Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.2023106138
Vol. 10, No. 2, April 2023, hlm. 449-456 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

KETAHANAN DAN KUALITAS VISUAL WATERMARKED IMAGE MENGGUNAKAN INTEGER WAVELET TRANSFORM (IWT) DAN CHINESE REMAINDER THEOREM (CRT)

Bambang Harjito[*1], Eka Tri Kustanti[2]

[1,2]Universitas Sebelas Maret, Surakarta
Email: [1]bambang_harjito@staff.uns.ac.id, [2]ekauns2015@student.uns.ac.id
[*]Penulis Korespondensi

(Naskah masuk: 07 Februari 2022, diterima untuk diterbitkan: 12 April 2023)

Abstrak

Kemudahan untuk mengakses dan berbagi media digital saat ini menimbulkan kekhawatiran mengenai pelanggaran hak cipta atau pembajakan. Sehingga perlu untuk memberikan identitas kepada setiap media digital agar tidak mudah dibajak atau diklaim oleh pihak-pihak yang tidak bertanggung jawab. Salah satu cara untuk memberikan identitas pada suatu media digital tanpa mengurangi kualitas dari medianya sendiri yaitu dengan menggunakan digital watermarking. Pada paper ini mengusulkan metoda digital watermarking dengan menggunakan gabungan *Integer Wavelet Transform* (IWT) dan *Chinese Remainder Theorem* (CRT) untuk untuk menghasilkan watermarking dengan kualitas visual dan ketahanan yang baik dari beberapa serangan. Hasil penelitian diperoleh nilai-nilai *Peak Signal-to-Noise Ratio* (PSNR) mendekati 1 dan *Normalized Correlation Coefficient* (NCC) sama dengan 0,71337, menunjukkan metode IWT dan CRT mampu menghasilkan watermarked image dengan kualitas visual atau *imperceptibility* yang baik dan mampu memberikan ketahanan image terhadap beberapa serangan seperti gaussian, salt & pepper dan kompresi JPEG2000 tetapi tidak tahan terhadap serangan rotasi dan kontras karena nilai NCC dibawah 0,5.

Kata kunci: *PSNR, NCC, IWT, CRT, Watermark image*

ROBUSTNESS AND VISUAL QUALITY OF WATERMARKED IMAGE USING INTEGER WAVELET TRANSFORM (IWT) AND CHINESE REMAINDER THEOREM (CRT)

Abstract

Today's ease of accessing and sharing digital media raises concerns about copyright infringement or piracy. So it is necessary to give identity to each digital media so that it is not easily hijacked or claimed by irresponsible parties. One way to give identity to a digital media without reducing the quality of the media itself is to use digital watermarking. This paper proposes a digital watermarking method using a combination of Integer Wavelet Transform (IWT) and Chinese Remainder Theorem (CRT) to produce watermarking with good visual quality and resistance from several attacks. The results obtained that Peak Signal-to-Noise Ratio (PSNR) values are close to 1 and Normalized Correlation Coefficient (NCC) equal to 0.71337. shows the IWT and CRT methods are able to produce watermarked images with good visual quality or imperceptibility and are able to provide image resistance to several attacks such as gaussian, salt & pepper and JPEG2000 compression but are not resistant to rotation and contrast attacks because the NCC value is below 0.5.

Keywords: *PSNR, NCC, IWT, CRT, Watermark image*

1. PENDAHULUAN

Kemudahan untuk mengakses dan berbagi konten digital saat ini menimbulkan kekhawatiran mengenai pelanggaran hak kepemilikan atau pembajakan (Adi, Rahmanti et al. 2018). Konten digital perlu memiliki identitas maka untuk mengidentifikasi kepemilikan dari konten digital tersebut, salah satu cara adalah dengan menggunakan *digital watermarking.* Penggunaan digital watermarking mempunyai tujuan agar supaya pihak yang tidak bertanggung jawab tidak bisa menuntut kepemilikan.. *Digital watermarking* adalah suatu proses penyisipan *watermark* atau data rahasia ke dalam media digital untuk mengidentifikasi pemilik dari media tersebut(Shih, 2017). *Watermark* yang telah disisipkan ke media digital lain maka mata

manusia tidak dapat melihat dan kualitas konten data yang disisipi tidak berpengaruh dengan *watermark*. Proses watermarking terdiri dari dua langkah utama, yaitu penyisipan *watermark* dan ekstraksi *watermark*.

