ROBUST WATERMARKING PADA CITRA MENGGUNAKAN *FAST DISCRETE CURVELET TRANSFORM, REDUNDANT DISCRETE WAVELET TRANSFORM,* DAN *SINGULAR VALUE DECOMPOSITION*

ROBUST WATERMARKING IN IMAGE USING FAST DISCRETE CURVELET TRANSFORM, REDUNDANT DISCRETE WAVELET TRANSFORM, AND SINGULAR VALUE DECOMPOSITION

Muhammad Fikri Aufa[1], Rita Purnamasari[2], Ledya Novamizanti[3]

[1,2,3] Universitas Telkom, Bandung
[1]aufafikri@student.telkomuniversity.ac.id, [2]**ritapurnamasari@telkomuniversity.ac.id**,
[3]**ledyaldn@telkomuniversity.ac.id**

Abstrak

Perkembangan era yang semakin pesat menciptakan penyebaran data pada internet dalam wujud multimedia khususnya citra akan sangat mudah diambil. Data multimedia tersebut dapat dengan mudah disalin dan disalah gunakan oleh penipu tanpa hak cipta. Teknik *robust watermarking* merupakan solusi untuk mengamankan dan menjaga informasi data multimedia khususnya citra agar *watermark* yang disisipkan akan sulit dihilangkan dan dapat dipulihkan walaupun diubah oleh berbagai jenis serangan. Sistem yang dirancang memiliki dua proses, proses penyisipan dan ekstraksi. Metode *Fast Discrete Curvelet Transform* dan *Redundant Discrete Wavelet Transform* disisipkan pada citra *host*. Kemudian *watermark* disisipkan ke citra dengan cara menerapkan *Discrete Cosine Transform* pada *watermark*, kemudian nilai singular *watermark* dimasukkan ke dalam nilai singular citra *host* menggunakan metode *Singular Value Decomposition*. Sedangkan pada proses ekstraksi, *watermark* akan diekstraksi untuk mengembalikan gambar tanpa merusak citra *host*. Pada penelitian ini citra *host* berupa *grayscale* dengan ukuran 512×512 piksel dan *watermark* berupa data biner dengan ukuran 128×128 piksel. Hasil dari penelitian memperoleh nilai *Peak Signal to Noise Ratio* maksimum sebesar 71,7630 dB, *Structural Similarity Index Metric* maksimum 1, *Normalized Correlation* maksimum 1, dan *Bit Error Rate* 0 yang berarti skema ini memiliki *imperceptibility* yang baik. Skema *watermarking* yang diusulkan dapat bertahan dari serangan kompresi JPEG, *Gaussian noise* dengan *variance* di bawah 0,001, *salt & pepper* dengan *variance* 0,001, *speckle noise* dengan *variance* di bawah 0,003, *Gaussian filtering*, dan *rotation*.

Kata Kunci : ***Discrete Cosine Transform* (DCT), *Fast Discrete Curvelet Transform* (FDCuT), *Redundant Discrete Wavelet Transform* (RDWT), *Singular Value Decomposition* (SVD), *Watermarking***

Abstract

The development of an increasingly rapid era creates the dissemination of data on the internet in the form of multimedia especially images which will be very easy to retrieve. Such multimedia data can be easily copied and misused by fraudsters without copyright. Robust watermarking technique is a solution to secure and maintain multimedia data information, especially images so that the embedded watermark will be difficult to remove and can be recovered even though it is changed by various types of attacks. The designed system has two processes, the embedding process and the extraction process. Fast Discrete Curvelet Transform and Redundant Discrete Wavelet Transform methods are embedd into the host image. Then the watermark is embedd into the image by applying a Discrete Cosine Transform to the watermark, then the singular watermark value is entered into the singular value of the host image using the Singular Value Decomposition method. While in the extraction process, the watermark will be extracted to restore the image without damaging the host image. In this research, the host image is grayscale with a size of 512×512 pixels and a watermark in the form of binary data with a size of 128×128 pixels. The results of the research obtained a maximum Peak Signal to Noise Ratio value of 71,7630 dB, a maximum Structural Similarity Index Metric 1, a maximum Normalized Correlation 1, and a Bit Error Rate 0 which means this scheme has good imperceptibility. The proposed watermarking scheme can withstand JPEG compression attacks, Gaussian noise with variance under 0,001, salt & pepper with variance 0,001, speckle noise with variance below 0,003,Gaussian filtering, and rotation.

Keywords: Discrete Cosine Transform (DCT), Fast Discrete Curvelet Transform (FDCuT), Redundant Discrete Wavelet Transform (RDWT), Singular Value Decomposition (SVD), Watermarking

