IMPLEMENTASI *DATA ENCRYPTION STANDARD* (DES) PADA *IMAGE WATERMARKING* CITRA MENGGUNAKAN ALGORITMA *DISCRETE COSINE TRANSFORM* (DCT)

IMPLEMENTATION OF DATA ENCRYPTION STANDARD (DES) IN IMAGE WATERMARKING USING DISCRETE COSINE TRANSFORM (DCT) ALGORITHM

Rizqi Muhammad[1], Jangkung Raharjo[2], Nur Andini[3]

[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1] **good.rizqi13@gmail.com,** [2] **jangkung.raharjo@gmail.com**, [3]**nurandini@telkomuniversity.ac.id**

Abstrak

Pencurian dan penyalahgunaan data, merupakan hal yang sangat wajar seiring berkembangnya teknologi. Dengan memanfaatkan teknologi informatika hari ini, dapat memudahkan manusia dalam penyalinan, penyebaran dan pengarsipan data multimedia. Perkembangan jaringan komunikasi digital, dapat memudahkan data-data digital diakses dan tersebar luas oleh khalayak melalui jaringan internet. Banyaknya pengguna internet yang melakukan pertukaran data dengan pengguna lainnya, dapat memungkinkan pertukaran data dilakukan secara ilegal. Untuk melindungi keamanan dan kerahasiaan pemilik data beserta datanya, maka diperlukan suatu teknik untuk menjamin keamanan hal tersebut. *Watermarking* merupakan suatu teknik yang dapat digunakan untuk menyembunyikan pesan atau menandai pesan. Dengan penggunaan teknik pada berbagai jenis data media digital, diharapkan dapat mencegah terjadinya pelanggaran hak cipta atas hasil karya seni dan intelektual. Dalam tugas akhir ini, penulis merancang sistem *watermarking* dengan tujuan menyisipkan pesan informasi berbentuk citra (*.jpeg*) pada gambar (*.jpeg*). Dengan mengkombinasikan algoritma *Discrete Cosine Transform* (DCT) dan *Data Encryption Standar* (DES), dimana *plaintext* merupakan *secret image.* Pada proses sistem yang dirancang berjalan akan dicari nilai *PSNR* dan MSE pada saat *embedding* serta nilai BER pada saat *extraction* dan *decryption.* Hasil penelitian tugas akhir ini adalah sebuah sistem yang dapat menyisipkan sebuah pesan informasi berbentuk citra (*secret image*) ke dalam sebuah gambar (*host image*). Pada hasil uji *avalanche effect* DES, data nilai yang diperoleh membuktikan bahwa DES dapat mengubah isi pesan sebanyak 50% jika *key* masukan diubah 1-bit. Hasil *PSNR* yang didapat memiliki nilai >>30dB, membuat pesan yang disisipkan kasat mata terhadap penglihatan manusia. Uji coba terbaik dilakukan saat *secret image* berukuran 32x32 pixel, dimana nilai rata-rata BER <<0.03.

Kata kunci: *Watermarking*, Kriptografi, *Discrete Cosine Transform*, *Data-Encryption Standar*

Abstract

Data theft and misuse are very common as technology develops. By utilizing informatics technology today, it can facilitate humans in copying, distributing and archiving multimedia data. The development of digital communication networks, can facilitate digital data accessed and widely distributed by the public through the internet network. Many internet users who exchange data with other users, can allow data exchange to be done illegally. To protect the security and confidentiality of data owners and their data, a technique is needed to guarantee the security of this. Watermarking is a technique that can be used to hide messages or mark messages. By using techniques in various types of digital media data, it is expected to prevent copyright infringement on works of art and intellectuals. In this thesis, the author designed a watermarking system with the aim of inserting an information message in the form of an image (.jpeg) in an image (.jpeg). By combining the Discrete Cosine Transform (DCT) algorithm and the Standard Data-Encryption (DES), where the plaintext is a secret image. In the system process that is designed to run will look for the value of *PSNR* and MSE when embed-ding and the value of BER when extraction and decryption. The result of this final project research is a system that can insert an information message in the form of an image (secret image) into an image (host image). In the DES avalanche effect test results, the data values obtained show that DES can change the message content by as much as 50% if the input *key* is changed to 1-bit. *PSNR* results obtained have a value of> 30dB, making the message inserted invisible to human vision. The best test is done when the secret image is 32x32 pixels, where the average value of BER << 0.03.

