Perbaikan Deteksi *Watermark* Dengan Knn Pada Penyembunyian Data Berbasiskan *Histogram-Based Reversible Data Hiding*

1st Rina Media Sari
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
rinamediyas@student.telkomuniversity.ac.id

2nd Gelar Budiman
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
gelarbudiman@telkomuniversity.ac.id

3rd Ledya Novamizanti
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
ledyaldn@telkomuniversity.ac.id

***Abstrak* — Penggunaan internet pada era ini sangat mempermudah segala hal, salah satunya dalam hal mengakses data. Dampak negatif dari hal tersebut adalah penyalahgunaan hak cipta. Penelitian Tugas Akhir ini bertujuan merancang skema *reversible watermarking* pada suatu citra. Pada proses penyisipan menggunakan metode *Integer Wavelet Transform* (IWT). dan *Histogram Shifting*. Pada proses ekstraksi menggunakan metode *Integer Wavelet Transform*, *Histogram Shifting* dan *K-nearest Neighbor* (KNN) untuk meningkatkan proses deteksi *watermark* sehingga menghasilkan nilai BER yang kecil. Penelitian ini menggunakan 5 *host* yang berbeda. Pengujian terhadap berbagai serangan dilakukan pada setiap *host*. Hasil terbaik untuk berbagai serangan yang di uji yaitu serangan *Speckle* dengan variansi 0.00001 yang memiliki nilai PNSR *reversible* yaitu sebesar 52.7029, nilai BER tanpa KNN yaitu sebesar ≥ 41%, nilai BER dengan KNN yaitu sebesar ≥ 24%, nilai Kapasitas yaitu sebesar 0.0028 dan waktu komputasi yaitu 1.3425 detik.**

***Kata kunci*— image watermarking, Histogram Shifting, reseversible data hiding, K- Nearest Neighbor**

I. PENDAHULUAN

Dunia teknologi dan informasi berkembang dengan pesatnya. Penyebaran media digital yang semakin mudah menyebabkan maraknya tindakan seperti duplikasi dan penyebaran data secara ilegal, serta penyalahgunaan Hak akan Kekayaan Intelektual (HAKI). Digital watermarking yaitu teknik deteksi dan penyembunyian data atau informasi pada suatu berkas citra dan mampu tidak terlihat serta tahan terhadap proses-proses digitalisasi [1]. Digital image watermarking dengan teknik reversible data hiding merupakan salah satu teknik untuk menyembunyikan watermark pada suatu berkas citra dan mengekstrak kembali watermark untuk membuktikan hak cipta berkas citra tersebut. Penelitian reversible watermarking dilakukan oleh Alfian Ghifari [2] yang memilih border point dan localization guna meningkatkan kapasitas penyisipan. Alfian Ghifari [2] menghasilkan nilai PSNR sebesar >56 dB, serta tidak memiliki ketahanan yang baik terhadap noise Gaussian, kompresi dibawah 99%, dan rescaling.

Penelitian [3] menggunakan metode block-wise histogram shifting. Penelitian tersebut melakukan percobaan dengan empat host citra grayscale. Hasil percobaan mendapatkan nilai PSNR yang tinggi yaitu 50.93 dB, 51.07 dB, 50.92 dB, dan 52.20 dB. Namun skema belum diuji ketahanannya terhadap serangan. P. rahmani dan G. Dastghaibyfard [4] melakukan penelitian reversible data hiding dengan pixel-based pixel value ordering (PPVO) sebagai predictor. Penelitian dilakukan dengan menggunakan sembilan host citra grayscale dan menghasilkan PSNR sebesar 35.54 dB hingga 48.91 dB. Namun kualitas citra belum diuji ketahannya terhadap serangan. Penelitian [5] menggunakan metode reversible data hiding dengan kompresi JPEG. Percobaan tersebut menghasilkan distorsi yang besar dari pengekstraksian data. Untuk penelitian selanjutnya, diharapkan agar mengembangkan metode yang efisien untuk penyematan dan pengekstraksian data.