1. Pendahuluan

Pada masa seperti saat ini, penggunaan komputer digital telah banyak digunakan untuk membantu mempermudah dan mempercepat suatu proses pekerjaan yang sifatnya teratur. Dengan perkembangan komputer yang sangat pesat, data-data dalam bentuk digital semakin banyak digunakan. Penggunaan data digital berbentuk multimedia seperti gambar, video, dan teks dapat ditransfer melalui internet, seluler, dan cloud adalah salah satu contoh dari banyaknya data digital di komputer. Data multimedia dapat dengan mudah disalin dan ditransfer oleh penipu tanpa hak cipta dan data tersebut dapat digunakan di berbagai tempat dengan menggunakan internet, akses seluler dan cloud [1]. Penyebabnya karena data digital selain mudah dalam hal penyebaran, juga disebabkan akan murahnya biaya penggandaan serta penyimpannya untuk digunakan di kemudian hari. Teknik *digital watermarking* adalah solusi yang tepat untuk melindungi data multimedia dan otentikasi hak cipta [2]. *Watermarking* yaitu teknik untuk perlindungan informasi kepemilikan yang disembunyikan di objek multimedia, yang dapat di ekstraksi atau diterjemahkan lebih lanjut untuk tujuan otentikasi [3]. Objek multimedia yang dimaksud bisa dalam bentuk teks, gambar, atau logo. Jenis *watermarking* ada dua yaitu, *Robust watermarking* untuk perlindungan hak cipta atas data multimedia dan *Fragile watermarking* untuk perlindungan hak cipta dan otentikasi data multimedia [1].

Tugas Akhir ini mengacu pada penelitian Khare dkk [4] yang menggunakan metode RDWT-DCT-SVD, skema yang digunakan dinilai sangat baik terhadap serangan *geometric*, *noise*, dan *filtering*. Adapun perbedaan dengan Tugas Akhir ini yaitu menambahkan metode FDCuT. Alasan penambahan metode FDCuT karena berdasarkan penelitian [5] menyatakan bahwa metode FDCuT mampu menghasilkan *imperceptibility*, *robustness*, *security* yang baik sehingga memiliki perlindungan yang kuat dari berbagai jenis serangan *watermarking*. Metode FDCuT pun dapat memberikan transparansi yang lebih baik pada gambar yang disisipkan *watermark*. Metode RDWT dipilih karena DWT memproses citra dengan menguraikannya dalam empat sub-pita yaitu LL, HL, LH, dan HH yang menyebabkan *downsampling* karena invariansi pergeseran yang mengarah pada ekstraksi gambar *watermark* yang tidak tepat, maka digunakan metode RDWT untuk menghindari *downsampling* dan memberikan invariansi shift [4]. Metode DCT dipilih karena mampu memberikan persepsi yang baik dari ketahanan dan tembus pandang [6]. Pemilihan metode SVD karena keunggulan dari metode SVD yaitu memiliki sifat ketersebaran dan stabil yang cocok untuk *watermarking* dan penginderaan kompresi dan hasil nilainya kurang berpengaruh pada kapasitas visualisasi manusia saat dimodifikasi [7].

2. Tinjauan Pustaka

A. Watermarking

Watermarking adalah proses penyematan data menjadi objek sampul multimedia digital sedemikian rupa sehingga *watermark* tersebut dapat dideteksi atau diekstraksi untuk membuat pernyataan tentang keaslian dari objek [8]. Konsep dasar *watermarking* digital sangat erat kaitannya dengan steganografi yang di tekankan *bandwidth* pesan tersembunyi dalam bentuk gambar atau file didalamnya. Namun pada kasus *watermarking*, ketahanan *watermark* adalah parameter performa utama [9].

Watermarking citra dapat dilakukan dalam 2 domain, yaitu domain spasial dan domain frekuensi. Penanaman fungsi domain spasial memberikan kompleksitas komputasi yang rendah dan kapasitas penyematan yang tinggi, akan tetapi ketahanan dan transparansinya lebih buruk. Dalam pendekatan domain frekuensi dapat memastikan kekokohan dan transparansi yang lebih, tetapi mengurangi kapasitas penyematan [10]. Klasifikasi *watermarking* menurut pandangan manusia dapat dibedakan menjadi 2 yaitu *visible watermark* dan *invisible watermark*. *Visible watermark* dapat melindungi konten digital secara dengan lebih aktif, yang sangat berbeda dengan *invisible watermark*. Data digital yang di *embedding* dengan *visible watermark* akan berisi pola hak cipta yang dapat dikenali namun tidak mengganggu dan data dari *host* tersebut tetap ada, sedangkan *invisible watermark* merupakan *watermark* yang disisipkan sedemikian rupa sehingga tidak dapat dilihat oleh mata manusia [11]. Kegunaan dari *invisible watermark* yaitu berfungsi sebagai *integrity verification* dan *copyright protection*.

B. *Redundant Discrete Wavelet Transform (RDWT)*

Redundant Discrete Wavelet Transform (RDWT) adalah properti *shift invariance*. Skema RDWT digunakan untuk mengatasi masalah *shift variant* dari metode DWT [12]. RDWT dapat menghilangkan *downsampling* dan *upsampling* proses transformasi wavelet diskrit. Transformasi ini memberikan proses yang lebih kuat daripada DWT [7]. Seperti pada DWT, penerapan RDWT pada citra digital akan menguraikannya menjadi empat sub-band. Tiap ukuran sub-band sama dengan ukuran citra *host* yang mencapai lebih banyak ketahanan. Karena redundansi dalam domain yang diganti lebih kokoh dalam membawa data *watermarking*. RDWT juga mempunyai dekomposisi yang

terbagi menjadi empat sub-pita yaitu LL, LH, HL, dan HH [12]. Analisis dan sintesis RDWT dapat dituliskan dengan persamaan berikut:

a. Analisis RDWT

$$c_j[k] = \left(C_{j+1}[k] * h_j[-k]\right) \quad (1)$$
$$d_j[k] = \left(C_{j+1}[k] * g_j[k]\right)$$

b. Sintesis RDWT

$$c_{j+1}[k] = \frac{1}{2}(c_j[k] * h_j[k] + d_j[k] * g_j[k]) \quad (2)$$

dengan * menyatakan konvolusi. $h[-k]$ dan $g[-k]$ menunjukkan *low pass* dan *high pass* pada filter analisis. Sedangkan $h[k]$ dan $g[k]$ menunjukkan *low pass* dan *high pass* filter sintesis.