Key words: Watermarking, Cryptography, Discrete Cosine Transform, Data-Encryption Standar

1. Pendahuluan

Teknologi dalam bidang infomatika memberikan banyak manfaat pada kehidupan manusia. Untuk melindungi hak cipta dan keaslian data, dapat mengaplikasikan teknik *watermarking* pada sebuah data. *Watermarking* itu sendiri merupakan sebuah teknik yang dapat menyisipkan data informasi berupa teks pada data multimedia digital [3]. Teknik dan metode *watermarking* telah banyak diteliti dan dikembangkan agar dapat menjaga kualitas data yang sama dengan data sebelum informasi citra tersebut disisipkan (*embedding*). Dengan penambahan algoritma kriptografi tertentu dalam proses *watermarking*, akan menambahkan keamanan pada data informasi. Metode kriptografi tersebut digunakan untuk melindungi data informasi yang disisipkan atau dapat

digunakan untuk melindungi data multimedia yang dikirimkan. Skema kriptografi sendiri dapat menyembunyikan data informasi yang dikirimkan untuk mendukung keamanan informasi. DES (*Data Encryption Standar*) merupakan salah satu algoritma kriptografi yang populer dan dijadikan sebagai standar algoritma enkripsi yang memiliki jenis kunci simetri [4]. Dalam tugas akhir ini, penulis merancang sistem *watermarking* dengan tujuan menyisipkan pesan informasi berbentuk citra (*.jpg*) pada gambar (*.jpeg*). Dengan mengkombinasikan algoritma *Discrete Cosine Transform* (DCT) dan *Data-Encryption Standar* (DES), dimana *plaintext* merupakan *secret image*. Sebelum *host image* di *embedding encrypted image* (watermark), *secret image* akan melalui proses *encryption* kriptografi dengan metode algoritma DES dengan ukuran 32x32 dan 64x64 piksel. Pada penelitian [1], sistem menyisipkan pesan rahasia dalam *ASCII* pada citra dengan menggunakan metode *Discrete Cosine Transform* (DCT). Pada penelitian tersebut sistem dianalisis dari pengaruh banyak karakter yang disisipkan, letak *embedding* karakter, ketahanan pesan terjadap kompresi gambar, dan ketahanan pesan terhadap perubahan brightness dan contrast. Hasil penelitian tugas akhir ini adalah sebuah sistem yang dapat menyisipkan sebuah pesan informasi berbentuk citra ke dalam sebuah gambar. Pada hasil uji *avalanche effect* DES, data nilai yang diperoleh membuktikan bahwa DES dapat mengubah isi pesan sebanyak 50% jika *key* masukan diubah 1 bit. Hasil PNSR yang didapat memiliki nilai >>30dB, membuat pesan yang disisipkan kasat mata terhadap penglihatan manusia. Uji coba terbaik dilakukan saat citra *watermark* berukuran 32x32 pixel, dimana nilai rata-rata BER <<0.03.

2. Dasar Teori dan Perancangan

A. Watermarking

Watermarking merupakan bentuk dari steganografi, yaitu ilmu yang mempelajari tentang penyembunyian atau penyisipan pesan rahasia pada suatu media sehingga keberadaan pesan tidak dapat terdeteksi oleh indra manusia. Pada digital *watermarking*, pesan data yang akan disisipkan dan medianya merupakan bentuk sinyal digital. Tujuan dasar *watermarking*, yaitu menyisipkan pesan informasi pada suatu media untuk melindungi pesan informasi dan media yang disisipkan informasi.

a. Syarat Kualitas *Watermarking*

Teknik *watermarking* yang baik harus memenuhi kriteria sebagai berikut.

