

WATERMARKING CITRA MEDIS MENGGUNAKAN SPREAD SPECTRUM DENGAN KODE HADAMARD

MEDICAL IMAGE WATERMARKING USING SPREAD SPECTRUM WITH HADAMARD CODE

Ghea Aldama Wulanda¹, Gelar Budiman², Sofia Sa'idah³

^{1,2,3}Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

¹ghealdama@telkomuniversity.ac.id, ²gelarbudiman@telkomuniversity.ac.id,

³sofiasaidahsfi@telkomuniversity.ac.id

Abstrak

Dalam era digital, perlindungan data medis semakin penting karena citra medis disimpan dan dibagikan secara elektronik. Salah satu cara efektif melindungi integritas citra medis adalah melalui *watermarking*, pada Tugas Akhir ini metode yang digunakan adalah watermarking spread spectrum dengan kode Hadamard pada citra medis. Kode Hadamard dipilih karena dapat melindungi citra dari serangan dan perubahan. *Watermark* disisipkan ke spektrum citra asli menggunakan kode Hadamard pada piksel citra. Ini memungkinkan penyisipan data yang kuat sambil menjaga kualitas citra penting untuk diagnosis. Penelitian ini menguji ketahanan citra ter-*watermark* terhadap berbagai serangan dan kemampuan sistem mendeteksi *watermark* pada citra yang diserang. Tugas Akhir ini menemukan bahwa sistem *watermarking* menunjukkan ketahanan yang baik terhadap berbagai serangan pada citra ter-*watermark*. Namun, terdapat beberapa serangan seperti serangan crop dengan parameter [2] dan serangan kompresi (jpeg) dengan parameter [70] yang menyebabkan sedikit kesulitan dalam pemulihan *watermark*. Meskipun begitu secara keseluruhan sistem *watermarking* tetap menunjukkan kinerja yang sangat baik dalam memulihkan *watermark* dari berbagai jenis serangan pada citra ter-*watermark*. Sistem ini telah diuji kualitasnya melalui parameter PSNR (Peak Signal-to-Noise Ratio) ≥ 30 dB, BER (Bit Error Rate) = 0, dan MOS (Mean Opinion Square) = 4.

Kata kunci : *Watermarking* , Citra medis , *Spread Spectrum* dan kode *Hadamard*

Abstract

In the digital era, safeguarding medical data has become increasingly crucial due to the electronic storage and sharing of medical images. One effective method to ensure the integrity of medical images is through watermarking. In this Final Project, the employed method is spread spectrum watermarking with Hadamard codes on medical images. Hadamard codes were selected for their ability to safeguard images against attacks and alterations. The watermark is embedded into the original image spectrum using Hadamard codes on the image pixels. This allows for robust data embedding while preserving image quality essential for diagnostics. This research examines the resilience of watermarked images against various attacks and the system's capability to detect watermarks on attacked images. The Final Project discovered that the watermarking system exhibited strong resilience against various attacks on watermarked images. However, some attacks, like crop attacks with [2] parameters and compression attacks (jpeg) with [70] parameters, posed slight challenges in watermark recovery. Nonetheless, overall, the watermarking system maintained excellent performance in recovering watermarks from various types of attacks on watermarked images. The system's quality was evaluated with parameters such as PSNR (Peak Signal-to-Noise Ratio) ≥ 30 dB, BER (Bit Error Rate) = 0, and MOS (Mean Opinion Square) = 4.

Keywords: *Watermarking* , *Medical Image*, *Spread Spectrum* and *Hadamard Code*

1. Pendahuluan

Citra medis merupakan bagian penting dalam bidang kedokteran dan pelayanan kesehatan. Citra medis, seperti hasil pemindaian *MRI*, *CT scan*, atau citra sinar-X, sering digunakan untuk *diagnosis*, perencanaan perawatan, dan pemantauan kondisi pasien[1]. Dengan kemajuan teknologi digital, citra medis kini dapat dengan mudah dibagikan dan diakses melalui platform digital, seperti jaringan komputer atau internet. Namun, dengan penyebaran yang cepat ini, muncul tantangan baru terkait perlindungan keaslian dan privasi data pasien[2]. Perlindungan keaslian citra medis menjadi sangat penting dalam memastikan integritas data dan mencegah penyalahgunaan. Dalam konteks ini, teknik *watermarking* menjadi solusi yang efektif untuk menyematkan informasi identifikasi pemilik atau hak cipta pada citra medis[3]. Teknik ini memungkinkan pelacakan citra, mencegah pemalsuan, dan memastikan keaslian citra medis[4].