C. *Singular Value Decomposition* (SVD)

SVD adalah sejenis alat untuk menganalisis numerik yang efektif di analisis matriks. *Singular Value Decomposition* (SVD) telah banyak digunakan dalam *watermarking* citra yang kuat. Ide utama dalam metode *watermarking* berbasis SVD adalah untuk menanamkan *watermark* ke dalam nilai singular dengan menerapkan SVD ke blok keseluruhan atau sebagian kecil dari citra. Tidak seperti kebanyakan metode *watermarking* lainnya, SVD dapat digunakan untuk matriks non-persegi karena sifat dekomposisinya yang tidak simetris. Setelah menggunakan transformasi SVD, sebuah matriks dapat dipecah menjadi tiga bagian. Diberikan gambar A dengan berukuran N × N, matriks ini bisa dipisahkan menjadi tiga besar konstitusi utama yaitu [13] :

$$A = USV^T = [u_1, u_2, \dots, u_N] \begin{bmatrix} \Sigma & 0 \\ 0 & 0 \end{bmatrix} [v_1, v_2, \dots, v_N] \quad (3)$$

dengan **'U'** dan **'V'** adalah matriks kesatuan N × N. $[u_1, u_2, \dots, u_N]$ dan $[v_1, v_2, \dots, v_N]$ adalah vektor kolom. **'S'** diagonal matriks yang terdiri dari SV yang disusun dengan format pesan menurun. SVD merupakan analisis terkenal yang dicoba pada citra karena memberikan stabilitas yang sangat baik sedangkan SV_S tidak memberikan perubahan pada sedikit modifikasi yang dicoba pada citra semacam terjemahan, pergeseran, dan lain-lain yang dapat meningktakan ketahanan pada algoritme.

D. *Fast Discrete Curvelet Transform* (FDCuT)

FDCuT digunakan pada suatu citra untuk mendapatkan berbagai *subband* frekuensi. FDCuT berperan penting pada pengaplikasian *image processing* seperti mempresentasikan suatu citra menjadi sisi atau sudut [5]. Metode ini mengambil dari *Cartesian arrays* yang memungkinkan keluarn sebagai kumpulan koefisien sebagai berikut [14]:

$$C^D(j,l,k) \coloneqq \Sigma 0 \ \leq t_1, t_2 < nf[t_1, t_2] \emptyset j, l, k[t_1, t_2] \quad (4)$$

dengan j = 0, 1, 2, … merupakan parameter skala, l = 0, 1, 2, … merupakan parameter orientasi, dan $k = (k_1, k_2) \in Z^2$ merupakan parameter translasi. Parameter skala berdasarkan pada ukuran citra yang digunakan dan dihitung dari $\log_2(Min(M.N) - 3)$, dimana M dan N adalah ukuran baris dan kolom dari citra dan parameter orientasi harus kelipatan 4 atau *default* yang bisa digunakan yaitu 16 [14]. Transformasi curvelet dibagi menjadi 2 tipe yaitu *Uniqui Spaced Fast Fourier Transform (USFFT) based* FDCuT dan *Frequency Wrapping based* FDCuT. USSFT *based* FDCuT bersifat memiliki ukuran sampel tidak sama, rumit dan membutuhkan banyak waktu untuk komputasi. *Frequency Wrapping based* FDCuT mempunyai sifat lebih mudah diimplementasikan, lebih sederhana untuk dipahami, dan waktu komputasi lebih cepat dibanding USFFT. Jika *Frequency Wrapping* diaplikasikan ke dalam gambar, dapat menghasilkan 3 sub-bands frekuensi berbeda yaitu *Low Frequency* (LF), *Middle Frequency* (MF), dan *High Frequency* (LF) [5].

E. *Discrete Cosine Transform* (DCT)

DCT hanya mempunyai transformasi ortogonal dari bilangan real. Matriks DCT mempunyai kemiripan dengan matriks *Toeplitz* yaitu matriks koefisien simetris dengan penjumlahan yang sama antara tiap diagonal bantu dan yang sejajar dengan diagonal. DCT sendiri telah disediakn oleh item yang diekstraksi dengan cosinus dalam tranformasi fourier diskrit [15]. Sepanjang transformasi berjalan, bagian-bagian yang relevan citra terkonsentrasi jadi sebagian frekuensi rendah komponen dengan transformasi diberikan sebagai berikut [10]:

$$F(u,v) = \frac{2}{\sqrt{mn}} C(u)C(v) \sum_{x=0}^{y-1} \sum_{y=0}^{N-1} f(x,y).cos\frac{(2x+1)u\pi}{2m} \times cos\frac{(2y+1)v\pi}{2n} \quad (5)$$