Terdapat dua kategori pada metode watermarking, yaitu *spatial domain* dan *transform domain* (Poonam & Arora, 2018). Pada *spatial domain,* watermark langsung disisipkan ke dalam setiap *pixel* sehingga mempunyai kompleksitas yang kecil tetapi tingkat ketahanannya rendah. Salah satu algoritma pada *spatial domain* adalah *Chinese Remainder Theorem* (CRT) (Nugraha et al., 2017) dan (Wagdarikar et al., 2019). Sedangkan pada *transform domain*, *watermark* disisipkan ke dalam *pixel* yang ditransformasi yang disebut koefisien dalam beberapa level frekuensi sehingga mempunyai tingkat ketahanan yang lebih baik. *Wavelet transform* merupakan salah satu metode transformasi pada *transform domain*, (Sundararajan, 2017) dan (Sudibyo et al., 2017)

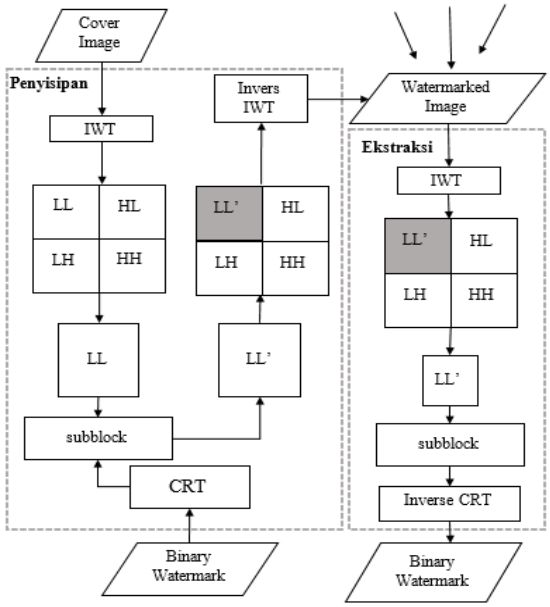
. Jurnal penelitian berikutnya oleh Hannoun (Hannoun, Hamiche et al. 2018). Pada penelitian ini original image dienkripsi dengan menggunakan peta modified henon dan discrete-time chaotic system untuk disisipkan ke dalam domain DWT pada host image. transmisi berdasarkan sinkronisasi dari discrete-time chaotic system. Untuk meningkatkan ketahanan dari serangan peretas, watermark disisipkan menggunakan metode inklusi pada dinamika discrete-time chaotic system. Algoritma yang diusulkan pada penelitian tersebut memiliki tingkat keamanan yang tinggi terhadap serangan statistikal. Penerapan algoritma ini memberikan hasil yang baik saat recovery watermark. Penelitian selanjutnya dilakukan oleh Najafi (Najafi 2017) dan Ahmed (Ahmed, Riaz et al. 2018). Algoritma yang digunakan adalah DWT. Watermark disisipkan ke dalam 3 sub-band DWT level 3 yaitu LH3, HL3 dan HH3. Penelitian ini menghasilkan watermarked image dengan nilai PSNR yang tinggi dan hasil ekstraksi watermark-nya mempunyai nilai NCC yang tinggi pula. Sehingga algoritma DWT pada penelitian ini mampu menghasilkan digital watermarking dengan ketahanan dan tingkat imperceptibility yang baik

Beberapa penelitian tentang *digital watermarking* dengan menerapkan algoritma *Discrete Wavelet Transform* (DWT) dan CRT antara lain penelitian oleh Patra (Patra dkk., 2010) dan Tuncer (TUNCER, 2018). Pada kedua penelitiannya tersebut Patra dan tuncer melakukan perbandingan *running time* dan PSNR antara dua algoritma, yaitu CRT dan *Singular Value Decomposition* (SVD). Hasil dari penelitian tersebut menunjukkan algoritma CRT mampu menyisipkan *watermark* dengan *running time* lebih singkat dan menghasilkan PSNR yang lebih besar. Tetapi algoritma CRT ini memiliki ketahanan yang lebih rendah saat dilakukan serangan berupa *JPEG compression* dan *brightening*. Perbedaan diantaranya adalah Patra tidak dapat digunakan sebagai *authentication* sementara Tuncer dapat digunakan sebagai *image authentication*.