Salah satu pendekatan yang digunakan dalam *watermarking* citra medis adalah *spread spectrum*. *Spread spectrum* adalah teknik yang memanfaatkan domain frekuensi untuk menyembunyikan informasi pada citra. Dalam konteks *watermarking*, informasi identifikasi atau pesan tersembunyi disematkan pada frekuensi yang tidak terlalu terlihat secara visual pada citra medis. Dengan menggunakan teknik *spread spectrum*, informasi *watermark* dapat diambil kembali dengan menggunakan kunci yang tepat[5]. Selain itu, dalam tugas akhir ini, digunakan juga kode *Hadamard* sebagai bagian dari proses *watermarking*. Kode *Hadamard* adalah jenis kode matematis yang sering digunakan dalam komunikasi dan pengolahan sinyal. Dalam konteks *watermarking*, kode *Hadamard* dapat digunakan untuk mengacak dan menyematkan informasi *watermark* pada citra medis dengan cara yang tidak mudah terdeteksi[6].

Tujuan dari tugas akhir ini adalah mengembangkan metode *watermarking* yang efektif dan efisien untuk melindungi keaslian citra medis tanpa merusak kualitas visualnya. Dalam konteks ini, pendekatan berbasis *spread spectrum* dengan menggunakan kode *Hadamard* dipilih sebagai pendekatan yang dapat memberikan perlindungan dan keaslian pada citra medis. Diharapkan bahwa metode *watermarking* yang dikembangkan dapat memberikan tingkat keamanan yang tinggi, ketahanan terhadap serangan.

2. Penelitian Terkait

Kumar dkk [5] mengusulkan metode aman *watermarking spread-spectrum* dengan kapasitas yang ditingkatkan dalam domain transformasi gelombang (*wavelet transform*) untuk menyisipkan informasi medis sensitif dalam bentuk teks. Teknik *encoding* BCH (*Bose-Chaudhuri-Hocquenghem*) digunakan untuk mengurangi kesalahan bit dalam proses pemulihan *watermark*. Keamanan dan kinerja dari metode tersebut diuji terhadap berbagai serangan, termasuk kompresi, penyaringan, gangguan saluran, penguatan, dan equalisasi histogram. Meskipun penggunaan kode pembenaran kesalahan seperti BCH masih menjadi masalah yang terbuka, terdapat alternatif lain seperti *turbo codes* yang dapat memberikan hasil yang lebih baik jika dibandingkan dengan *coder* BCH.

Reza Ahmad Nurfauzan dkk mengusulkan menggunakan metode *Discrete Wavelet Transform* dan *Singular Value Decomposition* dengan penyisipan *Spread Spectrum Image* ini dapat bekerja dengan baik dan memiliki ketahanan yang cukup baik terhadap *noise*, namun karena sistem ini termasuk *semi-blinded* maka sistem ini memerlukan beberapa informasi dari pesan dan cover untuk dapat mengekstrak pesan rahasia. Sistem ini tahan terhadap *noise salt & pepper* dan *noise Gaussian* dengan intensitas 0,6. Sistem ini juga tahan terhadap filter HPF namun tidak tahan terhadap filter LPF. Sistem ini memiliki nilai rata-rata PSNR 44 dB, SNR 39 dB, SSIM 0,9988 pada penyisipan kedua dan BER mendekati 0%.

Kumar dkk [7] mengusulkan dari metode *watermarking* yang diusulkan telah dipelajari secara mendalam hanya untuk *watermark* teks pada sub-blok DWT multilevel dengan menerapkan kode BCH pada *watermark* yang dianggap sebagai data EPR sebelum disisipkan ke dalam citra utama. Dalam pengujian, metode yang dikembangkan telah diuji terhadap serangan yang sudah diketahui sebelumnya. Kinerja PSNR dan BER dari metode yang diusulkan juga dibandingkan dengan teknik lain yang telah dilaporkan. Terbukti bahwa metode yang diusulkan menawarkan peningkatan kualitas visual citra ter*watermark* sebesar 7,93% dan mengurangi BER sebesar 1,53% jika dibandingkan dengan teknik yang telah dilaporkan. Selain itu, metode ini juga mengatasi masalah manajemen data kesehatan dengan menyisipkan *watermark* teks terenkripsi pada beberapa level sub-blok DWT dari citra sampel. Dari pembahasan di atas, terlihat bahwa metode ini berhasil mengurangi BER hingga 0,124% sambil memberikan tingkat keamanan tambahan untuk *watermark* teks melalui metode enkripsi. Selain itu, kinerja metode juga diuji untuk *multiple watermark* dengan menggunakan enkripsi dan kode BCH secara bersamaan.

3. Metode Penelitian

3.1 Spread Spectrum

Metode *Spread Spectrum* (Penyebaran Spektrum) adalah sebuah teknik yang digunakan untuk menyebarkan energi sinyal melalui rentang frekuensi yang lebih lebar daripada yang diperlukan secara normal. Tujuan utama dari metode *Spread Spectrum* adalah untuk meningkatkan ketahanan sinyal terhadap gangguan atau serangan serta memperbaiki keamanan dan privasi komunikasi.