Dan transform invers diberikan sebagi berikut:

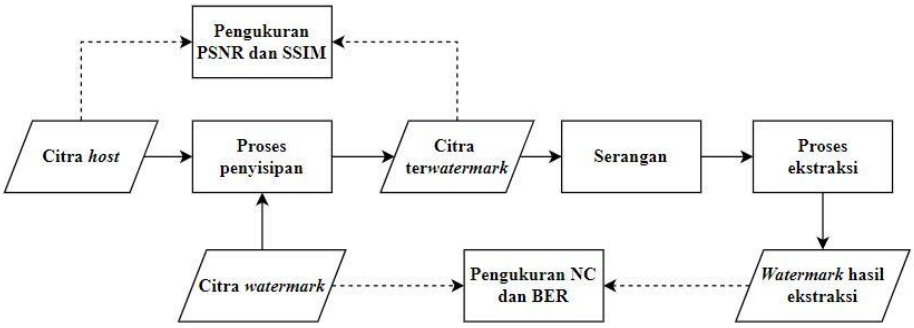
$$f(x,y) = \frac{2}{\sqrt{mn}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} C(u)C(v)f(m,n).cos\frac{(2x+1)u\pi}{2m} \times cos\frac{(2y+1)v\pi}{2n}$$
$$C(u), C(v) = \begin{cases} \frac{1}{\sqrt{2}} & if\ (u,v) = 0 \\ 1 & else. \end{cases} \quad (6)$$

Koefisien pada citra dengan DCT kebanyakan bernilai nol. Bagian citra dengan frekuensi yang lebih rendah mempunyai nilai yang lebih besar, sebaliknya bagian citra dengan frekuensi tengah serta frekuensi yang lebih besar mempunyai nilai tengah serta nilai yang lebih kecil. Dalam hal tersebut maka digital *watermarking* bisa disematkan kebagian citra dengan tengah dan frekuensi yang lebih kecil. Penyematan ini bisa menahan serangan kompresi JPEG dengan lebih banyak data tersemat [15].

3. Perancangan Sistem

A. Desain Sistem

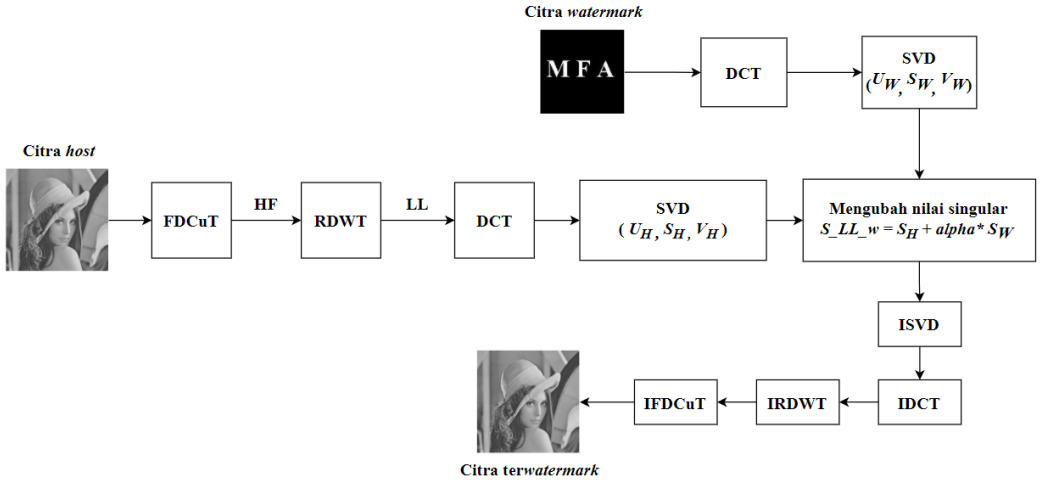
Pada Tugas Akhir ini dilakukan proses perancangan sistem *watermarking* pada citra. Citra *host* yang digunakan adalah citra dengan format *grayscale*, sedangkan untuk citra *watermark* menggunakan format biner. Citra *host* memiliki ukuran 512×512 piksel dan citra *watermark* memiliki ukuran 128×128 piksel. Sistem akan dirancang menjadi dua proses, yang pertama yaitu proses penyisipan (*embedding*) dan proses yang kedua yaitu ekstraksi *watermark* (*extraction*). Pada proses penyisipan akan menghasilkan sebuah citra ter-*watermark* yang diperoleh dari penyisipan citra *watermark* ke citra *host*. Setelah dilakukan proses penyisipan, akan dilihat kualitas citra ter-*watermark* dengan menggunakan perhitungan nilai PSNR dan SSIM. Kemudian pada proses kedua yaitu proses ekstraksi, citra ter-*watermark* di pisahkan menjadi citra *watermark* kembali. Kemudian dilihat kualitas citra *watermark* hasil ekstraksi dengan mencari nilai NC dan BER.



Gambar 2. Diagram blok sistem *watermarking*.