Metode yang digunakan pada jurnal ini adalah K-Nearest Neighbor dengan penyisipan oleh IWT dan Histogram Shifting. Tujuan dari penggunaan metode tersebut adalah untuk meningkatkan deteksi watermark dan menciptakan sistem watermarking yang tahan terhadap serangan, stabil, dan memiliki kapasitas tinggi. Secara singkat host image akan melalui subband CD pada IWT, kemudian disisipkan watermark berupa teks pada proses Histogram Shifting lalu pada proses ekstraksi detected watermark akan melalui proses KNN dan dilakukan perhitungan BER dengan KNN.

Pada jurnal ini terdapat beberapa bagian. Bagian 2 akan menjelaskandasar teori yang dipakai dalam penelitian ini, dimana teori dari semua metode akan dijelaskan. Bagian 3 akan mejelaskan model dari sistem watermarking yang dirancang dan menjelaskan proses penyisipan, proses ekstraksi serta serangan yang diberikan bagian 4 akan menjelaskan hasil dan analisis berdasarkan dari uotput sistem yang dirancang dan bagian 5 adalah kesimpulan dari jurnal ini.

II. KAJIAN TEORI

Pada bagian ini gambaran dasar untuk metode yang digunakan dalam sistem watermarking ini ditampilkan. Metode-metode ini terdiri dari IWT dan *Histogram Shifting* untuk metode penyisipan dan KNN untuk memperbaiki deteksi watermark.

A. *Integer Wavelet Transform* (IWT)

Integer Wavelet Transform merupakan teknik transformasi linear untuk memfilter output dan dapat digunakan dalam kompresi data *lossless* [6]. *Integer Wavelet Transform* (IWT) adalah suatu metode transformasi *wavelet* yang memiliki nilai hasil transformasi yang berupa bilangan bulat. Ini berbeda dengan metode transformasi wavelet biasa (seperti Continuous Wavelet Transform), yang memiliki nilai hasil transformasi yang berupa bilangan real. Pada penyembunyian data yang bersifat *reversible* tranformasi *wavelet* yang konvosional tidak terlalu berguna karena tidak sepenuhnya data dapat kembali seperti semula. Gambar sampul asli tidak dapat dipulihkan jika terdapat *floating point* yang menyebabkan adanya informasi yang hilang [7]. Untuk mengatasi masalah ini pada skema yang diusulkan menggunakan transformasi *wavelet integer* berdasarkan skema *lifting*. *Lifting Wavelet Transform* adalah suatu metode transformasi wavelet yang menggunakan pendekatan *lifting scheme*. *Lifting scheme* adalah suatu pendekatan yang memecah transformasi *wavelet* menjadi beberapa tahap yang lebih sederhana, sehingga mempermudah proses pemrosesan dan mempercepat kecepatan proses.

Transformasi LWT digunakan untuk membagi sinyal menjadi dua bagian yaitu frekuensi tinggi (*high*) dan frekuensi rendah (*low*). Operasi ini terdiri dari tiga langkah [8] :

1. *Split/Decomposition*

Pada tahap *Split/Decomposition* atau pemisahan sinyal pada transformasi *Lifting Wavelet*, sinyal dibagi menjadi dua bagian yaitu bagian frekuensi rendah (*low*) dan frekuensi tinggi (*high*). Proses pemisahan ini melibatkan perhitungan matematis pada setiap pasangan *sample* sinyal. Rumus yang digunakan untuk pemisahan sinyal adalah sebagai berikut:

$$low[n] = \frac{(x(2n)) + (x(2n+1))}{2} \qquad (2.11)$$

$$high[n] = \frac{(x(2n)) - (x(2n+1))}{2} \qquad (2.2)$$

Dimana: *x[n]* adalah sinyal asli, *low[n]* adalah bagian frekuensi rendah dari sinyal, *high[n]* adalah bagian frekuensi tinggi dari sinyal, *2n dan 2n + 1* adalah pasangan *sample* dari sinyal

2. *Prediction* (HPF)

Prediction (HPF) merupakan proses untuk memprediksi nilai *sample* berikutnya dari sinyal dalam frekuensi rendah (*low*) berdasarkan *sample* sebelumnya dalam sinyal yang sama. Rumus yang digunakan untuk melakukan prediction adalah sebagai berikut:

$$pred[n] = low[n-1] \qquad (2.3)$$

Dimana: *pred[n]* adalah nilai prediksi dari *sample* berikutnya., *low[n - 1]* adalah nilai *sample* sebelumnya dalam frekuensi rendah.

