

Peningkatan *Reversible Watermarking* Menggunakan Metode *Spread Spectrum (SS)* Adaptif

1st Nurafifah Annida
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia

afifahnda@student.telkomuniversity.ac.id

2nd Ledy Novamizanti
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia

ledyaldn@telkomuniversity.ac.id

3rd Gelar Budiman
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia

gelarbudiman@telkomuniversity.ac.id

Abstrak — Dalam era digital yang terus berkembang, keamanan data menjadi tantangan signifikan akibat risiko modifikasi, akses tidak sah, dan pemalsuan informasi. Untuk mengatasi hal ini, berbagai langkah keamanan seperti enkripsi dan otentikasi telah dikembangkan guna melindungi integritas dan privasi data. Penelitian lebih lanjut diperlukan untuk mengembangkan metode yang lebih efisien dan aman dalam menjaga keamanan informasi digital di masa depan. Metode yang digunakan adalah *Robust Reversible Watermarking* menggunakan metode *reversible Spread Spectrum (SS)* Adaptif. Prosesnya dilakukan pemilihan skema *wavelet DWT* atau *IWT* dan membagi blok menjadi empat *sub-band LL, LH, HL, HH* dengan ukuran 8×8 . Setelah membagi blok citra, akan dilakukan penyematan *watermark key*. Setelah *watermark* disematkan, blok citra akan dikembalikan ke ukuran semula yaitu 32×32 dan dilakukan *invers* skema *wavelet DWT* atau *IWT*. Pengujian dilakukan menggunakan citra standar untuk pengolahan citra, dengan empat citra dari dataset yang ada dengan format citra BPM. Dengan melakukan serangan *JPEG Quality Factor*, *JPEG 2000 Compression Ratio*, *AWGN*, *Salt and Pepper Noise*, serta *Rotation attack*. Hasil menunjukkan bahwa ketahanan terhadap serangan *watermark* dan kemampuan memulihkan citra asli meningkat secara signifikan dengan nilai *PSNR* yang tinggi dan nilai *BER* 0. Kesimpulannya, metode ini secara efektif meningkatkan kinerja *watermarking reversibel* yang kuat.

Kata kunci— *Watermarking, citra digital, reversible, robust*

I. PENDAHULUAN

Dalam era digital yang semakin berkembang, teknologi telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari, membuat pertukaran informasi lebih efisien. Namun, kemudahan akses dan pertukaran informasi digital juga menghadirkan tantangan keamanan seperti modifikasi, penghapusan, akses tidak sah, dan pemalsuan oleh pihak yang tidak berwenang [1]. Salah satu metode yang sering digunakan untuk melindungi karya digital adalah teknik *watermarking* [2]. Teknologi digital *watermarking* menjadi sangat penting di berbagai bidang karena menawarkan solusi.

praktis untuk berbagai pendekatan dan metode [4]. Meskipun begitu, hasil *watermarking* tidak selalu sesuai harapan, sering kali disebabkan oleh gangguan atau perubahan yang ditimbulkan oleh *noise*.

Salah satu metode yang umum digunakan untuk melindungi citra digital adalah dengan menggunakan teknik *watermarking*. Teknik ini memungkinkan penyisipan informasi tambahan ke dalam citra digital tanpa mempengaruhi kualitas visualnya. *Watermarking* melibatkan metode dan teknologi yang menanamkan informasi (*watermark*) ke dalam objek *host* seperti gambar, video, audio, atau data digital lainnya [5]. Dalam bidang kesehatan, *watermarking* dapat digunakan untuk berbagai tujuan, seperti mengidentifikasi asal usul citra digital, melacak riwayat perubahan citra, dan melindungi privasi pasien. Namun, teknologi *watermarking* digital dapat menyebabkan penurunan kualitas citra asli. Meskipun penurunan kualitas ini mungkin tidak terasa oleh pengguna, di beberapa bidang, seperti digital, penurunan kualitas tersebut tidak dapat diterima [2].