Mengacu pada beberapa penelitian sebelumnya, dengan memadukan watermarking pada *spatial domain* dan *transform domain* dapat meningkatkan kualitas *watermarked image* (*imperceptibiliy*) dan ketahanannya *(robustness)* terhadap beberapa serangan. Maka pada pada paper ini mengusulkan algoritma *Chinese Remainder Theorem* (CRT) untuk meningkatkan kualitas visual *image* dan *Integer Wavelet Transform* yang merupakan turunan dari *wavelet transform* untuk meningkatkan ketahanan serta untuk menghindari terjadinya *loss of information* sehingga dapat mempertahankan kualitas visual yang lebih baik

2. METODE PENELITIAN

Secara umum penerapan *digital watermarking* dengan IWT-CRT terdiri dari dua tahap yaitu proses penyisipan dan proses ekstraksi *watermark* dapat dilihat pada Gambar 1.



Gambar 1 Skema Watermarking IWT-CRT

Kedua tahap yaitu proses penyisipan dan proses ekstraksi *watermark* dapat dijelaskan sebagai berikut:

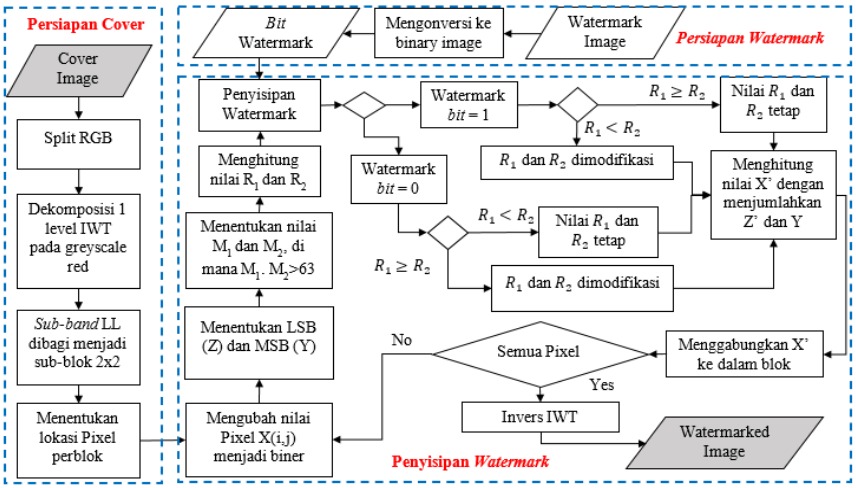
2.1 Proses Penyisipan Watermark

2.1.1. Persiapan Cover Image

Cover image yang digunakan berupa *image* dengan model warna RGB dengan ekstensi .bmp berukuran 512x512.

2.2.2 Persiapan Watermark

Watermark image yang digunakan berupa *binary image* berukuran 128x128. *Input image* yang berupa *greyscale image* dikonversi menjadi *binary image*. *Binary image* adalah image yang terdiri dari warna yaitu warna putih dan warna hitam.



Gambar 2 Proses Penyisipan Watermark

2.2.2 Penyisipan Watermark

Proses penyisipan *watermark* (lihat pada Gambar 2) dilakukan dengan menerapkan metode *Chinese Remainder Theorem* pada domain *Integer Wavelet Transform* dapat dijelaskan dengan menggunakan algortima 1

Algoritma 1

Input : *Cover image* dan *watermark image*
Output : *watermarked image*

1. *Cover image* dibagi menjadi 3 layer warna, yaitu *greyscale red, greyscale green dan greyscale blue*.
2. *Cover image* dengan channel *greyscale red* diproses menggunakan metode *Integer Wavelet Transform* untuk menghasilkan 4 sub-band, yaitu LL, LH, HL dan HH. Pada kasus ini menggunakan sub-band LL untuk disisipi *watermark*.
3. Membagi sub-band LL menjadi menjadi beberapa blok yang sesuai
4. Menetapkan lokasi penyisipan pada setiap blok yaitu pada indeks pertama.
5. Setelah lokasi ditentukan, nilai *pixel* (*X*) dengan rentang [0 255] diubah menjadi *biner* ukuran 8 bit.
6. Mengambil 6 angka *biner* terakhir yang disebut *Least Significamt Bits* (*LSB*) dari X. Kemudian dikonversi menjadi nilai desimal Z Rentang nilai LSB adalah 1-64.
7. Dua angka sisanya yaitu *Most Significant Bits (*MSB) digunakan untuk perhitungan selanjutnya dikonversi menjadi nilai desimal Y. Nilai MSB adalah 0, 64, 128 dan 192.
8. Menghitung nilai *residual* dari R_1 dan R_2 dengan menggunakan inverse *Chinese Remainder Theorem* pada persamaan (1) dan (2)

$$R_1 = Z \bmod m_1 \quad (1)$$

$$R_2 = Z \bmod m_2 \quad (2)$$

di mana: m_1 dan m_2 merupakan bilangan relatif prima $m_1 \, x \, m_2 > 64$, Z merupakan LSB yang diubah menjadi desimal