1) *Imperceptible*
2) *Recovery*
3) *Robustness*
4) *Trustworthiness*

b. Batasan dan Gangguan terhadap *Watermarking*

Watermarking merupakan teknik menyembunyikan atau menyisipkan informasi (*watermark*) pada *data host* tetapi tidak sepenuhnya *data host* akan aman. *Watermark* yang disisipkan dapat dipengaruhi oleh batasan-batasan dan juga beberapa faktor (operasi) pada teknik *watermarking*. Menurut M. Kutter dan F. A. P. Petitcolas [2], beberapa operasi yang dapat mempengaruhi *watermark*, yaitu:

1) *JPEG Compression*
2) *Geometric Transformation*
3) *Enhanchement Techniques*

B. Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) merupakan *transform coding* yang mengubah *data byte* ke domain frekuensi dari domain spasial dan mampu memisahkan *data byte* tersebut menjadi dua buah bagian, yaitu frekuensi rendah (koefisien AC) dan frekuensi tinggi (koefisien DC). Untuk menjaga kualitas *data host* agar tidak berubah saat disisipi maka frekuensi tingggi (koefisien DC) akan digunakan sebagai tempat penyisipan informasi (*watermark*). Hal ini dikarenakan frekuensi rendah (koefisien AC) tidak memiliki kapasitas persepsi yang lebih tinggi dari frekuensi tinggi (koefisien DC).

C. Data Encryption Standard (DES)

DES merupakan *system* kriptografi simetri dan tergolong jenis *cipher* blok. DES beroperasi pada ukuran blok 64-bit. DES dapat mengenkripasi 64-bit plainteks dengan keluaran 64-bit chipherteks dengan menggunkan 56 kunci internal atau upa-kunci. Kunci internal di bangkitkan dari kunci eksternal yang panjangnya 64-bit.

Secara global, operasi algoritma DES dimulai dari *plaintext* melakukan proses *initial permutation* (IP) yang akan memisahkan plaintext menjadi 2 blok, yaitu kiri dan kanan. Hasil permutasi akan di-*enchipering* sebanyak 16 putaran dengan kunci yang berbeda-beda seiap putarannya. Hasil *enchipering* akan melakukan proses *invers initial permutation* (IP^{-1}) menjadi blok *ciphertext*.

D. Parameter Pengujian

1) *Bit Error Rate* (BER)

$$BER = \frac{\sum Bit\ salah}{\sum Bit\ total} \quad (1)$$

2) *Mean Square Error* (MSE)

$$MSE = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}[I'(x,y)-I(x,y)]^2}{MxN} \quad (2)$$

3) *Peak Signal to Noise Ratio* (PSNR)

$$PSNR = 10x\log_{10}\left[\frac{Max_{(W(i,j))}{}^2}{\frac{1}{MN}\sum_{i=1,j=1}^{M,N}[W(i,j)-W'(i,j)^2]}\right] \quad (3)$$