Oleh karena itu, beberapa teknik *Robust Reversible Watermarking (RRW)* diusulkan sebagai solusi. Salah satunya adalah skema *reversible* yang dikembangkan oleh Huang, dkk. dan rekan-rekannya. Skema ini melibatkan dua tahap dalam proses penyisipan *watermark* ke dalam citra. Pada tahap pertama, *watermark* disisipkan menggunakan teknik *robust watermarking*, menghasilkan citra perantara. Pada tahap kedua, perbedaan antara citra sampul dan citra perantara dikompresi secara *lossless* dan dimasukkan kembali ke dalam citra perantara menggunakan teknik *watermarking* yang dapat dibalik, menghasilkan citra ber*watermark*. Namun, *noise* tetap akan muncul pada citra perantara karena baik penyematan yang kuat maupun *reversible* diterapkan dalam domain yang sama [6]. Oleh karena itu, disarankan penggunaan metode *Spread Spectrum (SS)* Adaptif untuk mencapai ketahanan (*robust*) dan reversibilitas secara bersamaan.

II. KAJIAN TEORI

RRW adalah teknik yang memungkinkan penyisipan dan ekstraksi *watermark* pada citra digital tanpa mengakibatkan kehilangan atau kerusakan permanen pada citra asli [3]. Teknik ini memanfaatkan redundansi di antara piksel-piksel

citra untuk menyisipkan dan mengekstrak *watermark*, sehingga citra asli dapat dipulihkan sepenuhnya tanpa kehilangan data akibat serangan. Teknik ini juga dikenal sebagai penyembunyian data reversibel atau penyembunyian informasi tanpa kehilangan, yang memungkinkan pemulihan citra asli secara utuh dan dapat digunakan untuk otentikasi yang sensitif. Keuntungan dari metode ini adalah kemampuannya untuk melakukan penyisipan dan ekstraksi *watermark* tanpa menyebabkan kerusakan pada citra asli, membuatnya ideal untuk aplikasi yang memerlukan ketelitian tinggi dan kehilangan data minimal, seperti penerbitan citra satelit, diagnosis citra digital, dan pemrosesan citra mikro. Terdapat beberapa skema RRW yang telah diusulkan, yaitu :

A. Reversible dengan Metode Spread Spectrum (SS)

Adaptif

Huang, dkk. mengusulkan metode RRW baru yang menggunakan metode *Spread Spectrum* (SS) adaptif untuk mencapai ketahanan dan reversibilitas secara bersamaan. Metode penyisipan, bersama dengan amplitudo SS dirancang sesuai dengan sinyal *host* untuk menangkal sumber interferensi, serta menyeimbangkan ketahanan dan citra ber*watermark*. Selanjutnya, amplitudo dibentuk sehingga nilainya dapat diperkirakan dengan benar pada penerima. Metode ekstraksi juga disarankan untuk meningkatkan akurasi ekstraksi di bawah serangan yang kuat. Hasil eksperimen menunjukkan bahwa skema yang diusulkan memberikan ketahanan yang baik terhadap serangan umum seperti JPEG *Quality Factor*, *Salt and Pepper Noise*, *Rotation*, dan sebagainya, serta dapat memulihkan citra asli dengan baik setelah citra ber*watermark* diserang [6].

B. Two-Stage Framework for Robust Reversible Watermarking

Metode *two-stage framework for robust reversible watermarking* yang diusulkan oleh Coltuc, dkk. adalah kerangka dua tahap untuk menyisipkan *watermark* ke dalam citra. Pada tahap pertama, *watermark* disisipkan menggunakan teknik *robust watermarking* tradisional, menghasilkan citra perantara. Di tahap kedua, perbedaan antara citra sampul dan citra perantara dikompresi secara *lossless* dan dimasukkan ke dalam citra perantara menggunakan teknik *reversible watermarking*, menghasilkan citra ber*watermark*. Keuntungan dari metode ini adalah kemampuannya menggabungkan teknik *Robust Watermarking* dengan *Reversible Watermarking*, memungkinkan ekstraksi dan pemulihan *watermark* meskipun terdapat distorsi. Namun, kelemahan metode ini termasuk penurunan ketahanan terhadap penyisipan tahap pertama akibat distorsi pada tahap kedua, yang dapat mengurangi efektivitas ekstraksi *watermark*. Selain itu, penggunaan domain penyisipan yang sama untuk kedua tahap dapat menambah *noise* pada citra perantara, mengurangi efektivitas *watermark* [8].