B. Proses Penyisipan

Pada proses ini, dilakukan proses penyisipan sinyal berupa citra *watermark* ke citra *host*. Adapun prosesnya dapat dilihat pada diagram blok yang ditampilkan pada Gambar 3.

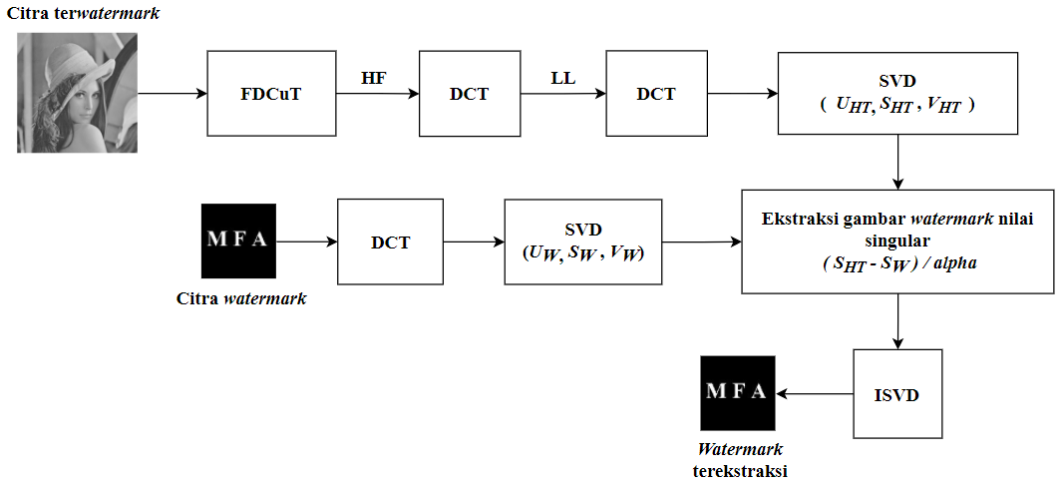


Gambar 3. Diagram blok proses penyisipan *watermark*.

Berdasarkan Gambar 3, proses penyisipan dilakukan dengan menerapkan FDCuT dan memilih *high frequency curvelet coefficient* pada citra *host*. Kemudian menerapkan RDWT pada citra *host* untuk mendapatkan sub-band LL. Setelah itu, terapkan DCT dengan blok 8×8 pada citra *host* dan citra *watermark*. Sisipkan gambar *watermark* ke dalam citra *host* menggunakan SVD, ubah nilai singular citra *host* pada sub-band LL dengan nilai singular gambar *watermark* yang sudah di terapkan SVD. Setelah itu, lakukan *inverse* SVD, DCT, RDWT, dan FDCuT untuk mendapatkan band LL yang sudah termodifikasi lalu citra ter*watermark* akan didapatkan.

C. Proses Ekstraksi

Proses ekstraksi merupakan proses pemisahan citra *host* dengan *watermark* yang telah disisipkan sebelumnya. Untuk prosesnya dapat dilihat pada Gambar 4.



Gambar 4. Diagram blok proses ekstraksi *watermark*.

Berdasarkan Gambar 4, proses ekstraksi dilakukan dengan menerapkan FDCuT dan memilih *high frequency curvelet coefficient* pada citra ter*watermark*. Lalu menerapkan transformasi RDWT pada citra ter*watermark* dan *watermark* untuk mendapatkan sub-band LL. Selanjutnya menerapkan transformasi DCT di sub-band LL kemudian terapkan SVD pada hasil sub-band LL yang telah di DCT pada citra ter*watermark* dan *watermark*. Setelah itu, lakukan *inverse* pada SVD untuk merekonstruksi *watermark* yang sudah terekstraksi dan citra *watermark* awal akan didapatkan.

4. Simulasi *Watermarking*

Pada penelitian ini, akan diuji dan dianalisis menggunakan citra *host* dengan format grayscale berukuran 512×512 piksel. Sedangkan untuk citra *watermark* yang digunakan merupakan citra biner berukuran 128×128 piksel. Citra *host* dan *watermark* yang digunakan dapat dilihat pada Gambar 5.

(a) (b)

Gambar 5. (a) Citra *host*, (b) *watermark*

A. Hasil Pengujian Tanpa Serangan

Pengujian ini menggunakan ukuran citra *host* berupa *grayscale* dengan ukuran 512×512 piksel dan citra *watermark* berupa biner berukuran 128×128 piksel tanpa melalui serangan. Pengujian ini dilakukan untuk mengetahui nilai dari parameter PSNR dan SSIM saat proses penyisipan. Pengujian ini pula akan menghitung nilai dari parameter NC dan BER saat proses ekstraksi. Adapun hasil performa PSNR1, SSIM, NC, dan BER dapat dilihat pada Tabel 1.