Metode *Spread Spectrum* biasanya melibatkan modulasi sinyal dengan menggunakan suatu kode (*code*) atau rangkaian pengacak (*sequence*). Dalam metode ini, sinyal asli (sinyal informasi atau data) disebarkan atau diacak dengan menggunakan kode pengacak sehingga sinyal yang dihasilkan menjadi terlihat seperti *noise*.

Terdapat beberapa varian metode *Spread Spectrum* yang umum digunakan, seperti *Frequency Hopping Spread Spectrum* (FHSS) dan *Direct Sequence Spread Spectrum* (DSSS). Pada FHSS, frekuensi pembawa sinyal secara periodik berpindah-pindah secara acak, sedangkan pada DSSS, sinyal informasi dikalikan dengan sebuah kode pengacak yang memperluas spektrum sinyal.

Metode *Spread Spectrum* memiliki berbagai aplikasi, termasuk dalam komunikasi nirkabel, telekomunikasi, jaringan sensor, navigasi global (GPS), sistem keamanan, dan juga dalam teknik *watermarking* citra atau audio. Dengan menggunakan metode ini, sinyal dapat diubah sedemikian rupa sehingga lebih tahan terhadap gangguan atau serangan, dan informasi yang diinginkan dapat diekstraksi kembali dengan akurasi yang tinggi [8].

3.2 Kode Hadamard

Metode transformasi *Hadamard* adalah suatu metode transformasi dengan menggunakan matriks bujursangkar yang berisikan hanya 1 dan -1 yang memiliki dua atau lebih kolom atau baris yang terletak berhadapan dimana setengahnya bagiannya memiliki tanda yang sama dan setengah bagian lainnya memiliki tanda yang berlawanan. Suatu matriks *Hadamard* berukuran $n \times n$ (H_n) mempunyai kotak putih sebanyak $n(n-1)/2$ (bemilai -1) dan kotak hitam sebanyak $n(n+1)/2$ (bemilai 1). Suatu definisi tentang matriks *Hadamard* diberikan oleh persamaan berikut ini:

$$H_n H_n^T = n I_n \quad (1)$$

dimana I_n adalah matriks identitas. Untuk orde 2 maka matriks transformasi H_2 adalah :

$$H_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (2)$$

sedangkan untuk orde yang lebih besar maka matriks transformasi H_n dapat dicari dengan rumus sebagai berikut :

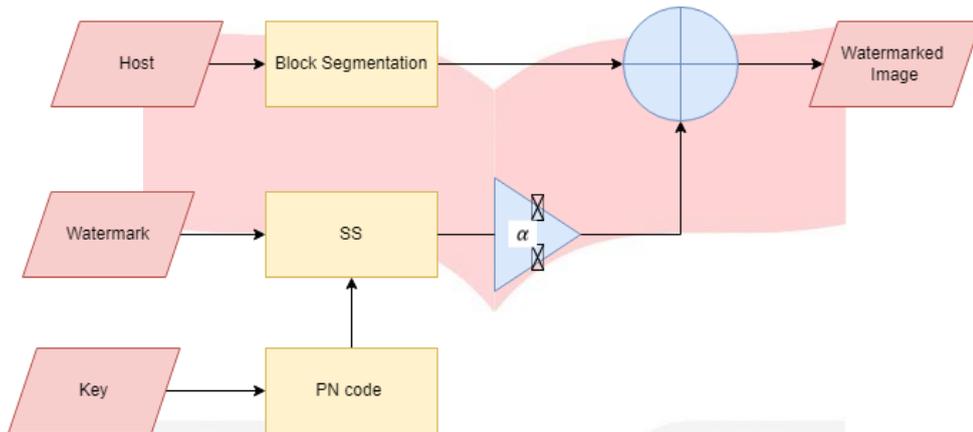
$$H_n = \frac{1}{\sqrt{n}} \begin{bmatrix} H_{n/2} & H_{n/2} \\ H_{n/2} & -H_{n/2} \end{bmatrix} \quad (3)$$

Setelah di-generate matriks sesuai dengan persamaan 2.6 kemudia dipilih baris atau kolom tertentu dari matriks H_n

untuk dijadikan kode yang memodulasi *watermark*, sesuai dengan kunci dalam proses penyisipan.

3.3 Embedding

Pada proses *embedding* terjadi proses penyisipan ke dalam seluruh bit sebuah *host*. Proses *embedding* dilakukan dengan menggunakan metode *Spread spectrum*. Citra *host* yang sudah disisipkan *watermark* akan mendapat hasil citra yang sudah ter-*watermark*. Proses penyisipan digambarkan melalui diagram blok sebagai berikut :



Gambar 1. Diagram Blok Embedding

Proses penyisipan adalah langkah dimana data *watermark* disematkan ke dalam sebuah citra *host*. Proses ini dimulai dengan melakukan segmentasi citra *host* dan kemudian menyematkan *watermark* yang telah dimodulasi menggunakan matriks *Hadamard* ke dalam citra *host*. Berikut ini adalah gambar diagram blok yang menggambarkan proses penyisipan *watermark* :