C. Robust Reversible Watermarking

RRW adalah sebuah teknik yang memungkinkan penyematan dan ekstraksi *watermark* pada citra digital tanpa menyebabkan kehilangan atau kerusakan permanen pada citra asli [9]. Teknik ini memanfaatkan redundansi di antara piksel citra untuk menyisipkan dan mengekstrak *watermark*, untuk memastikan citra asli dapat dipulihkan dengan

sempurna tanpa serangan apa pun. Teknik ini merupakan teknik yang menjanjikan untuk melindungi citra digital karena dapat memulihkan citra asli tanpa kehilangan data. RRW bertujuan untuk memberikan kinerja *Imperceptibility*, kapasitas, dan ketahanan yang optimal pada citra digital.

III. METODE

Solusi *reversible watermarking* ini menggunakan skema yang telah diusulkan oleh Huang, dkk., skema *reversible watermarking* dirancang menggunakan aplikasi MATLAB R2020a dengan citra *host grayscale* berukuran 512×512 , dan *watermark* berupa citra yang berisi identitas penulis, berukuran 32×32 . Gambar disisipkan menggunakan DWT atau IWT, dan kemudian dibagi menjadi empat *sub-band*: LL, LH, HL, dan HH. Proses penyisipan dilakukan pada *sub-band* LL, dan citra dibagi lagi menjadi 8×8 blok. Pada setiap blok, 16 piksel dipilih secara acak sesuai dengan kunci *watermark* untuk disisipkan. metode RRW menggunakan *Spread Spectrum* (SS) Adaptif ini diharapkan dapat menjadi salah satu solusi yang efektif untuk meningkatkan nilai PSNR.

A. Penyisipan Watermark

Skema ini akan memilih sub-band LL dengan ukuran 256×256 untuk penyisipan. Kami menetapkan ukuran blok citra ke 8×8 . Di setiap blok, 16 piksel dipilih secara acak sesuai dengan kunci *watermark*. Setiap blok akan disisipkan dengan satu bit *watermark*, dan bit *watermark* harus memiliki panjang 1024. Misalkan \mathbf{X} , \mathbf{Y} , dan $\tilde{\mathbf{Y}} \in [0, 255]^{512 \times 512}$ masing-masing menyatakan citra *host*, citra yang diberi *watermark*, dan citra yang diterima, dan biarkan $\mathbf{m} \in \{0, 1\}^{1024}$ menyatakan bit-bit *watermark* yang disisipkan. Kerangka kerja prosedur penyematan ditunjukkan pada langkah-langkah berikut:

Langkah 1. Pada tahap ini, kami melakukan parameterisasi vektor dengan nilai $1 \times N_x$ dengan ukuran $\mathbf{x} = [\mathbf{x}_1, \mathbf{x}_2, \dots,]$ dengan menyisipkan satu bit pesan $m \in \{0, 1\}$ dengan

$$\mathbf{Y} = \begin{cases} \mathbf{x} + \alpha \mathbf{w}, & \text{if } m = 1 \\ \mathbf{x} - \alpha \mathbf{w}, & \text{if } m = 0 \end{cases} \quad (1)$$

Langkah 2. Terapkan transformasi wavelet Haar pada \mathbf{X} dan bagi sub-band LL menjadi blok-blok yang tidak tumpang tindih dengan ukuran 8×8 .

Langkah 3. Untuk blok ke- i , gunakan kunci *watermark* k untuk memilih 16 koefisien di setiap blok, membentuk vektor

$$\alpha = F(\mathbf{x}, \mathbf{w}) + \lambda \times G(\mathbf{x}, \mathbf{w}) \quad (2)$$

Langkah 4. Hitung $F()$ dan $G()$ masing-masing, lalu hitung α dengan menggunakan

$$F(\mathbf{x}, \mathbf{w}) = \sqrt{\frac{N_x \alpha^2 - \lambda^2 \alpha_x^2}{N_x}}, \quad (3)$$

$$G(\mathbf{x}, \mathbf{w}) = \frac{\mathbf{x} \mathbf{w}^T}{N_x}, \quad (4)$$

Langkah 5. Sisipkan bit *watermark* m_i ke dalam \mathbf{x}_i dengan Persamaan (4) dengan α yang dihitung pada Langkah 3.