9. Berikutnya menanamkan *bit watermark* (w) ke dalam setiap *pixel*, dengan syarat:
   - Jika w = 1, maka $R_1 \geq R_2$
   - Jika w = 0, maka $R_1 < R_2$

   Jika nilai R_1 dan R_2 memenuhi syarat di atas maka nilai Z tetap sehingga Z'=Z, apabila tidak memenuhi syarat tersebut, maka nilai Z diubah dengan menambah 1 dan mengurangi 1 nilai Z sampai terpenuhi syarat di atas maka nilai Z' adalah Z terbaru yang sudah didapatkan
10. Selanjutnya mencari nilai Z baru dari nilai R_1 dan R_2 yang telah ditentukan dengan menggunakan persamaan (3)

$$Z^1 = \left(R_1 \frac{M}{m_1} K_1 + R_2 \frac{M}{m_2} K_2\right) mod\ M \quad (3)$$

Nilai K didapatkan dari persamaan (4) dan (5)

$$K_1 \frac{M}{m_1} = 1 (mod\ M_1) \quad \text{.....(4)}$$

$$K_2 \frac{M}{m_2} = 1 (mod\ M_2) \quad (5)$$

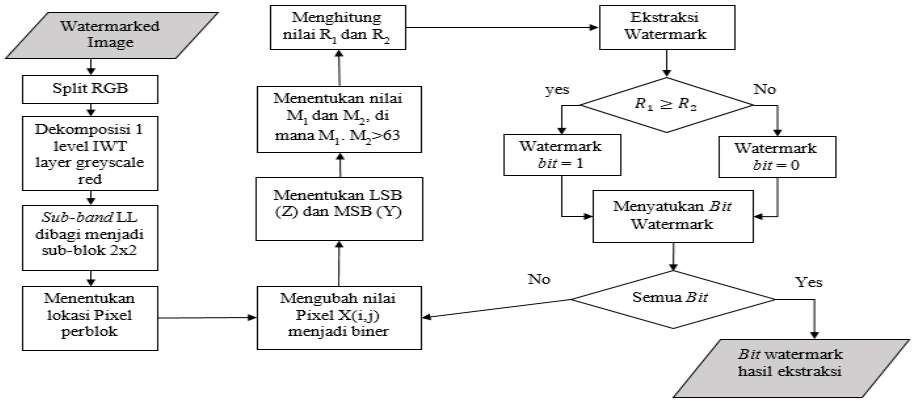
11. Menghitung nilai X baru setelah disisipi dengan dengan persamaan (6)

$$X' = Y + Z' \quad (6)$$

di mana: *X'* adalah *pixel* indeks pertama yang baru, *Y'*adalah MSB yang sudah didesimalkan,*Z'* adalah LSB baru yang didapatkan setelah langkah 7
12. Langkah 3 sampai 8 diulangi sampai setiap blok tersisipi *watermark*.
13. Rekonstruksi *image* dengan menerapkan *invers Integer Wavelete Transform*
14. Rekontruksi citra dengan menyatukan layer greyscale red yang baru dengan layer greyscale green dan blue sehingga menghasilkan watermarked image dengan model warna RGB.

2.2 Proses Ektraksi Wateramark

Setelah proses penyisipan langkah selanjutnya yaitu proses ekstraksi. Proses ini untuk memulihkan *bit watermark* yang telah disisipkan ke dalam *cover image*. Proses ekstraksi *watermark* (lihat pada Gambar 3). Proses ektraksi dapat dijelaskan dengan menggunakan algoritma 2.