1. Baca *host* citra medis sebagai X_n berukuran $N \times M$ untuk dilakukan segmentasi

$$\text{Misalkan, } X_n = \begin{bmatrix} 1 \\ 0 \\ 4 \\ 2 \end{bmatrix}$$

2. Uraikan PN code melalui modulasi *spread spectrum* dan menggunakan matriks *Hadamard* hingga menghasilkan W_c

$$\text{Misalkan } W_c = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

3. Lanjutkan proses penyisipan sampai sistem *watermarking* menghasilkan citra ter-*watermark*

$$X_w = X + \alpha \cdot W_c \tag{4}$$

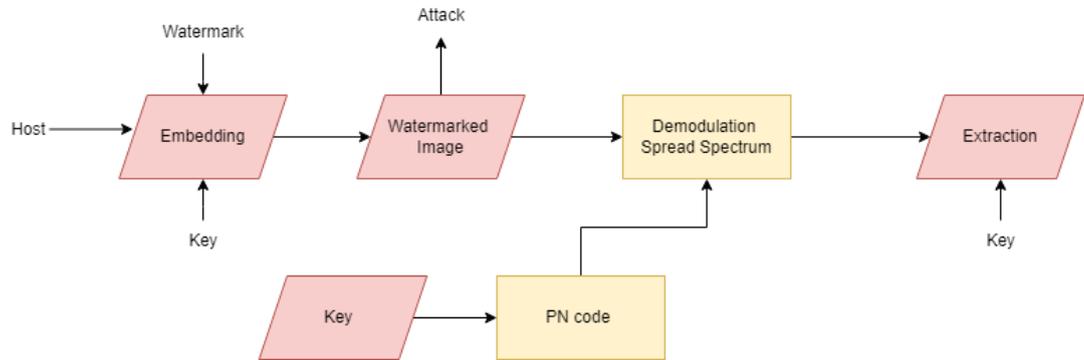
$$\text{Misalkan, citra } host \ X_n = \begin{bmatrix} 1 \\ 0 \\ 4 \\ 2 \end{bmatrix} \text{ disisipkan } watermark \ W_c = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Dengan alfa sebesar 2, maka X_w adalah sebagai berikut :

$$X_w = \begin{bmatrix} 1 \\ 0 \\ 4 \\ 2 \end{bmatrix} + 2 \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 4 \\ 2 \end{bmatrix} + \begin{bmatrix} 2 \\ 2 \\ 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \\ 6 \\ 4 \end{bmatrix}$$

3.4 Extraction

Melalui proses ekstraksi, *watermark* yang telah disisipkan dalam citra dapat diambil atau dikembalikan. Hal ini penting untuk membuktikan bahwa citra tersebut telah diberi *watermark*. Proses ekstraksi dilakukan dalam mode *blind*, yang berarti tidak membutuhkan sinyal *host*. Proses ini dapat digambarkan dalam bentuk diagram blok sebagai berikut:



Gambar 2. Diagram Blok Esktraksi

Pada Tugas Akhir ini , digunakan *watermark* berupa citra yang bertuliskan "TEL-U". Setelah proses ekstraksi selesai, citra tersebut akan muncul kembali. Proses ekstraksi melibatkan pengambilan kembali citra yang memiliki *watermark* berupa tulisan "TEL-U". Proses ekstraksi adalah sebagai berikut :

1. Deteksi *watermark* W_c dan citra ter-*watermark* X_w

$$\text{Misalkan, } W_c = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \text{ dan } X_w = \begin{bmatrix} 3 \\ 2 \\ 6 \\ 4 \end{bmatrix}$$

2. Lakukan perkalian pada *watermark* dan citra ter-*watermark*

$$\text{Misalkan, } W_c \times X_w = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \times \begin{bmatrix} 3 \\ 2 \\ 6 \\ 4 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \\ 6 \\ 4 \end{bmatrix}$$

3. Hasil perkalian antara *watermark* dan citra ter-*watermark* menghasilkan kembali nilai citra ter-*watermark* X_w

3.5 Parameter Kinerja Image Watermarking

Parameter dan performansi pada sistem *watermarking* citra adalah sebagai berikut :

1. *Peak Signal to Noise Ratio (PSNR)*

Peak Signal to Noise Ratio (PSNR) adalah suatu parameter yang digunakan untuk mengukur kualitas citra digital dengan membandingkan antara kekuatan sinyal maksimum dengan kekuatan derau yang mempengaruhi citra tersebut. PSNR biasanya diukur dalam satuan desibel (dB) dan memberikan indikasi seberapa dekat citra yang dihasilkan oleh sistem dengan citra aslinya Secara matematis dapat dituliskan sebagai berikut :

$$PSNR = 10 \cdot \log_{10} \frac{MAX^2}{MSE} \tag{5}$$

Dimana MAX adalah Nilai maksimum yang dapat dicapai oleh sinyal (misalnya, 255 untuk citra 8-bit) sedangkan MSE dirumuskan sebagai berikut :

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (X_w(i, j) - (X_{\hat{w}z}(i, j)))^2 \tag{6}$$

MSE adalah *Mean Squared Error*, yaitu rata-rata dari selisih kuadrat antara piksel citra asli dan piksel citra yang direkonstruksi.