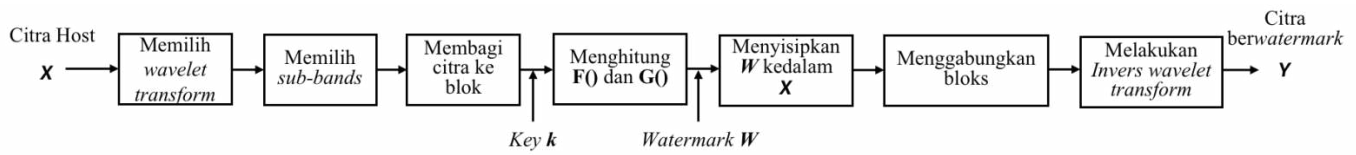
$$\tilde{m}_{i^*} = \begin{cases} 0, & \text{if } i^* \leq N_0 \\ 1, & \text{if } i^* > N_0 \end{cases} \quad (5)$$

Langkah 6. Ulangi Langkah. 2 sampai semua bit pesan telah disisipkan.

Langkah 7. Gabungkan semua blok berwatermark, yang menghasilkan *sub-band* LL berwatermark. Terapkan *invers*

transformasi *wavelet* Haar untuk mendapatkan citra berwatermark Y .

Langkah 8. Catat jumlah 0 pada urutan *watermark*, N_0 , dan kode ke dalam file citra.



GAMBAR 1
Proses Penyisipan Watermark

B. Ekstraksi Watermark

Ekstraksi *watermark* adalah proses mengisolasi *watermark* yang tertanam pada citra *host* sehingga dapat dipulihkan dalam bentuk aslinya. Proses ini bertujuan untuk mengembalikan *watermark* ke kondisi semula untuk dibandingkan dengan *watermark* asli untuk mengevaluasi kualitas ekstraksi. Metode yang diusulkan dapat mengekstrak *watermark* sepenuhnya tanpa degradasi atau kerusakan pada citra *host*. Bahkan ketika diserang, *watermark* masih dapat berhasil diekstraksi untuk verifikasi hak cipta, dan upaya dapat dilakukan untuk memulihkan citra *host*. Kerangka kerja prosedur ekstraksi ditunjukkan pada langkah-langkah berikut:

Langkah 1. Terapkan transformasi *wavelet* Haar pada citra yang diterima, dibagi *sub-band* LL ke dalam blok-blok yang tidak tumpang tindih dengan ukuran 8×8 .

Langkah 2. Untuk blok ke- i , temukan 16 koefisien *watermark* di blok tersebut sesuai dengan kunci *watermarking* x .

Langkah 3. Estimasi α dengan menggunakan $i(y', w)$ dan estimasi ambang batas G' dengan menggunakan

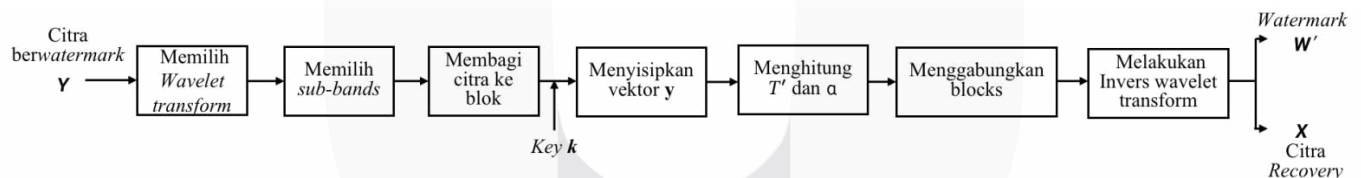
$$\tilde{G}(y', w) = \alpha + \frac{xw^T + nw^T}{N_x} \quad (6)$$