4) *Avalanche Effect*

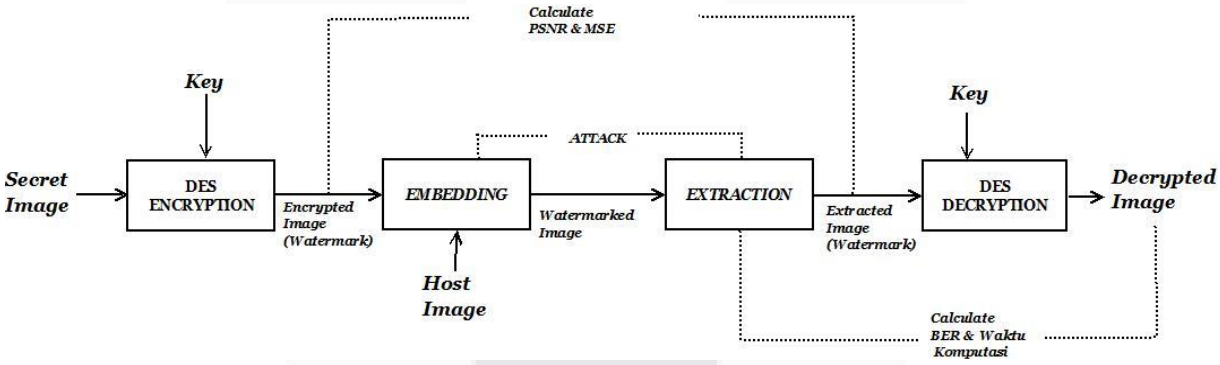
$$BER = \frac{\sum Bit\ setelah\ key\ diubah}{\sum Bit\ sebelum\ key\ diubah} x100\% \quad (4)$$

5) Waktu Komputasi

E. Perancangan Sistem

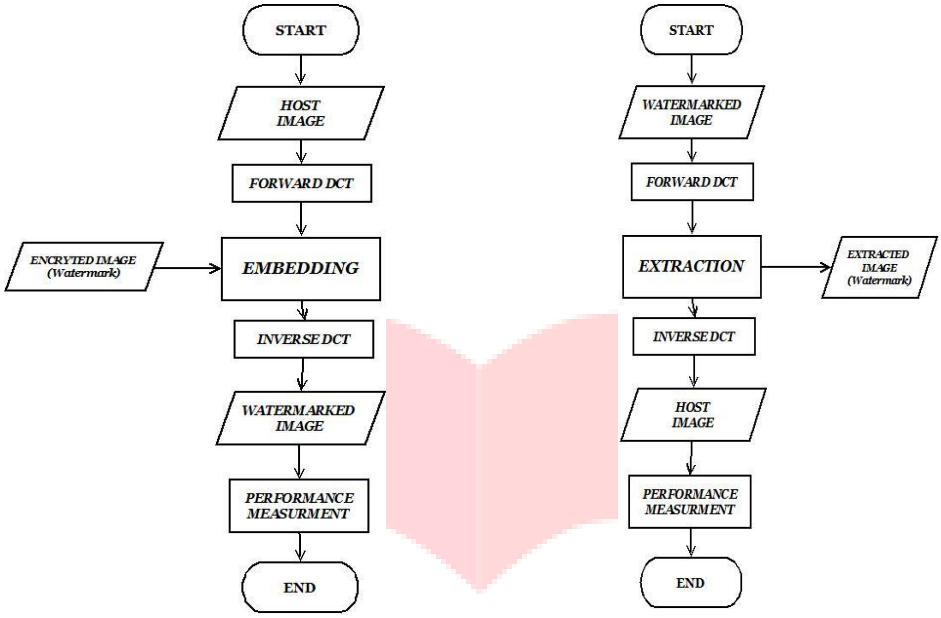
a. Peracangan Model Sistem

Pada gambar 3.1, menggambarkan bahwa model sistem pada *watermarking* terbagi menjadi dua proses penting, yaitu penyisipan (*embedding*) dan pencabutan (*extraction*). Pada proses *embedding*, gambar akan disisipi oleh encrypted image. *Watermarked image* merupakan keluaran dari proses *embedding* yang nantinya akan masuk ke proses ekstraksi. PSNR dan MSE dapat dihitung nilainya setelah *watermarked image* keluar. *Watermarked image* akan diuji kehandalannya dengan serangan rotasi. Kemudian bentuk keluarannya menjadi *extracted image*. Lalu, *extraction image* akan masuk ke proses dekripsi yang keluarannya akan berbentuk *watermark* berformat *.jpg. Untuk memisahkan citra dan *watermark* maka akan dilakukan *decription* yang dimana hasil keluaran tersebut dapat dihitung nilai BER .Gambaran perancangan system DES-DCT dapat dilihat pada gambar berikut:



Gambar 1. Diagram Alir Model Perancangan Sistem

b. Diagram Alir Proses *Embedding* dan Ekstraksi



(a) (b)

Gambar 2. Diagram Alir Proses (a) *Embedding* dan (b) Ekstraksi

3. Pembahasan

Pada tugas akhir ini, menggunakan *grayscale* citra dan *watermark* berupa citra yaitu *secret image*. *Host image* memiliki ukuran 512x512 pixel. Citra *watermark* yang digunakan untuk pada proses enkripsi merupakan citra yang sama dengan 2 buah ukuran yaitu 32x32 pixel dan 64x64 pixel. Berikut adalah citra yang digunakan.

(a) (b)

Gambar 3. (a) *Secret Image* dan (b) *Host Image*

A. Pengujian *Avalanche Effect*

Pengujian memiliki 2 skenario. Pada skenario 1, secret *image* melakukan *encryption* dengan *key* diubah 1 bit, *encrypted image* keluarannya akan dibandingkan dengan *encrypted image* keluaran tanpa adanya bit *key* yang diubah. Pada skenario 2, *secret image* masukan diubah 1-bit tetapi diinginkan bahwa data *secret image* tidak berubah, sehingga nilai *avalanche effect* akan semakin baik jika mendekati nilai nol. Dari data di bawah, menunjukan bahwa baik 1-bit berubah pada *plaintext* maupun pada *key*, sama-sama dapat merubah hasil output enkripsi. Tetapi, dapat dilihat semakin besar ukuran *plaintext* maka akan semakin besar nilai *avalanche effect* dengan *key* yang diubah 1-bit. Selain itu, semakin besar ukuran *plaintext* maka akan semakin kecil pula nilai *avalanche effect* dengan *plaintext* yang diubah 1-bit.

Percobaan ke-	Skenario 1		Skenario 2	
	Ava. Eff 32x32	Ava. Eff 64x64	Ava. Eff 32x32	Ava. Eff 64x64
1	46.7773	50.6104	3.0273	0.7568
2	48.9258	49.7559	3.3203	0.7568
3	48.8281	48.7305	3.3203	0.7568
4	47.6563	49.3896	3.2227	0.7568
5	47.4609	50.3906	3.0273	0.8545
6	51.9531	51.3916	2.6367	0.8301
7	51.1719	50.9277	3.5156	0.8301
8	50.5859	49.1455	3.3203	0.8789
9	50.0977	47.9004	3.125	0.8789
10	51.1719	50.7568	3.6133	0.8789
11	49.6094	50.1221	2.832	0.8789
12	45.8008	50.0488	2.2461	0.7568
13	48.1445	49.6582	2.7344	0.7568
14	50.4883	50.8057	3.7109	0.8545
15	49.8047	50.1221	3.125	0.9766
Rata-Rata	49.23177333	49.98372667	3.11848	0.826813333

Tabel 1. Hasil Pengujian *Avalanche Effect*

B. Pengujian Nilai PSNR, MSE, BER

Pada pengujian ini dinginkan bahwa nilai PSNR lebih dari 30dB agar *watermark yang* disisipkan terlihat kasat mata. Nilai MSE berbanding terbalik dengan nilai PSNR jika nilai MSE besar maka nilai PSNR akan kecil. Pengujian nilai BER dilakukan untuk melihat apakah watermark yang disispkan berubah atau tidak. Semakin nilai 0 maka BER semakin bagus.

Tabel 2. Hasil Pengujian PSNR, MSE, BER

Ukuran File	Nilai Rata-Rata					
	Tanpa diberi serangan rotasi (0)			Dengan diberi serangan rotasi (90)		
	PSNR	MSE	BER	PSNR	MSE	BER
32x32	41.5622	4.5474	0.038	41.5622	0.5474	0.4981
64x64	35.5229	18.2455	0.0376	35.5229	18.2455	0.497

C. Nilai Rata-Rata Komputasi

Tabel di bawah ini menunjukkan hasil perhitungan rata-rata waktu komputasi dari *encryption*, *embedding*, *extraction*, dan *decryption*. Waktu komputasi pada pengujian dibandingkan antara sistem tanpa serangan dengan sistem yang diberi serangan.