2. *Error Rate (BER)*

BER merupakan ukuran yang digunakan untuk mengukur tingkat kesalahan bit dalam proses *watermarking*. Dalam konteks *watermarking*, BER memiliki pengaruh yang signifikan terhadap kualitas. Semakin kecil BER maka semakin bagus kualitas *watermarking*. Jika nilai BER=0 maka tidak terdapat *error* pada acitra hasil *watermarking*.

BER dituliskan atau dirumuskan sebagai berikut

$$BER = \frac{\text{Total bit error}}{\text{Total bit}} \times 100\% \quad (7)$$

3. Mean Opinion Score (MOS)

MOS adalah penilaian untuk mengevaluasi kualitas kinerja *watermarking* yang sifatnya subjektif. Penggunaan MOS dalam *watermarking* dapat membantu dalam mengevaluasi sejauh mana *watermark* dapat dipertahankan tanpa mengorbankan kualitas visual citra. MOS yang tinggi menunjukkan bahwa *watermark* tidak mengganggu kualitas citra secara signifikan, sementara MOS yang rendah dapat menunjukkan adanya distorsi atau gangguan yang terlihat pada citra.

Rating	Label
5	Excellent
4	Good
3	Fair
2	Poor
1	Bad

Tabel 1. Skala Rating MOS

4. Hasil dan Pembahasan

4.1 Pengaruh Alfa terhadap PSNR dan BER

Pengujian pengaruh alfa terhadap sistem *watermarking* dilakukan terhadap citra *host* (a) dan diuji dengan sistem *watermarking* menggunakan kode *Hadamard*. Blok yang digunakan pada pengujian ini bernilai 16.

alfa	PSNR (dB)	BER
0.1	68.1308	0.4141
1	48.1308	0.2168
10	28.1308	0.0527
35	17.2494	0
35.67	17.0847	0
100	8.1308	0

Tabel 2. Pengaruh Alfa Terhadap PSNR dan BER

Tabel menunjukkan perbandingan nilai PSNR (*Peak Signal-to-Noise Ratio*) dan BER (*Bit Error Rate*) pada sistem *watermarking* citra medis dengan variasi parameter alfa. Hasil dari pengujian menunjukkan bahwa nilai PSNR menurun seiring dengan peningkatan nilai alfa, sedangkan nilai BER cenderung meningkat dengan peningkatan nilai alfa. Hal ini menunjukkan bahwa semakin tinggi nilai alfa, maka PSNR akan menurun dan BER akan mendekati 0.

4.2 Pengaruh Blok Terhadap PSNR dan BER

Dalam pengujian untuk mengamati pengaruh parameter blok terhadap performa sistem yang diusulkan, dilakukan variasi pada nilai besaran blok yang digunakan dalam proses penyisipan. Hal ini bertujuan untuk mengevaluasi pengaruh parameter blok terhadap performa sistem yang telah dibuat alfa yang digunakan pada pengujian ini bernilai 4.

blok	PSNR (dB)	BER
2	36.0896	0.1667
4	36.0896	0.1578
8	36.0896	0.1582
16	36.0896	0.1416
32	36.0896	0.0703
64	36.0896	0

Tabel 3. Pengaruh Blok Terhadap PSNR dan BER

Dari tabel tersebut menunjukkan bahwa semua ukuran blok yang diuji (2, 4, 8, 16, 32, dan 64) menghasilkan nilai PSNR yang sama yaitu 36.0896. Hal ini menunjukkan bahwa ukuran blok tidak memiliki pengaruh terhadap kualitas citra hasil *watermarking* dalam hal PSNR. Namun, terdapat perbedaan yang signifikan dalam nilai BER antara ukuran blok yang berbeda. Semakin besar ukuran blok, semakin rendah nilai BER. Hal ini menunjukkan bahwa ukuran blok yang lebih besar memiliki kemampuan pemulihan data *watermark* yang lebih baik dan mengurangi kesalahan dalam proses pemulihan data *watermark*. Dalam skema *watermarking* pada Tugas Akhir ini, ukuran blok tidak memiliki pengaruh terhadap kualitas citra hasil *watermarking* dalam hal PSNR, tetapi memiliki pengaruh terhadap kemampuan pemulihan data *watermark* yang ditunjukkan oleh nilai BER. Ukuran blok yang lebih besar memberikan hasil yang lebih baik dalam pemulihan data *watermark* dengan nilai BER yang lebih rendah.