Langkah 4. Jika jumlah $\tilde{G}(y', w)$ yang terdistribusi di antara, $[-\frac{\tau+\alpha}{2}, \frac{\tau+\alpha}{2}]$ sama dengan N_0 , maka tidak ada atau hanya sedikit serangan pada gambar. Pergi ke Bagian Prosedur pemulihan citra.

$$\tilde{x} = y - \text{sign}(Z(y, w)) \times m \times \alpha \times w. \quad (7)$$

Langkah 5. Terapkan *invers* transformasi *wavelet* Haar pada citra yang diterima, dan bagi *sub-band* LL ke dalam blok-blok yang tidak tumpang tindih dengan ukuran 32×32 .

Langkah 6. Gabungkan semua blok berwatermark, yang menghasilkan *sub-band* LL berwatermark untuk mendapatkan citra berwatermark Y' dan citra yang dipulihkan x' .



GAMBAR 2
Proses Ekstraksi Watermark

IV. HASIL DAN PEMBAHASAN

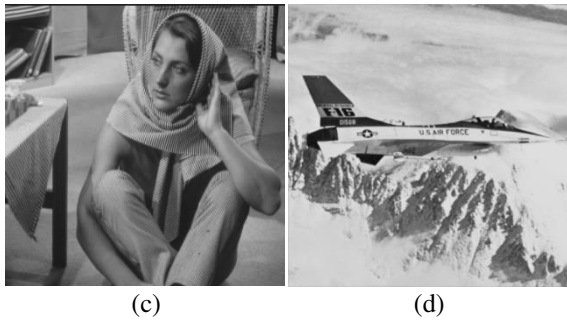
Dalam penelitian ini, dirancang sistem *watermarking* menggunakan aplikasi MATLAB R2020a dengan citra *host* *grayscale* berukuran 512×512 dan *watermark* berupa citra identitas penulis berukuran 32×32 . Pengujian dilakukan dengan menggunakan citra standar dari dataset yang terdiri dari empat citra: Peppers, Barbara, Airplane, dan Goldhills, semua dalam format BPM. Sistem ini mencakup dua proses utama, yaitu penyisipan (*embedding*) dan ekstraksi (*extraction*). Metode yang digunakan untuk penyisipan dan ekstraksi *watermark* adalah RRW dengan metode *reversible Spread Spectrum* (SS) Adaptif. Tujuan dari *watermarking* ini adalah untuk mencapai tingkat ketahanan yang lebih baik, sehingga sistem menjadi lebih *robust* terhadap serangan dan *watermark* tidak dapat dihapus atau dimodifikasi oleh pihak yang tidak berwenang. Proses *watermarking* akan dilakukan sesuai dengan skema yang ditunjukkan di bawah.

Gambar 3 merupakan citra *host* yang digunakan dalam sistem *watermarking* yang diusulkan. Gambar tersebut akan dilakukan proses penyisipan dengan menggunakan metode yang telah dirancang. Proses penyisipan *watermark* dilakukan untuk menyisipkan informasi bit biner ke dalam citra *host*. Penelitian ini dilakukan untuk melihat apakah metode yang di uji coba berhasil meningkatkan nilai *Imperceptibility*, *Robustness*, dan *Capacity*.



(a)

(b)



GAMBAR 3

Citra Host (a) Goldhills (b) Peppers (c) Barbara (d) Airplane

Tabel I merupakan hasil uji coba yang telah dilakukan.

TABEL 1

PERBANDINGAN METODE YANG DIUSULKAN DENGAN METODE SEBELUMNYA

Aspek Perbandingan	Robust Reversible Watermarking	Reversible based on Spread Spectrum (SS) Adaptif
<i>Imperceptibility</i>	Nilai rata-rata PSNR inf.	Nilai rata-rata PSNR 51.67 dB.
<i>Robustness</i>	Sistem memiliki ketahanan yang baik terhadap serangan JPEG, JPEG2000, dan AWGN.	Sistem memiliki ketahanan yang baik terhadap serangan JPEG dan AWGN.
<i>Capacity</i>	Dapat menyisipkan watermark hingga 32 bit.	Dapat menyisipkan watermark hingga 32 bit.