Gambar 3. Proses Ekstraksi Watermark

Algoritma 2

Input : *Watermarked image*

Output : *Bit watermark*

1. *Watermarked image* dibagi menjadi 3 layer warna, yaitu *greyscale red, greyscale green* dan *greyscale blue*.
2. *Watermarked image* dengan layer *greyscale red* diproses menggunakan metode *Integer Wavelet Transform* untuk menghasilkan 4 sub-band, yaitu LL, LH, HL dan HH.
3. Sub-band LL dibagi menjadi blok-blok
4. Menentukan lokasi nilai *pixel* (X) pada blok sesuai dengan lokasi pada saat penyisipan. Kemudian mengubah nilai X menjadi bilangan biner 8 bit.
5. Menentukan 6 *Least Significamt Bits (LSB)*, yaitu 6 angka terakhir dari X. Dua angka sisanya adalah *Most Significant Bits (MSB)*
6. Menghitung nilai residual dari R_1 dan R_2 dengan menggunakan persamaan (1) dan (2)
   di mana: m_1 dan m merupakan bilangan relatif prima
   $m_1 \, x \, m_2 > 63$
   Z merupakan LSB yang diubah menjadi desimal
7. Menentukan *bit watermark (w)* yang akan diekstraksi dengan syarat seperti pada persamaan (8)
   Jika
   $$R_1 \begin{cases} \geq R_2 & , w = 1 \\ < R_2 & , w = 0 \end{cases} \quad (8)$$
8. Ulangi langkah di 3 sampai 6 hingga semua *bit watermark* terekstraksi.

3. HASIL DAN PEMBAHASAN

Pengujian yang dilakukan dalam pembahasan ini terdapat dua macam, yaitu pengujian dengan ukuran watermark yang berbeda dan pengujian dengan melakukan serangan kepada watermarked image. Pada paper ini data yang digunakan sebagai cover image adalah Lena.bmp, Papers.bmp dan Baboon.bmp (ukuran tiga cover image adalah sama yaitu 512x512 dapat dilihat pada Gambar 4, Gambar 5 dan Gambar 6).

Sedangkan yang digunakan untuk *watermark* adalah *8.jpg* berukuran 128x128 dapat dilihat pada Gambar 7. Sehingga dalam pengujian ini bertujuan untuk mendapatkan nilai PSNR dan NCC sebagai acuan untuk mengetahui kualitas hasil *watermarking* dan hasil ekstraksi setelah diberi beberapa serangan

Gambar 4. Lena.bmg

Gambar 5. Papers.bmg

Gambar 6. Baboon.bmg

Gambar 7. 8.jpg

3.1. Pengujian penyisipan tanpa serangan

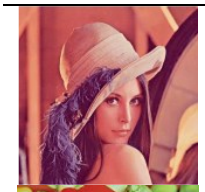
Analisis hasil pengujian dilakukan dengan mengukur nilai PSNR dan NCC untuk penyisipan dan ektraksi tanpa serangan didapatkan seperti dapat dilihat dalam Tabel 1. Tabel 1 menunjukkan hasil penyisipan dan ekstraksi dari tiga *cover image* berbeda. Tabel 1 juga menunjukkan nilai PSNR yang cukup tinggi untuk masing-masing *watermarked,* dengan hasil PSNR yang cukup tinggi menunjukkan bahwa algoritma yang diusulkan mampu menghasilkan *watermarked image* dengan kualitas visual yang baik. Proses ekstraksi *watermark* memiliki hasil yang sangat baik, karena dari ketiga hasil ekstraksi memiliki rata-rata nilai NCC mendekati nilai 1

3.2. Pengujian dengan serangan serangan

Dalam pembahasan ini dilakukan pengujian dengan memberikan serangan berupa *gaussian noise*, *salt & pepper*, *JPEG2000 compression, rotate dan contrast*. Analisis hasil pengujian dilakukan dengan mengukur nilai NCC, dengan membandingkan

watermark image dengan *watermark image* hasil ekstrak.

Tabel 1. Hasil Penyisipan Dan Ektraksi Watermark

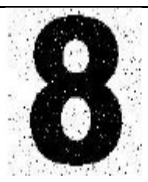
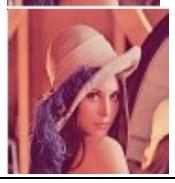
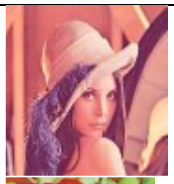
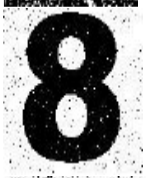
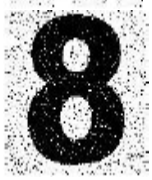
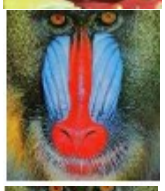
Watermarked image	*Watermark* Hasil Ektraksi	Nilai-Nilai PSNR, NCC
		PSNR = 55,343 NCC= 0,999661
		PSNR = 55,8669 NCC= 0,999661
		PSNR = 55,7143 NCC= 0,999661