4.3 Parameter Terbaik

Setelah melakukan beberapa analisis seperti pada subbab 4.2, diambil yang dapat menghasilkan nilai PSNR ≥ 30 dB, nilai BER = 0, serta MOS ≥ 4 sebagai berikut :

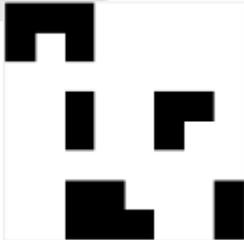
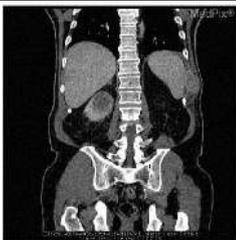
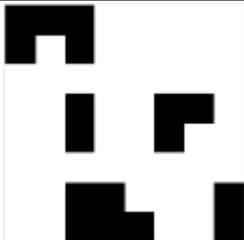
Host	Alfa	Blok	PSNR (dB)	MOS Terwatermark	BER
					Tanpa Serangan
a	8	64	30.069	4	0
b	6	64	32.5678	4	0
c	7	64	31.2288	4	0
d	3	64	38.5884	4	0
Rata-rata			33.1135	4	0

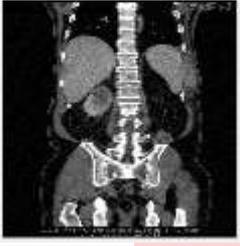
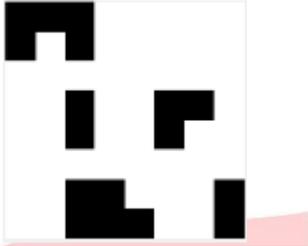
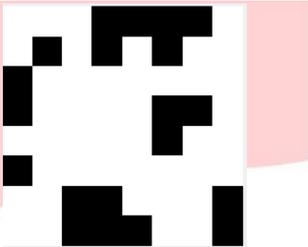
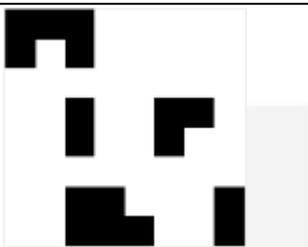
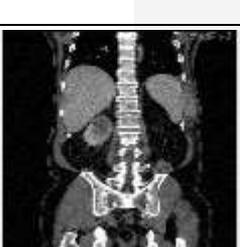
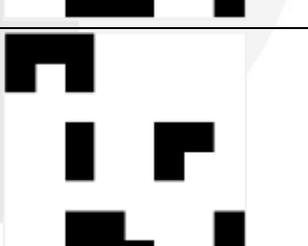
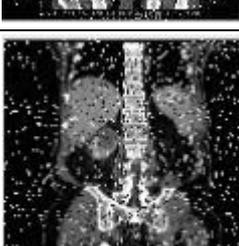
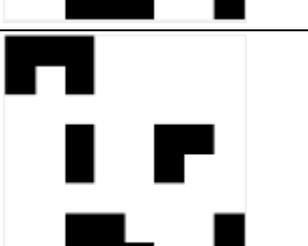
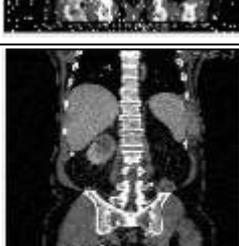
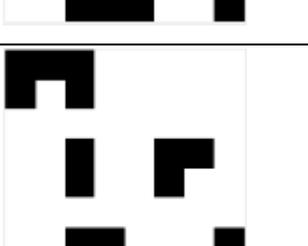
Tabel 4. Parameter Terbaik

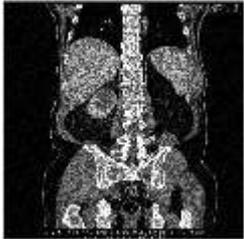
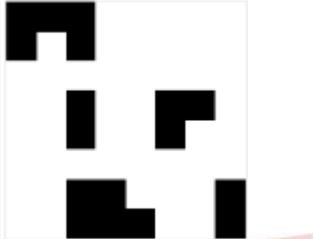
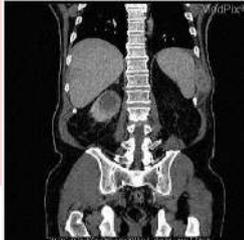
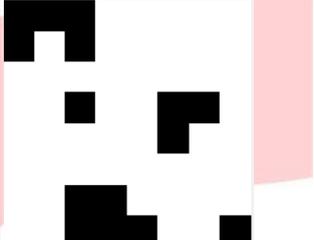
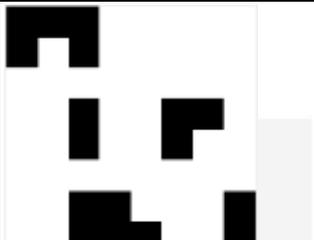
Hasil uji parameter terbaik pada sistem *watermarking* untuk secara keseluruhan dapat dilihat pada Lampiran I. Tabel 4.3 menunjukkan bahwa ada beberapa percobaan (a, b, c, dan d) yang dilakukan dengan berbagai kombinasi alfa dan ukuran blok tanpa ada serangan pada citra, percobaan dengan alfa = 3 menghasilkan nilai PSNR yang lebih tinggi (38.5884), MOS ter-*watermark* sebesar 4 (dari skala 1 hingga 5). Setiap *host* citra diberikan nilai alfa dan ukuran blok yang berbeda. Semua *host* citra memiliki MOS terwatermark yang sama yaitu 4, menunjukkan bahwa semua citra terwatermark dinilai memiliki kualitas visual yang baik. Selain itu, nilai BER untuk setiap citra adalah 0, menunjukkan bahwa proses ekstraksi *watermark* berjalan dengan baik dan tanpa kesalahan.