3. *Update* (LPF)

Update (LPF) adalah tahap selanjutnya dalam proses *lifting wavelet transform* setelah tahap *Prediction* (HPF). Tahap ini bertujuan untuk menentukan nilai dalam frekuensi tinggi (*high*) berdasarkan nilai *sample* asli dan hasil prediksi dalam tahap sebelumnya. Rumus yang digunakan untuk melakukan *update* adalah sebagai berikut:

$$high[n] = input[n] - pred[n] \qquad (2.4)$$

Dimana: *high[n]* adalah nilai dalam frekuensi tinggi untuk sample ke-n, *input[n]* adalah nilai sample asli, *pred[n]* adalah nilai prediksi dari tahap *Prediction* (HPF).

B. *Histogram Shifting*

Histogram Shifting menyisipkan pesan rahasia menggunakan tingkat kecerahan (*grey level*) dengan frekuensi piksel terendah pada histogram citra. Histogram citra sendiri merupakan plot frekuensi atau jumlah piksel terhadap tingkat kecerahan citra. Tingkat kecerahan citra pada histogram ditunjukkan oleh sumbu horizontal yang berdasarkan nilai 0 sampai 255. Frekuensi atau jumlah piksel untuk tingkat kecerahan tertentu ditunjukkan oleh sumbu vertikal [9]. Pada histogram gambar tingkat frekuensi piksel tertinggi atau titik puncak disebut *peak point*, sedangkan frekuensi terendah atau titik nol disebut *zero point*. Nilai *peak point* dan *zero point* digunakan untuk menggeser tingkat kecerahan ke arah nilai *zero point*. Pergeseran dilakukan guna mencari ruang untuk menyisipkan *watermark* [9]. Setelah *watermark* tersemat, nilai piksel diubah sesuai dengan bit *watermark* menggunakan rumus [10] :

$$P_{c-2} = P_{c-2} + i \qquad (2.5)$$

$$P_{c+2} = P_{c+2} - i \qquad (2.6)$$

Dengan *P* adalah nilai piksel yang disisipkan, *P* didefinisikan sebagai nilai piksel asli, dan *i* adalah nilai bit *watermark* (0 atau 1). Jika bit *watermark* yang dihasilkan bernilai "1" maka terjadi perubahan pada nilai piksel, tetapi jika bit *watermark* yang dihasilkan bernilai "0" maka tidak ada perubahan pada nilai piksel [23].

C. *K-Nearest Neighbor* (KNN)

KNN merupakan salah satu metode dalam pengklasifikasian data. *K-Nearest Neighbor* merupakan salah satu metode yang menggunakan algoritma *supervised* dimana data yang akan diuji diklasifikasikan berdasarkan data pembelajaran yang terdekat dengan objek tersebut [11]. Prinsip kerja pada *KNN* adalah mencari jarak terdekat antara data yang akan di evaluasi dengan *k* tetangga (*neighbor*) [12]. *K-Nearest Neighbor* (KNN) dapat digunakan untuk memperbaiki *watermark* dengan menggunakan metode interpolasi. Dalam hal ini, *watermark* yang terdistorsi akan dibandingkan dengan beberapa *pixel* tetangga terdekatnya, dan nilai *pixel* tersebut akan digunakan untuk menentukan nilai *pixel* yang hilang atau rusak pada *watermark*. Dengan menggunakan algoritma KNN, nilai *pixel* baru akan

ditentukan berdasarkan jumlah tetangga terdekat (k) dan metode pembagian bobot tertentu. Ini dapat membantu mengurangi *noise* dan memperbaiki kualitas *watermark* yang rusak. Untuk menghitung jarak terdekat dapat menggunakan *Euclidean Distance*. *Euclidean Distance* atau jarak *Euclidean* merupakan proses perhitungan untuk mencari jarak antara dua titik pada ruang *Euclidean* (yang meliputi dua dimensi, tiga dimensi ataupun lebih). Untuk menghitung *Euclidean Distance* dapat menggunakan rumus :