3.2.1 Serangan *Gaussian Noise*

Gaussian noise adalah macam *noise* yang mengikuti *standard* distribusi normal dengan rata-rata 0 dan *standard* deviasi . *Gaussian noise* dibangkitkan dengan cara mengenerate bilangan acak dengan nilai interval 0 dan 1. Selanjutnya, titik-titik yang terkena *noise,* nilai fungsi *image* ditambahkan dengan *noise* yang ada. Pengaruh dari *Gaussian Noise* pada *image* adalah timbulnya titik-titik berwarna yang jumlahnya sama dengan persentase *noise*

Hasil pengujian dengan *gaussian noise* ditunjukkan pada Tabel 2 sebagai berikut :

Tabel 2 Hasil Pengujian Serangan Gaussian Noise

Nilai Variasi $V=10^{-6}$	Hasil Pemberian *Gaussian*	*Watermark* Hasil ektraksi	NCC
$M=10^{-6}$			0,95748
$M=10^{-3}$			0,86921
$M=10^{-1}$			-0,1952
$M=10^{-6}$			0,96215
$M=10^{-3}$			0,86769
$M=10^{-1}$			-0,2740
$M=10^{-6}$			0,9617
$M=10^{-3}$			0,8681
$M=10^{-1}$			-0,2098

Tabel 2 menunjukkan nilai NCC yang dihasilkan dari ketiga nilai variasi tersebut berbeda-beda sesuai nilai variasi yang digunakan. Semakin besar nilai variasinya maka hasil ekstraksi semakin tidak dapat dikenali dan nilai NCC-nya akan lebih kecil

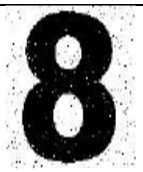
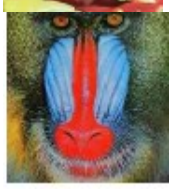
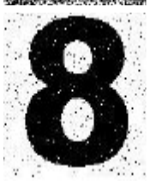
3.2. 2. Serangan S*alt & Pepper*

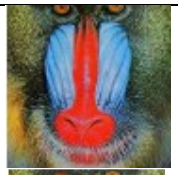
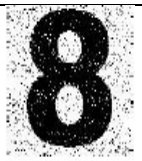
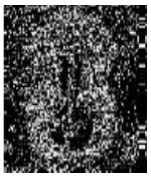
Noise impuls positif dan negatif biasa dinamakan *Salt & Pepper.* Noise ini muncul dikarenakan terjadinya *error bit* dalam pengiriman data, *pixel-pixel* yang tidak berfungsi dan kerusakan pada lokasi memori. *Noise* ini berbentuk bintik-bintik putih atau hitam dalam *image*. Banyak sedikitnya noise pada image ditentukan oleh nilai *density(df)* pada interval 0 sampai 1.

Pengujian *salt & pepper* menggunakan tiga *watermarked image* dengan menggunakan tiga nilai *density* untuk masing-masing *watermarked image*, yaitu 0.01, 0.05 dan 0.3. Hasil pengujian dengan *gaussian noise* ditunjukkan pada Tabel 3 berikut:

Tabel 3 menunjukkan nilai NCC yang dihasilkan dari ketiga nilai *density* tersebut menurun seiring bertambah besarnya nilai *density* yang digunakan. Semakin besar nilai *density*-nya maka hasil ekstraksinya semakin tidak dapat dikenali dan nilai NCC-nya akan lebih kecil.

Tabel 3 Hasil Pengujian Serangan Salt & paper

Nilai *Density*	Hasil Pemberian *Gaussian*	*Watermark* Hasil Extraksi	NCC
0,01			0,96388
0,05			0,80259
0,3			0,23653
0,01			0,95588
0,05			0,81397
0,3			0,24480
0,01			0,95829

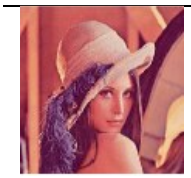
Nilai *Density*	Hasil Pemberian *Gaussian*	*Watermark* Hasil Extraksi	NCC
0,05			0,80607
0,3			0,24958

3.2.3 Serangan *JPEG2000*

JPEG 2000 adalah kompresi *image digital* yang berdasarkan *Discrete Wavelet Transform* (DWT) dan termasuk metode kompresi yang simetris, yaitu proses kompresi dan dekompresi menggunakan algoritma yang sama namun mempunyai arah yang berlawanan.