4.4 Analisis Ketahanan Sistem Watermarking Terhadap Serangan

Setelah melakukan uji coba terhadap parameter terbaik dalam sistem *watermarking*, dilakukan pula pengujian dengan menggunakan berbagai serangan untuk menguji sejauh mana sistem *watermarking* tersebut tahan terhadap serangan. Jenis serangan yang digunakan termasuk serangan rotasi, serangan *crop*, serangan *resize*, serangan *salt and pepper*, serangan *speckle*, serta serangan kompresi (jpeg).

Serangan	Citra Ter- watermark	Citra Diserang	Watermark Ekstraksi	BER
Rotasi [90]				0
Rotasi [180]				0

Cropping [1]				0
Cropping [2]				0.2656
Resize [3/2]				0
Resize [2]				0
Salt and Pepper [0.01]				0
Salt and Pepper [0.1]				0
Speckle [0.01]				0

Speckle [0.1]				0
JPEG [70]				0.0313
JPEG [90]				0

Tabel 5. Serangan Pada Citra Host CT scan

Hasil dari pengujian terhadap serangan tersebut adalah sistem *watermarking* di *host* (a) dengan Alfa=4 dan Blok=64 cenderung tahan terhadap serangan rotasi, serangan *crop* dengan parameter [1], serangan *resize*, serangan *salt and pepper*, serangan *speckle* serta serangan kompresi (jpeg) dengan parameter [90]. Di beberapa serangan seperti serangan *crop* dengan parameter [2] dan serangan kompresi (jpeg) dengan parameter [70] sistem *watermarking* mengalami sedikit kesulitan dalam memulihkan *watermark* namun secara keseluruhan, sistem *watermarking* menunjukkan kinerja yang sangat baik dalam memulihkan *watermark* dari berbagai jenis serangan pada citra *watermark*, dengan kualitas citra hasil *watermarking* yang tinggi dan tingkat kesalahan (BER) yang sangat rendah dan menghasilkan nilai PSNR yang sama yaitu 30.069 dB, dikarenakan nilai PSNR yang di hasilkan dari pengujian serangan ini memakai PSNR sebelum diberikan serangan maka nilai PSNR akan sama. Pada hasil uji terhadap serangan, terlihat bahwa *watermark* yang diekstraksi mengalami kerusakan. Hal ini disebabkan oleh modifikasi skema *watermarking* dalam Tugas Akhir ini, di mana citra *watermark* diubah menjadi ukuran 8x8 piksel perubahan ini dilakukan agar menghindari waktu ekstraksi yang sangat lama jika menggunakan ukuran asli citra *watermark*.

4.5 Perbandingan dengan Penelitian Terkait

Perbandingan dilakukan dengan penelitian terkait sebelumnya, yaitu dengan penelitian [5],[9], dan [7]. Parameter yang dibandingkan adalah PSNR dan BER saat sistem *watermarking* diberikan berbagai macam serangan. Berikut adalah tabel hasil perbandingan sistem yang diusulkan pada Tugas Akhir ini dengan penelitian terkait [5],[9], dan [7].

Ref	PSNR (dB)	BER					
		Rotasi	Cropping	Resize	Salt And Pepper	Speckle Noise	JPEG
[5]	44.3408	N/A	N/A	N/A	N/A	0	0
[9]	44	N/A	N/A	N/A	0	N/A	N/A
[7]	N/A	N/A	N/A	N/A	0.0472	N/A	0
Skema yang diusulkan	30.0690	0	0	0	0	0	0

Tabel 6. Perbandingan dengan penelitiin Terkait

Skema usul adalah skema yang diusulkan pada Tugas Akhir ini dan N/A merupakan tidak tersedia atau tidak ada data pada jurnal referensi. Dari hasil pengujian pada tabel 4.5 terlihat bahwa skema *watermarking* yang diusulkan memiliki nilai PSNR yang lebih rendah daripada beberapa metode lain yang diuji, tetapi memiliki nilai BER yang

lebih baik pada sebagian besar serangan, namun tetap mampu memulihkan *watermark* dengan akurasi yang tinggi dengan nilai BER yang rendah. Hal ini menunjukkan bahwa skema yang diusulkan mampu bersaing.