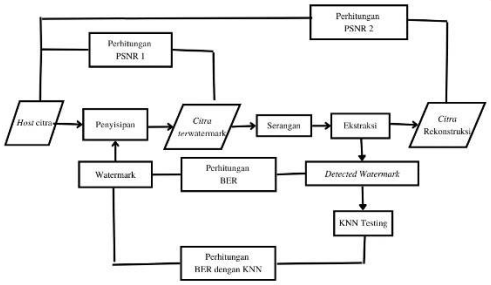
$$dist(p,q) = \sum(pi - qi)^2 \qquad (2.7)$$

Dimana *dist* merupakan jarak p dan q, p adalah data objek pertama, q adalah data objek kedua, i merupakan urutan nilai dari setiap data.

III. METODE

A. Model *Image Watermarking*

Pada jurnal ini, skema dari sistem *image watermaking* yang dirancang secara keseluruhan dapat dilihat pada gambar berikut :

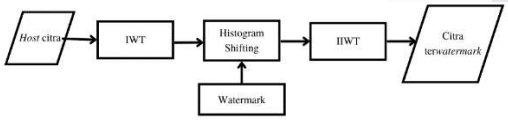


GAMBAR 3.1
General Image Watermarking.

Pada gambar 3.1 adalah gambaran dari sistem secara keseluruhan, proses pertama yang dilakukan adlaah proses penyisipan kemudian keluaran dari proses akan diberikan serangan. Proses ekstraksi dilakukan setelah citra mendapat serangan. Inti dari proses ini ada pada kedua proses yakni proses penyisipan dan proses ekstraksi.

B. Proses Penyisipan

Proses penyisipan dilakukan dengan memilih 1 dari 5 host citra yang telah disiapkan sebelumnya. Gambaran Proses Penyisipan pada tugas akhir ini adalah sebagai berikut.



GAMBAR 3. 1
Proses Penyisipan.

1. Langkah 1

Membaca *file* berupa citra *host* jenit *bitmap* (BMP) dan *watermark* berupa teks.

2. Langkah 2

Melakukan inialisasi filter IWT dengan menetapkan tipe *wavelet* yang akan digunakan.

3. Langkah 3

Proses IWT pada 4 *subband* yaitu CA,CH,CV dan CD pada citra *host*. S*ubband* yang digunakan adalah CD

4. Langkah 4

Mencari estimasi jumlah piksel w*atermark* yang dapat disispkan menggunakan citra *host*.

5. Langkah 5

Watermark diberi penambahan *zero padding*.

6. Langkah 6

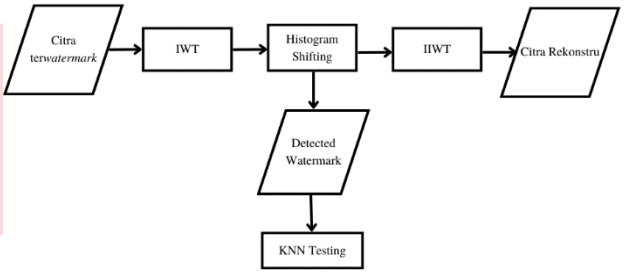
Hasil estimasi dan citra memasuki proses *Histogram Shifting*.

7. Langkah 7

Dilakukan *inverse* IWT untuk mendapatkan citra ter*watermark*.

C. Proses Ekstraksi

Pada proses ekstraksi, citra terwatermark akan dianalisis kualitasnya terhadap host citra dan watermark yang disisipkan. Keseluruhan pada proses ekstraksi dapat dilihat pada gambar berikut.



GAMBAR 3. 3
Proses Ekstraksi.

1. Langkah 1

Citra ter*watermark* melakukan proses IWT seperti pada saat proses penyisipan.