Tabel 1. Hasil Pengujian Tanpa Serangan

Jenis *Watermark*	PSNR1	SSIM	NC	BER	Capacity
Logo	54,6634	0,9944	1,0000	0	0,0313
Inisial Nama	67,9567	0,9998	1,0000	0	0,0313

Berdasarkan Tabel 1, hasil pengujian tanpa serangan menggunakan *watermark* logo menghasilkan nilai rata-rata PSNR, SSIM, NC, dan BER dari 5 citra yang diuji, yaitu nilai PSNR1 sebesar 54,6634 dB, SSIM 0,9944, NC 1, dan BER 0. Sedangkan untuk *watermark* inisal nama menghasilkan nilai rata-rata PSNR, SSIM, NC, dan BER dari 5 citra yang diuji, yaitu nilai PSNR1 sebesar 67,9567 dB, SSIM 0,9998, NC 1, dan BER 0. Hasil pengujian tanpa serangan ini dapat menunjukkan bahwa skema *watermarking* yang diusulkan memiliki kualitas yang baik, karena nilai rata-rata PSNR1 dan SSIM yang dihasilkan cukup baik, nilai NC yang dihasilkan maksimal 1, serta nilai BER 0 yang menandakan bahwa tingkat kesalahan bit setelah proses dari ekstraksi *watermark* tidak ada.

B. Hasil Pengujian Menggunakan Serangan

Pengujian dan analisis pengaruh serangan pada skema *watermarking* ini bertujuan untuk mengetahui seberapa *robust* sistem yang telah dibuat. Pengujian ini menggunakan citra *host* berukuran 512×512 piksel dan citra *watermark* berukuran 128×128 piksel. Serangan yang akan diberikan yaitu sebagai berikut:

1. Kompresi JPEG = *Quality* 30, 50, dan 70.
2. *Noise addition attack*, yaitu: *Salt & Pepper Noise* (*Variance* = 0,001), *Speckle Noise* (*Variance* = 0,001), dan *Gaussian Noise* (*Mean* = 0, *Variance* = 0,0001).
3. *Filtering attack*, yaitu: *Median Filter* (3×3), *Gaussian filter* (3×3), dan *Mean Filter*.
4. *Geometric attack*, yaitu: *Rotation* 90°, *Scalling attack*, dan *Cropping*.
5. Serangan pemrosesan sinyal, yaitu: *Motion Blur*, *Image Sharpening*, dan *Histogram Equalization*.

C. Hasil Pengujian dan Analisis Serangan Kompresi JPEG

Tabel 2. Hasil Pengujian Serangan Kompresi JPEG

Quality	PSNR2	SSIM	NC	BER
30	30,3101	0,7758	1	0,0268
50	32,8759	0,8409	1	0,0217
70	34,5093	0,8738	1	0,0307

Tabel 2 merupakan hasil pengujian serangan kompresi JPEG dengan *quality* yang berbeda, yaitu 30, 50, 70. Pada *quality* 30 diperoleh nilai PSNR2 sebesar 30,3101 dB, SSIM sebesar 0,7758, NC sebesar 1, dan BER sebesar 0,0268. Pengujian dengan *quality* 50 diperoleh nilai PSNR2 sebesar 32,8759 dB, SSIM sebesar 0,8409, NC sebesar 1, dan BER sebesar 0,0217. Selanjutnya untuk pengujian dengan *quality* 70 diperoleh nilai PSNR2 sebesar 34,5093 dB, SSIM sebesar 0,8738, NC sebesar 1, dan BER sebesar 0,0307. Saat pengujian menggunakan serangan kompresi JPEG, terjadi perubahan pada nilai performa. Semakin besar *quality* yang diberikan, maka semakin besar pula nilai performa yang dihasilkan. Berdasarkan hasil pengujian tersebut, skema ini tahan terhadap serangan kompresi JPEG karena *watermark* ter-ekstraksi masih terlihat jelas yang ditunjukkan melalui nilai NC dan BER yang dihasilkan masih cukup baik.

D. Hasil Pengujian dan Analisis Serangan *Noise Addition*

Tabel 3. Hasil Pengujian Serangan *Noise Addition*

Serangan	PSNR2	SSIM	NC	BER
Speckle noise	36,0495	0,8565	0,9577	0,0333
Salt & pepper	35,4530	0,9765	0,9557	0,0341
Gaussian noise	39,8088	0,8884	0,9554	0,0341

Tabel 3 merupakan hasil pengujian serangan *noise addition*. Pada saat diberi serangan *speckle noise* diperoleh nilai PSNR2 sebesar 36,0495 dB, SSIM 0,8564, NC 0,9577, dan BER 0,0333. Untuk pengujian serangan *salt & pepper* menggunakan *watermark* inisial diperoleh nilai PSNR2 sebesar 35,4530 dB, SSIM 0,9765, NC 0,9577, dan BER 0,0341. Kemudian pengujian serangan *gaussian noise* menggunakan *watermark* inisial diperoleh nilai PSNR2 sebesar 39,8088 dB, SSIM 0,8884, NC 0,9554, dan BER 0,0341. Skema watermarking ini *tahan terhadap serangan* noise addition karena memiliki *imperceptibility* yang baik yang ditunjukkan melalui nilai PSNR2 diatas. Skema ini tahan terhadap serangan *noise addition* karena *watermark* ter-ekstraksi yang ditunjukkan melalui nilai NC dan BER yang dihasilkan masih cukup baik.