JPEG2000 dikembangkan oleh *Joint Photographic Experts Group* pada tahun 1997. Pengujian kompresi *JPEG2000* menggunakan tiga watermarked image. Hasil pengujian kompresi *JPEG2000* ditampilkan pada Tabel 4.

Tabel 4 Hasil Pengujian Kompresi JPEG2000

Image JPEG2000	*Watermark* hasil Ektraksi	NCC
		0,706493
		0,704634
		0,728992

Dari Tabel 4 didapatkan nilai rata-rata NCC yang dihasilkan dari ketiga *watermarked image* sebesar 0,71337. Karena kompresi *image JPEG2000* berbasis *Integer Wavelet Transform* (IWT) sehingga *watermark* dapat diekstraksi dengan kualitas yang cukup baik

3.2.4 Serangan *Contrast*

Contrast merupakan tingkat penyebaran *pixel-pixel* ke dalam *intensitas* warna. Untuk tingkat ketinggian contrast ditentukan oleh nilai *intensitas*

pada *image*. Dengan nilai pada *intensitas* rendah minimal 0 dan nilai pada *intensitas* tinggi maksimal 1. Pada pengujian *contrast* menggunakan tiga *watermarked image* dengan 2 nilai intensitas rendah 0,01 dan 0,04 serta nilai intensitas rendah 1. Hasil pengujian c*ontrast* dapat dilihat pada Tabel 5.

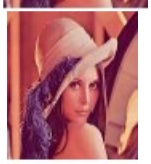
Dari hasil pengujian sesuai Tabel 5 menunjukkan bahwa ketiga *watermarked image* yang diberikan *contrast* dengan nilai intensitas rendah 0,01 dan 0,04 hasil ekstraksi *watermark* dari ketiga *watermarked image* memiliki nilai NCC yang sangat rendah yaitu di bawah 0,5, yang berarti kualitas *watermark* yang terekstraksi sangat buruk.

Pada pengujian rotasi menggunakan dua *watermarked image* dan dengan sudut rotasi 1° dan 90°.Hasil pengujian *rotate d*apat dilihat pada Tabel 6.

Dari Tabel 6 dapat dilihat bahwa kedua *watermarked image* yang telah diberikan serangan berupa rotasi dengan sudut rotasi 1° dan 90° menghasilkan ekstraksi *watermark* yang buruk dengan hanya memiliki nilai NCC dibawah 0,1.

Selanjutnya mengamati dari hasil pengujian yang telah dilakukan maka dapat dilakukan analisa perbandingan dari beberapa penelitian sebelumnya, dapat dilihat dalam Tabel 7. Hasil *experiment* yang telah dilakukan bahwa nilai PSNR dari berbagai serangan yang diberikan mendapatkan nilai mendekati 1.

Tabel 5 . Hasil Pengujian *Contrast*

Intent itas	*Image Contrast*	*Watermark* hasil Ektraksi	NCC
0,01			0,45782
0,04			-0,10711
0,01			0,28248
0,04			0,18219

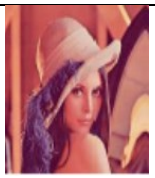
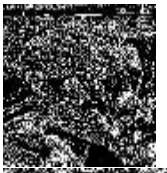
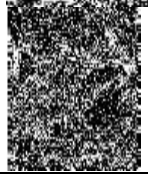
Intent itas	*Image Contrast*	*Watermark* hasil Ektraksi	NCC
0,01			0,21962
0,04			-0,12301

Sementara untuk nilai NCC dari metoda yang dihasilkan bervariasi, ini berarti bahwa metoda yang diusulkan tahan terhadap serang *Gaussian Noise, Salt & paper* dan *JPEG2000* namun tidak tahan terhadap serangan *contrast* dan *Rotate*. Metoda yang diusulkan lebih tahan serangan *Gaussion Noise* dan *salt &paper* dari pada yang diusulkan oleh (Hannoun, Hamiche et al. 2018).

3.2.5 Serangan *Rotate*

Namun metoda yang diusulkan tidak lebih tahan dari serangan *contrast* dan *rotate* dibandingkan dengan metoda yang sudah ada Najafi (Najafi 2017) dan Ahmed (Ahmed, Riaz et al. 2018).