2. Langkah 2

Melakukan proses *Histogram Shifting* untuk mengekstraksi *watermark*.

3. Langkah 3

Melakukan proses *inverse* IWT untuk mendapatkan citra *host* rekonstruksi seperti pada proses penyisipan.

4. Langkah 4

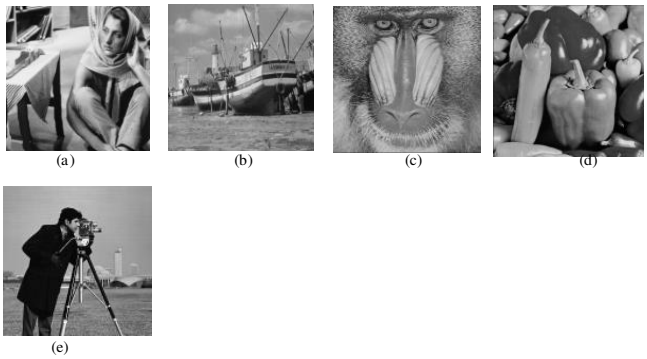
Selanjutnya memasuki proses *K-Nearest Neighbor* (KNN) untuk mendapatkan nilai BER yang lebih baik.

IV. HASIL DAN PEMBAHASAN

Pengujian dilakukan terhadap 5 file citra host yaitu: Barbara, Boat, Baboon, Peppers dan Cameraman dengan watermark berupa teks.

A. Parameter Terbaik Tanpa Serangan

Pengujian dilakukan dengan *level wavelet* 1 dan tipe *wavelet lazy* pada 5 host yang berbeda. Parameter terbaik yang didapatkan adalah sebagai berikut.



(a) (b) (c) (d) (e)

GAMBAR 4.1
Citra Host (a) Barbara, (b) Boat, (c) Baboon, (d) Peppers dan (e) Cameraman

TABEL 4.1
Performa Sistem Menggunakan Parameter Terbaik

Host	PSNR1	BER dengan KNN	BER	PSNR2	Kapasitas
Barbara	66.9814 dB	0%	0%	99.1339 dB	0.003567
Boat	57.9387 dB	0%	0%	99.3059 dB	0.005493
Baboon	55.5607 dB	0%	0%	81.8295 dB	0.002758
Peppers	54.8909 dB	0%	0%	86.0673 dB	0.002827
Cameraman	63.0098 dB	0%	0%	93.2853 dB	0.006229

B. Parameter dengan Serangan

Hasil parameter dengan serangan pada host Barbara dapat dilihat pada tabel berikut.

Serangan	**Variansi**	**BER tanpa KNN**	**BER dengan KNN**	**Watermark Ter-Ekstraksi**
Speckle	0.1	≥ 50%	≥ 34%	
	0.01	≥ 50%	≥ 26%	
	0.0001	0%	0%	
Kompresi JPEG 90%	*uint*8 *bithdepth* 8	≥50%	≥33%	
	*uint*8 *bithdepth* 12	≥49%	≥29%	
	*uint*16 *bithdepth* 16	0%	0%	
LPF		≥ 49%	≥ 37%	
Sharpening		≥52%	KNN ≥33%	

V. KESIMPULAN

A. Kesimpulan

Tugas Akhir ini mengusulkan sebuah skema *reversible watermarking* menggunakan metode *K-Nearest Neighbor*, *Histogram Shifting* dan *Integer Wavelet Transform*. Metode *K-Nearest Neighbor* digunakan pada proses ekstraksi untuk meningkatkan proses deteksi sehingga menghasilkan nilai BER yang kecil. Metode *Histogram Shifting* dan *Integer Wavelet Transform* digunakan pada proses penyisipan untuk menghasilkan *impercepbility* dan *robustness* yang baik.setelah dilakukan pengujian parameter dan serangan dilakukan analisis untuk sistem *watermarking* citra *reversible* yang dirancang. Dapat disimpulkan sistem ini memiliki nilai PSNR 1 maksimal antara citra *host* dan citra *host* ter-*watermark* sebesar 66.9815 dB dan nilai PSNR 2 maksimal antara citra *host* dan citra *host* rekontrsuksi sebesar 99.3059 dB. Nilai maksimal BER tanpa KNN dan BER dengan KNN pada saat sistem tidak diberi serangan masing-masing sebesar 0% dan 0% yang berarti sistem menghasilkan citra rekonstruksi yang baik. Nilai maksimal *payload* atau kapasitas sebesar 0.136272. Saat dilakukan pengujian dengan serangan pada sistem yang dirancang hanya mampu menahan serangan penambahan *noise* dengan variansi yang kecil serta tidak tahan terhadap serangan *Filtering* (LPF), *Geometric* (*Flipping*, *Resize*) dan serangan pemrosesan sinyal (*Histogram Equalization, Sharpening*).