Ukuran File	Rata-Rata Waktu Komputasi /Process							
	Tanpa diberi serangan rotasi (0)				Dengan diberi serangan rotasi (90)			
	Encryption	*Embedding*	*Extraction*	*Decryption*	*Encryption*	*Embedding*	*Extraction*	*Decryption*
32x32	2.125	1.8729	1.0073	1.6062	2.125	1.8729	1.0166	1.6177
64x64	4.8438	1.9256	1.5655	4.2666	4.8438	1.9256	1.5917	4.3864

Tabel 3. Hasil Pengujian Waktu Komputasi

4. Kesimpulan

Kesimpulan dari penelitian yang telah dilakukan sebagai berikut.

Dibuktikan dengan hasil data *avalance effect* pada *key* diubah 1-bit mendekati 50% dan pada *secret image* diubah 1-bit mendekati 0%. Jika *key* diubah 1-bit maka 50% *encrypted image* akan berubah dan jika *secret image* diubah 1-bit maka *encrypted image* yang berubah mendekati 0. Kualitas *watermarked image* dapat dilihat dari besarnya nilai PSNR dan MSE hasil dari pengujian *embedding*. Pada metode DCT, PSNR dengan rata-rata 41.5622 dB untuk ukuran *encrypted image* 32x32 piksel dan 35.5229 dB untuk ukuran 64x64 piksel menujukan bahwa performasi sistem cukup baik dengan nilai lebih besar dari 30 dB. Maka keluaran *embedding*, *secret image* kasat pada *host image* terlihat kasat mata oleh pengelihatan manusia. Semakin besar ukuran *watermark* maka akan semakin besar nilai MSE dan semakin besar nilai MSE maka akan semakin kecil nilai PSNR. Dapat dilihat nilai rata-rata MSE untuk ukuran *secret image* 32x32 piksel adalah 4.5474 dan 18,2455 untuk ukuran 64x64 piksel. Maka semakin nilai MSE mendekati nilai nol akan semakin baik. Jumlah piksel pada *watermark* ataupun *host image* sangat memengaruhi kualitas *watermarked image* hasil *embedding* dengan metode DCT. Dimana *secret image* disispkan pada piksel-piksel *host image*, *watermark* berukuran 32x32 piksel memiliki kualitas lebih baik daripada dengan 64x64 pixel. Pada saat diberikan

serangan rotasi, sistem yang dirancang tidak mendapatkan nilai BER sama dengan nol. Waktu komputasi sistem pada percobaan *secret image* 32x32 dan 62x62 yang dirancang tidak memiliki perbedaan yang besar dalam banyaknya jumlah *host image*. Maka waktu komputasi sistem berjalan dengan baik.

Daftar Pustaka:

[1] A. A. Faruqi, dan Imam Fahrur Rozil. "Implementasi *Steganography* Menggunakan Algoritma *Discrete Cosine Transform"*. Jurnal Informatika Polinema. 2015.

[2] M. Kutter and F. A. P. Petitcolas. 1999. A Fair Benchmark for *Image Watermarking* Systems Electronic Imaging '99. Security and *Watermarking* of Multimedia Contents, vol. 3657, The International Society for Optical Engineering, Sans Jose, CA, USA.

[3] I. Setiani, U. Sunarya, S. Aulia. "Modul Simulasi Teknik Watermarking pada Citra Digital Menggunakan Metode DWT dan DCT*"*. 2017.

[4] Rohmanu, Ajar. Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End Of File. Jurnal Informatika SIMANTIK Vol. 1 No. 2, Maret 2017.