E. Hasil Pengujian dan Analisis Serangan *Filtering*

Tabel 4. Hasil Pengujian Serangan *Filtering*

Serangan	PSNR2	SSIM	NC	BER
Median Filtering	26,2973	0,7511	0,1035	0,0336
Mean Filtering	25,6431	0,7604	0,1624	0,0263
Gaussian Filtering	34,7838	0,9673	0,6055	0,0358

Tabel 4 merupakan hasil pengujian serangan *filtering*. Pada saat diberi serangan *median filtering* diperoleh nilai PSNR2 sebesar 26,2973 dB, SSIM 0,7511, NC 0,1035, dan BER 0,0336. Untuk pengujian serangan *mean filtering* menggunakan *watermark* inisial diperoleh nilai PSNR2 sebesar 25,6431 dB, SSIM 0,7604, NC 0,1624, dan BER 0,0263. Kemudian pengujian serangan *gaussian filtering* menggunakan *watermark* inisial diperoleh nilai PSNR2 sebesar 34,7838 dB, SSIM 0,9673, NC 0,6055, dan BER 0,0358. Pada pengujian terhadap serangan *filtering*, *watermark* hasil ekstraksi dari ketiga jenis serangan masih dapat terlihat cukup jelas, tetapi mengalami banyak kerusakan. Oleh karena itu, berdasarkan hasil pengujian dan analisis skema ini tidak tahan terhadap jenis serangan *filtering* karena nilai NC dan BER yang dihasilkan kurang baik.

F. Hasil Pengujian dan Analisis Serangan *Geometric*

Tabel 5. Hasil Pengujian Serangan *Geometric*

Serangan	PSNR2	SSIM	NC	BER
Rotation	10,8824	0,0048	0,9497	0,0316
Scalling Attack	26,7563	0,7446	0,2327	0,0600
Cropping	9,5805	0,0077	0,1280	0,0602

Tabel 5 merupakan hasil pengujian serangan *geometric*. Pada saat diberi serangan *rotation* diperoleh nilai PSNR2 sebesar 10,8824 dB, SSIM 0,0048, NC 0,9497, dan BER 0,0316. Untuk pengujian serangan *scalling Attack* menggunakan *watermark* inisial diperoleh nilai PSNR2 sebesar 26,7563 dB, SSIM 0,7446, NC 0,2327, dan BER 0,0600. Kemudian pengujian serangan *cropping* menggunakan *watermark* inisial diperoleh nilai PSNR2 sebesar 9,5805 dB, SSIM 0,0077, NC 0,1280, dan BER 0,0602. Pada saat pengujian serangan *rotation* dan *cropping*, hasil PSNR2 dan SSIM masih sangat jauh dari rata-rata, dikarenakan serangan *geometric* dapat mengubah bentuk asli dari citra. Dari hasil analisis, skema yang digunakan tidak mampu bertahan dari serangan *geometric*, dikarenakan hasil parameter yang masih jauh di atas rata-rata.

G. Hasil Pengujian dan Analisis Serangan Pemrosesan Sinyal

Tabel 6. Hasil Pengujian Serangan Pemrosesan Sinyal

Serangan	PSNR2	SSIM	NC	BER
Blurring	29,5053	0,0048	0,3558	0,0334

Histogram Equalization	19,3431	0,7446	0,4980	0,0384
Sharpening	28,6740	0,0077	0,4133	0,0344

Tabel 6 merupakan hasil pengujian serangan pemrosesan sinyal dengan jenis serangan yang berbeda. Pada serangan *blurring* menghasilkan PSNR2 sebesar 29,5053 dB, SSIM 0,0048, NC 0,3558, dan BER 0,0334. Pada serangan *histogram equalization* menghasilkan PSNR2 sebesar 19,3431 dB, SSIM 0,7446, NC 0,4980, dan BER 0,0384. Terakhir pada pengujian serangan *sharpening* menghasilkan PSNR2 sebesar 28,6740dB, SSIM 0,0077, NC 0,4133, dan BER 0,0344. Pada saat pengujian serangan *histogram equalization* nilai PSNR yang didapatkan sangat rendah, dikarenakan serangan *histogram equalization* akan meningkatkan kontras pada citra yang akan sangat merubah citra tersebut. Hasil *watermark* terekstraksi dari ketiga jenis serangan masih bisa terlihat cukup jelas, akan tetapi nilai NC yang didapatkan masih sangat buruk. NC digunakan untuk mengukur ketahanan pada sistem *watermarking*. Jika nilai yang didapat bernilai 0 atau mendekati maka sistem *watermarking* mempunyai kekuatan yang rapuh, sedangkan jika mendapat nilai 1 maka sistem *watermarking* dapat dikatakan kuat.