REFERENSI

[1] N. Bhargava, M. M. Sharma, A. S. Garhwal, and M. Mathuria, "Digital image authentication system based on digital watermarking," *2012 Int. Conf. Radar, Commun. Comput. ICRCC 2012*, pp. 185–189, 2012, doi: 10.1109/ICRCC.2012.6450573.

[2] A. Ghifari, "Analisis dan Implementasi Image Watermarking Menggunakan Histogram-Based Reversible Data Hiding Dengan Border Point dan Localization" Analysis And Implementation of Image Watermarking Using Histogram-Based Reversible Data Hiding With Border Point And Local," pp. 1–7.

[3] K. S. R. Murthy and V. M. Manikandan, "A Block-wise Histogram Shifting based Reversible Data Hiding Scheme with Overflow Handling," *2020 11th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2020*, pp. 11–16, 2020, doi: 10.1109/ICCCNT49239.2020.9225552.

[4] P. Rahmani and G. Dastghaibyfard, "A reversible data hiding scheme based on prediction-error expansion using pixel-based pixel value ordering predictor," *19th CSI Int. Symp. Artif. Intell. Signal Process. AISP 2017*, vol.2018-Janua, pp. 219–223, 2018, doi: 10.1109/AISP.2017.8324085.

[5] K. Subramanian and S. Vairachilai, "Reversible data hiding in digital image," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 6 Special Issue 3, pp. 2132–2136, 2019, doi: 10.35940/ijeat.F1387.0986S319.

[6] R. Thabit and B. E. Khoo, "Medical image authentication using SLT and IWT schemes," *Multimed. Tools Appl.*, vol. 76, no. 1, pp. 309–332, 2017, doi: 10.1007/s11042-015-3055-x.

[7] H. Golpira and H. Danyali, "Reversible medical image watermarking based on wavelet histogram shifting," *Imaging Sci. J.*, vol. 59, no. 1, pp. 49–59, 2011, doi: 10.1179/136821910X12863758415720.

[8] A. Kala, "Robust Lossless Image Watermarking in Integer Wavelet Domain using SVD," *Int. J.*

Comput. Sci. Eng., vol. 2, no. 02, pp. 30–35, 2013

[9] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–361, 2006, doi: 10.1109/TCSVT.2006.869964.

[10] N. K. Chen, C. Y. Su, C. Y. Shih, and Y. T. Chen, "Reversible watermarkingfor medical images using histogram shifting with location map reduction," *Proc. IEEE Int. Conf. Ind. Technol.*, vol. 2016-May, pp. 792–797, 2016, doi: 10.1109/ICIT.2016.7474852.

[11] R. J. Ramteke and K. M. Y, "Automatic Medical Image Classification and Abnormality Detection Using K- Nearest Neighbour," *Int. J. Adv. Comput. Res.*, vol. 2, no. 4, pp. 190–196, 2012

[12] C. Sreevidhya, M. Kumar, and K. Ilango, "Design and Implementation of Non-Intrusive Load Monitoring using Machine Learning Algorithm for Appliance Monitoring," *IEEE Int. Conf. Intell. Tech. Control. Optim. SignalProcess. INCOS 2019*, pp. 1–6, 2019, doi: 10.1109/INCOS45849.2019.8951312.