5. Kesimpulan

Tugas Akhir ini merancang skema *watermarking* pada citra medis dengan menggunakan metode *watermarking spread spectrum* dengan kode *Hadamard* untuk memperoleh penyematan *watermark* yang memiliki impersibilitas tinggi dan ketahanan *watermark* yang baik. Dari segi ketahanan sistem *watermarking* yang di rancang ini cenderung tahan terhadap serangan rotasi, serangan *crop* dengan parameter [1], serangan *resize* , serangan *salt and pepper* , serangan *speckle* serta serangan kompresi (jpeg) dengan parameter [90]. Hal ini dapat dilihat dari hasil pengujiannya citra ter-*watermark* menunjukkan performa yang cukup baik pada parameter terbaik dan parameter optimal dengan $PSNR \geq 30$ dB[10][11], $BER = 0$, serta MOS ter-*watermark* maupun MOS *watermark* = 4.

Sedangkan perubahan pada nilai alfa memiliki pengaruh terhadap PSNR dan BER. Saat nilai alfa meningkat, PSNR cenderung menurun sementara BER mendekati 0. Selanjutnya, ukuran blok juga memiliki dampak pada PSNR dan BER. Semakin besar ukuran blok, semakin rendah nilai BER yang diperoleh. Hasil ini menunjukkan bahwa penggunaan ukuran blok yang lebih besar memiliki kemampuan yang lebih baik dalam memulihkan data *watermark*, sementara ukuran blok tersebut tidak memiliki dampak yang signifikan pada kualitas visual citra hasil *watermarking* yang diukur melalui PSNR.

Referensi

- [1] I. M. A. D. S. Atmaja, "Kompresi Citra Medis Menggunakan Packet Wavelet Transform Dan Run Length Encoding," *Matrix J. Manaj. Teknol. dan Inform.*, vol. 8, no. 1, p. 10, 2018, doi: 10.31940/matrix.v8i1.739.
- [2] A. Nanda and T. Gelar, "Enkripsi Selektif Pada Citra Medis Dengan Menggunakan Linear Congruential Generator," *J. Inform. Polinema*, vol. 8, no. 2, pp. 1–8, 2022, doi: 10.33795/jip.v8i2.913.
- [3] L. Novamizanti, I. Safitri, H. B. Arindaka, and I. I. Tritoasmoro, "Watermarking berbasis Redundant Discrete Wavelet Transform dan Arnold Transform pada Citra Medis," *J. Tek. Elektro*, vol. 13, no. 2, pp. 48–55, 2021, doi: 10.15294/jte.v13i2.31691.
- [4] A. W. Kusuma and R. L. Ellyana, "Penerapan Citra Terkompresi Pada Segmentasi Citra Menggunakan Algoritma K-Means," *J. Terap. Teknol. Inf.*, vol. 2, no. 1, pp. 65–74, 2018, doi: 10.21460/jutei.2018.21.65.
- [5] B. Kumar, S. B. Kumar, and Di. S. Chauhan, "Wavelet based imperceptible medical image watermarking using spread-spectrum," *2015 38th Int. Conf. Telecommun. Signal Process. TSP 2015*, no. Ll, pp. 660–664, 2015, doi: 10.1109/TSP.2015.7296412.
- [6] M. M. Abdel-aziz, K. M. Hosny, N. A. Lashin, and M. M. Fouda, "Blind watermarking of color medical images using hadamard transform and fractional-order moments," *Sensors*, vol. 21, no. 23, 2021, doi: 10.3390/s21237845.
- [7] A. K. Singh, B. Kumar, G. Singh, and A. Mohan, *Secure Spread Spectrum Based Multiple Watermarking Technique for Medical Images*. 2017. doi: 10.1007/978-3-319-57699-2.
- [8] A. suci Adriansyah Hafiz ,Budiman Gelar, "OPTIMASI AUDIO WATERMARKING BERBASIS LIFTING WAVELET TRANSFORM DENGAN METODE SPREAD SPECTRUM MENGGUNAKAN ALGORITMA GENETIKA AUDIO," vol. 5, no. 2005, pp. 8–10, 2018.
- [9] R. A. Nurfauzan, B. Hidayat, and S. Saidah, "Analisis Steganografi Ganda pada Citra Digital Menggunakan Metode Discrete Wavelet Transform dan Singular Value Decomposition dengan Penyisipan Spread Spectrum Image Steganography," *Proceeding Eng.*, vol. 5, no. 1, pp. 299–304, 2018.
- [10] I. G. A. Garnita Darma Putri, N. P. Sastra, I. M. O. Widyantara, and D. M. Wiharta, "Kompresi Citra Medis dengan DWT dan Variable Length Code," *Maj. Ilm. Teknol. Elektro*, vol. 20, no. 2, p. 187, 2021, doi: 10.24843/mite.2021.v20i02.p02.
- [11] W. Y. Sulistyio *et al.*, "Analisis Perbandingan Kualitas Kompresi Citra Digital pada Media Sosial," vol. 2, no. 1, pp. 1–6, 2022, doi: 10.53863/juristik.v2i1.473.