5. Kesimpulan

Tugas Akhir ini telah merancang dan mensimulasikan skema *watermarking* menggunakan metode FDCuT-RDWT-DCT-SVD yang dapat digunakan untuk membuat *watermark* yang *robust* dan mampu memberikan ketahan pada citra dari berbagai jenis serangan. Pengujian tanpa serangan dengan metode FDCuT-RDWT-DCT-SVD menghasilkan performa rata-rata nilai PSNR sebesar 67,9567 dB, SSIM 0,99982, NC 1, dan BER 0. Berdasarkan hasil pengujian, skema ini menandakan bahwa sistem *watermarking* yang diujikan memiliki *imperceptibility* dan *robustness* sehingga dapat memberikan keamanan dan ketahanan pada citra. Pada saat citra ter*watermark* diberikan serangan kompresi JPEG menggunakan *quality* 30, 50, dan 70, skema *watermarking* dapat bertahan dari serangan kompresi JPEG karena nilai NC dan BER yang dihasilkan cukup baik dan gambar *watermark* terekstraksi masih dapat dilihat dengan jelas. Pada serangan *noise addition*, skema ini tahan terhadap serangan *speckle noise*, *salt & pepper noise*, dan *Gaussian noise* karena *watermark* ter-ekstraksi masih terlihat jelas yang ditunjukkan melalui nilai NC dan BER yang dihasilkan masih cukup baik. Selanjutnya pada pengujian terhadap serangan *filtering*, *watermark* hasil ekstraksi dari ketiga jenis serangan masih dapat terlihat cukup jelas, tetapi mengalami banyak kerusakan. Oleh karena itu, berdasarkan hasil pengujian dan analisis skema ini tidak tahan terhadap jenis serangan *filtering* karena nilai NC dan BER yang dihasilkan kurang baik. Kemudian untuk pengujian serangan *geometric*, skema yang diusulkan tidak mampu bertahan dari dua jenis serangan *geometric* yang diberikan, yaitu *scalling attack* dan *cropping* karena hasil *watermark* terekstraksi yang dihasilkan tidak begitu jelas dan nilai NC dan BER yang cukup buruk. Pada pengujian pemrosesan sinyal, *watermark* terekstraksi dari ketiga jenis serangan masih bisa terlihat cukup jelas, akan tetapi nilai NC dan BER yang didapatkan masih sangat buruk.

Referensi

[1] F. Faizel and N. Vishwanath, "Noval Hybrid System Compressor Based Watermarking Scheme For Security Of Multimedia Data," *International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR)*, pp. 1-6, 2018.

[2] R. Thanki, V. Dwivedi and K. Borisagar, "A hybrid watermarking scheme with CS theory for security of multimedia data," *Journal of King Saud University – Computer and Information Sciences*, vol. 31, pp. 436-451, 2017.

[3] V. V. K, J. Lal G, V. Prabhu S, S. Kumar S and S. K. P, "A Robust Watermarking method based on Compressed Sensing and Arnold scrambling," in *International Conference on Machine Vision and Image Processing (MVIP)*, India, 2012.

[4] P. Khare and V. K. Srivastava, "Robust digital image watermarking scheme based on RDWT-DCT-SVD," *2018 5th International Conference on Signal Processing and Integrated Networks (SPIN). IEEE*, pp. 88-93, 2018.

[5] R. Thanki, S. Borra, V. Dwivedi and K. Borisagar, "An efficient medical image watermarking scheme based on FDCuT–DCT," *Engineering Science and Technology*, vol. 20, pp. 1366-1379, 2017.

[6] I. Assini, A. Badri, K. Safi, A. Sahel and A. Baghdad, "A Robust Hybrid Watermarking Technique for Securing Medical Image," *International journal of Intelligent Engineering & Systems,* vol. 11, no. 3, pp. 169-176, 2018.

[7] R. Thanki, V. Dwivedi, K. Borisagar and S. Borra, "A Watermarking Algorithm for Multiple Watermarks Protection Using RDWT-SVD and Compressive Sensing," *Informatica ,* vol. 41, no. 4, pp. 479-493, 2017.

[8] S. P. Mohanty, "Watermarking of Digital Images," Indian institute of science bangalore, India, 1999.

[9] A. K. Singh, B. Kumar, G. Singh and A. Mohan, Digital Image Watermarking: Concepts and Applications, India: Springer International Publishing AG 2017, 2017.

[10] K. K. Neetha and A. M. Koya, "A Compressive Sensing Approach to DCT Watermarking System," in *International Conference on Control, Communication & Computing India (ICCC)*, India, 2015.

[11] C.-H. Huang and J.-L. Wu, "Attacking visible watermarking schemes," *IEEE transactions on multimedia,* vol. 6, no. 1, pp. 16-30, 2004.

[12] T. H. Rassem, N. M. Makbol and B. E. Khoo, "Performance Evaluation of RDWT-SVD and DWT-SVD Watermarking schemes," in *AIP Conference Proceedings*, Penang, 2016.

[13] Z. Zhang, C. Wang and Z. Xiao, "Image Watermarking Scheme Based on Arnold Transform and DWT-DCT-SVD," in *IEEE 13th International Conference on Signal Processing (ICSP)*, China, 2016.

[14] R. M. Thanki, V. J. Dwivedi and K. R. Borisagar, "Multibiometric Watermarking Technique Using Fast Discrete Curvelet Transform (FDCuT) and Discrete Cosine Transform (DCT)," in *Multibiometric Watermarking with Compressive Sensing Theory*, India, Springer International Publishing AG 2018, 2018, pp. 137-160.

[15] S. Liu, Z. Pan and H. Song, "Digital image watermarking method based on DCT and fractal encoding," *IET Image processing,* vol. 11, no. 10, pp. 815-821, 2017.

[16] S. M. Mousavi, A. Naghsh and S. A. R. Abu-bakar, "Watermarking techniques used in medical images: a survey," *Journal of digital imaging,* vol. 27, no. 6, pp. 714-729, 2014.