chaos*. Algoritma FFT yang digunakan pada perangkat lunak sebagai algoritma enkripsi dapat melakukan proses enkripsi pada citra digital seperti yang terlihat pada gambar 3(d). Algoritma FFT yang digunakan pada perangkat lunak sebagai algoritma dekripsi dapat melakukan proses dekripsi pada citra yang terenkripsi, seperti yang terlihat pada Gambar 4(b). Algoritma FFT bekerja secara simetri karena dapat melakukan proses enkripsi dan dekripsi. Persamaan *Logistik Map* dari *Chaos* dapat digunakan sebagai kunci pada proses enkripsi dan dekripsi seperti yang terlihat pada Gambar 3(d) dan 4(b). Secara keseluruhan perangcangan perangkat lunak kriptografi pada citra digital dengan menggunakan algoritma FFT dan kunci *Chaos* dapat melakukan fungsi pengamanan pada citra digital.

Berikut ini akan dilakukan juga pengujian pada beberapa format, ukuran dan sumber citra yang berbeda:

Tabel 2. Hasil Pengujian untuk Format, Ukuran, sumber yang berbeda.

Format	Ukuran	Sumber	Lama Enkripsi(detik)	Lama Dekripsi(detik)	Status
PNG	448x297	Camera Digital	0.030228	0.041841	Berhasil
JPG	672x1024	Scanner	0.213526	0.173742	Berhasil
TIF	640x480	WebCam	0.070993	0.128195	Berhasil

Berdasarkan hasil pengujian yang ditunjukan pada tabel 2. Maka dapat dianalisa:
1. Perangkat lunak berhasil melakukan proses enkripsi dan dekripsi pada citra digital untuk format, sumber dan ukuran yang berbeda-beda.
2. Untuk ukuran citra digital yang semakin besar maka dibutukan waktu yang lebih lama dalam proses enkripsi maupu proses dekripsi. Hal ini disebakan karena jumlah pixel pada image digital yang ukuran lebih besar, lebih banyak sehingga dibutuhkan waktu yang lebih lama dalam menerapkan algoritma enkripsi/deskripsi serta kunci.
3. Dengan menggunakan metode FFT pada proses enkripsi dan dekripsi dan chaos sebagai kunci, waktu yang dibutuhkan untuk proses enkripsi dan deskripsi sangat cepat yaitu kurang dari 1 detik.

4. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, maka algoritma FFT dan kunci *chaos* yang digunakan pada perancangan perangkat lunak kriptografi citra digital telah berhasil melakukan proses enkripsi dan dekripsi pada citra digital. Proses enkripsi dan dekripsi dengan algoritma FFT dan kunci chaos pada citra digital yang dilakukan perangkat lunak kriptografi yang telah dirancang yaitu kurang dari 1 detik.

Referensi

[1] William Gibson. *Neuromancer:20th Anniversary Edition*. New York:Ace Books, 2004.
[2]. Suhono, Supangkat, H., Juanda, K.. Watermarking Sebagai Teknik Penyembunyian Hak Cipta Pada Data Digital. *Jurnal Departemen Teknik Elektro,* Institut Teknologi Bandung**.**2000.
[3] Melwin Syafrizal, ISO 17799: *Standar Sistem Manajemen Keamanan Informasi*, Seminar Nasional Teknologi *,*2007
[4] Dony Ariyus, *Computer Security*, Yogyakarta : Penerbit ANDI , 2006.
[5] S. R. M. Prasanna, Y. V. Subba Rao and A. Mitra, An Image Encryption Method with Magnitude and Phase Manipulation using Carrier Images, *International Journal of Electrical and Computer Engineering ,* 2006;*1:2* .
[6] Nik Goots, Boris Izotov, Alex Moldovyan, dan Nick Moldovyan, *Modern Cryptography: Protect Your Data with Fast Block Ciphers*, A-List Publishing, 2003.
[7] Fred Piper, Sean Murphy, *Cryptography: A Very Short Introduction*, Oxford University Press, 2002.
[8] Giuseppe Ateniese, Alfredo De Santis, dan Douglas R. Stinson, *On the Contrast in Visual Cryptography Schemes,* 1996.
[10] N. Bourbakis and C. Alexopoulos , Picture data encryption using SCAN patterns. Pattern Recognition 25 6 ,1992.
[11] C.J. Kuo , Novel image encryption technique and its application in progressive transmission. *J. Electron. Imaging 24* ,1993,.
[12] J. Scharinger, Fast encryption of image data using chaotic Kolmogrov flow, *J. Electronic Eng 7*,1998.
[13] J.C. Yen, J.I. Guo, *A new image encryption algorithm and its VLSI architecture,* in: Proceedings of the IEEE workshop signal processing systems, 1999
[14]. Chin-Chen Chang, Min-Shian Hwang, Tung- Shou Chen, "A new encryption algorithm for image cryptosystems", *The Journal of Systems and Software* 58 ,2001.
[15]. C.I, Emmanuel and B.W Jervis, *Digital Signal Processing A practical Approach*, Prentice Hall,2nd, 2001.
[16]. V. Patidar., K.K.Sud. *A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing*, Sir Padmapat Singhania University, Bhatewar, Udaipur – 313 601, India, 2008.