Tabel 6 Hasil pengujian Rotate

Sudut	*Image Rotate*	Watermark hasil Ektraksi	NCC
1°			0,034138
90^0			-0,024116
1^0			0,063104
90^0			0,028417

Tabel 7 Hasil Perbandingan Dengan Metoda yang telah ada

Jenis Serangan	Patra dkk	Hannoun et al	Najafi E	Ahmed et al	Metoda yang diusulkan
	2010	2018	2017	2018	2020
Gaussian Noise	√	x	√	√	√
Salt papers	√	x	√	√	√
JPEG2000	x	x	√	x	√
Contrast	x	x	x	√	x
Rotate	x	√	√	x	x

4. KESIMPULAN

Dalam paper ini telah diterapkan *Integer Wavelet Transform* dan *Chinese Remainder Theorem* pada sistem *digital watermarking*. Proses penyisipan berhasil dilakukan dengan PSNR yang cukup tinggi. Nilai PSNR yang tinggi menunjukkan bahwa algoritma ini mampu menghasilkan *watermarked image* dengan kualitas visual yang bagus. Hasil ekstraksi *watermarked image* tanpa serangan menunjukkan bahwa watermark dapat diekstraksi dengan baik dan memiliki nilai NCC yang tinggi.

Hasil pengujian dengan beberapa serangan menujukan algoritma yang diusulkan mampu menghasilkan *watermarked image* yang tahan terhadap serangan *kompresi JPEG2000, salt & pepper*, *dan gaussian noise* tetapi tidak tahan terhadap serangan *rotate* dan *contrast.*

DAFTAR PUSTAKA

ADI, P. W., RAHMANTI, F. Z. & WINARNO, E. 2018 Robust watermarking through dual band IWT and Chinese remainder theorem. Bulletin of Electrical Engineering and Informatics 7(4):561-569. DOI: 10.11591/eei.v7i4.690

AHMED, R., RIAZ, M. M. & GHAFOOR, A. 2018 Attack resistant watermarking technique based on fast curvelet transform and Robust Principal Component Analysis. Multimedia Tools and Applications 77(8):9443-9453. DOI 10.1007/s11042-017-5128-5

HANNOUN, K., HAMICHE, H., Lahdir, M., Laghrouche, M. & Kassim, S. 2018 A novel DWT domain watermarking scheme based on a discrete-time chaotic system. IFAC-PapersOnLine 51(33):50-55. DOI: https://doi.org/10.1016/j.ifacol.2018.12.089

NAJAFI, E. 2017 A robust embedding and blind extraction of image watermarking based on discrete wavelet transform. Mathematical Sciences 11(4):307-318. DOI: https://doi.org/10.1007/s40096-017-0233-1

NUGRAHA, D. A., RAHMADWATI, R. & MUSLIM, M. A. 2017 Skema Digital Watermarking Citra dengan Metode TLDCT dan Chinese Remainder Theorem. Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI) 6(2):133-140. DOI: http://dx.doi.org/10.22146/jnteti.v6i2.307

PATRA, J. C., KARTHIK, A., & BORNAND, C. 2010. A novel CRT-based watermarking technique for authentication of multimedia contents. Digital Signal Processing, 20(2), 442–453. DOI: https://doi.org/10.1016/j.dsp.2009.07.004

POONAM DAN S. M. ARORA, 2018 "A DWT-SVD based Robust Digital Watermarking for Digital Images," Procedia Comput. Sci., vol. 132, hlm. 1441–1448, , DOI: 10.1016/j.procs.2018.05.076

SHIH, F. Y. 2017 Digital watermarking and steganography: fundamentals and techniques. CRC press. DOIhttps://doi.org/10.1201/9781315121109

SUDIBYO, U., ERANISA, F., RACHMAWANTO, E. H. & Sari, C. A. 2017 A secure image watermarking using Chinese remainder theorem based on haar wavelet transform. In 2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE).) IEEE, pp. 208-212 DOI: 10.1109/ICITACEE.2017.8257704.

SUNDARARAJAN, D. 2017 Digital image processing: a signal processing and algorithmic approach. Springer. DOI:10.1007/978-981-10-6113-4

TUNCER, T. 2018 Analysis of CRT-based Watermarking Technique for Authentication of Multimedia Content. International Journal of Computer Network and Information Security 10(6):60-67. DOI: 10.5815/ijcnis.2018.06.06

WAGDARIKAR, A. M., SENAPATI, R. K. & EKKELI, S. 2019 A secure video watermarking approach using CRT theorem in DCT domain. In Microelectronics, Electromagnetics and Telecommunications.) Springer, pp. 597-606. DOI:https://doi.org/10.1007/978-981-13-1906-8_61

.