TABEL 2

HASIL PSNR PERBANDINGAN METODE YANG DIUSULKAN DENGAN METODE SEBELUMNYA

Metode	PSNR (dB)			
	Goldhills	Peppers	Barbara	Airplane
Huang, dkk.	50.44	49.36	48.70	48.70
Metode usulan	59.71	55.19	45.53	55.78

V. KESIMPULAN

Sistem *watermarking* ini dirancang untuk menjadi kuat dan memberikan ketahanan yang kuat terhadap berbagai serangan. Beberapa serangan diuji pada bagian ini untuk menentukan apakah sistem dapat bertahan secara efektif. Berdasarkan hasilnya, sistem menunjukkan ketahanan yang baik terhadap serangan JPEG *Quality Factor*, AWGN, dan *Salt and Pepper Noise*. Pengujian ini menunjukkan bahwa sistem berkinerja baik terhadap berbagai serangan *noise*, memungkinkan bit data dipulihkan dengan menggunakan informasi dari saat-saat lain, bahkan ketika ada *noise*. Namun demikian, sistem ini tidak tahan terhadap serangan Rotasi dan berkinerja buruk ketika terkena serangan Kompresi JPEG

2000. Hasil ini menunjukkan bahwa sistem *watermarking* dapat melindungi hak cipta dan integritas gambar dengan andal menggunakan skema DWT dan *sub-band* LL. Namun demikian, perbaikan lebih lanjut diperlukan untuk meningkatkan ketahanannya terhadap serangan yang lebih kompleks.

REFERENSI

- [1] L. Novamizanti, G. Budiman, and E. N. F. Astuti, "Robust audio watermarking based on transform domain and SVD with compressive sampling framework," TELKOMNIKA Telecommunication Computing Electronics and Control, vol. 18, no. 2, pp. 1079-1088, 2020, doi: 10.1093/icon/moab009.
- [2] Y. Hafizhana, I. Safitri, L. Novamizanti, and N. Ibrahim, Image Watermarking pada Citra Medis menggunakan Compressive Sensing berbasis Stationary Wavelet Transform. ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika, 8(1), p.43, 2020.
- [3] L. Novamizanti, I. Wahidah, and N. Wardana, "A Robust Medical Images Watermarking Using FDCuT-DCT-SVD," Int. J. Intell. Eng. Syst., vol. 13, no. 6, pp. 266–278, 2020, doi: 10.22266/ijies2020.1231.24.
- [4] L. Novamizanti, Suksmono, A.B., Danudirdjo, D., & Budiman, G. "Robust and Imperceptible Watermarking on Medical Images using Coefficient Pair Modification." IIUM Engineering Journal, vol. 24, no. 1, pp. 88-105, 2023.
- [5] A. H. Allaf and M. A. Kbir, "A Review of Digital Watermarking Applications for Medical Image Exchange Security", Springer International Publishing, 2019.
- [6] Z. Huang, B. Feng, S. Xiang, "Robust reversible image watermarking scheme based on spread spectrum", J. Vis. Commun. Image Represent., vol. 93, May 2023, doi: 10.1016/j.jvcir.2023.103808.
- [7] L. Novamizanti, A. B. Suksmono, D. Danudirdjo, & G. Budiman, "Robust Reversible Watermarking using Stationary Wavelet Transform and Multibit Spread Spectrum in Medical Images", International Journal of Intelligent Engineering and Systems, vol. 15, no. 3, pp. 343–354, 2022, doi: 10.22266/ijies2022.0630.29.
- [8] X. Wang, X. Li, and Q. Pei, "Independent Embedding Domain Based Two-Stage Robust Reversible Watermarking," IEEE Trans, Circuit and System for Video Technology, vol. 30, no. 8, pp. 2406-2417, 2020, doi: 10.1109/TCSVT.2019.2915116.
- [9] Y. Yunawan, I. Safitri, and L. Novamizanti. "Compressive sensing for image watermarking discrete wavelet transform and spread spectrum." In 2018 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), pp. 99-103. IEEE, 2018.