

# Watermarking berbasis *Redundant Discrete Wavelet Transform* dan *Arnold Transform* pada Citra Medis

Ledy Novamizanti\*, Irma Safitri, Hafizhan Bhamakerti Arindaka, dan Iwan Iwut Tritoasmoro

School of Electrical Engineering, Telkom University  
Jl. Telekomunikasi No. 1, Terusan Buahbatu, Bandung, 40257, Indonesia

\*Corresponding author. Email: ledyaldn@telkomuniversity.ac.id

**Abstract**— *In telemedicine, data transmission in digital medical images and electronic medical records through the internet is vulnerable to various threats of theft and manipulation. Image watermarking is needed to provide authentication and security to medical images. This paper proposes an image watermarking scheme based on Redundant Discrete Wavelet Transform (RDWT) and Discrete Cosine Transform (DCT) with watermark encryption using Arnold transform. First, the original host medical image was decomposed into four subbands using RDWT. Then, DCT is applied to the LH subband of the RDWT. On the other hand, the watermark is scrambled using Arnold transform to ensure identity security. The singular value of the watermarked image is obtained by modifying the singular value of the host image and the watermark. Tests were carried out on different medical images, namely X-ray, MRI, CT, and ultrasound, with a watermark in a proprietary logo. The host medical image is the same size as the watermark image. The result of this study can provide high authentication, imperceptibility and security in medical images, with an average PSNR value of 65.67 dB, SSIM 1, BER 0, NC 1. This scheme is resistant to JPEG compression, noise addition, filtering, image sharpening, image enhancement, geometric operations, motion blur, image sharpening, and histogram equalization.*

**Keywords**— *medical image, watermarking, RDWT, DCT, SVD, Arnold transform*

**Abstrak**— *Pada telemedicine, transmisi data berupa citra medis digital dan rekam medis elektronik melalui jaringan internet rentan terhadap berbagai ancaman pencurian dan manipulasi. Watermarking citra dibutuhkan untuk memberikan autentikasi dan keamanan pada citra medis. Makalah ini mengusulkan skema watermarking citra berbasis Redundant Discrete Wavelet Transform (RDWT) dan Discrete Cosine Transform (DCT) dengan enkripsi watermark menggunakan Arnold transform. Pertama, citra medis host asli diuraikan menjadi empat subband menggunakan RDWT. Kemudian, DCT diterapkan pada subband LH dari RDWT. Di sisi lain, watermark diacak menggunakan Arnold transform untuk menjamin keamanan identitas. Nilai singular dari citra dengan watermark diperoleh dari modifikasi nilai singular citra host dan watermark. Pengujian dilakukan pada citra medis yang berbeda, yaitu X-ray, MRI, CT, dan Ultrasound, dengan watermark berupa logo kepemilikan. Citra medis host berukuran sama dengan citra watermark. Hasil dari penelitian ini dapat memberikan autentikasi, imperceptibility, dan keamanan yang tinggi pada citra medis, dengan rata-rata nilai PSNR sebesar 65,67 dB, SSIM 1, BER 0, NC 1. Skema ini tahan terhadap kompresi JPEG, penambahan noise, penapisan citra, penajaman citra, peningkatan kualitas citra, operasi geometris, motion blur, penajaman citra, dan histogram equalization.*

**Kata kunci**— *citra medis, watermarking, RDWT, DCT, SVD, Arnold transform*

## I. PENDAHULUAN

Beberapa tahun terakhir, teknologi *telemedicine* berperan penting dalam perkembangan aplikasi medis. Teknologi tersebut memungkinkan pasien mengirimkan data informasi dan berkonsultasi dengan dokter secara jarak jauh [1], [2]. Namun, transmisi data berupa citra medis digital dan rekam medis elektronik (RME) melalui jaringan terbuka rentan terhadap berbagai ancaman pencurian, kerusakan, manipulasi, dan distribusi data secara tidak sah [3] - [5]. Pengiriman citra medis digital dan RME secara terpisah juga beresiko salah penempatan, tidak teratur, dan dibutuhkan *bandwidth* tambahan. Teknik *watermarking* digital memberikan solusi alternatif untuk transmisi citra medis dan RME pasien yang aman [1], [6].

*Watermarking* citra digital adalah teknik untuk menyematkan informasi rahasia (watermark) ke dalam citra tertentu (citra *host*), kemudian watermark diekstrak di sisi penerima. Pada aplikasi medis, watermark dapat berupa RME atau logo instansi. Kriteria yang paling penting dari teknik *watermarking* citra, yaitu: *imperceptibility*, ketahanan, keamanan dan kapasitas data [7] - [9]. Banyak metode *watermarking* telah diusulkan terutama untuk memperbaiki dua syarat yang pertama. Namun, ketahanan dan *imperceptibility* bertentangan satu sama lain. Tantangannya adalah bagaimana menjaga keseimbangan di antara persyaratan tersebut yang menjadi isu utama dalam penelitian *watermarking* [10] - [12]. Para peneliti berusaha untuk mengembangkan skema *watermarking* yang dapat mempertahankan *imperceptibility* yang baik sambil memastikan keamanan yang tinggi dan melawan serangan (*attack*) berbahaya. Alasan utamanya adalah

Received 22 August 2021, Accepted 13 December 2021, Published 20 December 2021.

DOI: <https://doi.org/10.15294/jte.v13i2.31691>

serangan dapat mendistorsi bagian-bagian dari citra *host* yang membawa watermark yang mengakibatkan penurunan kualitas watermark yang diekstraksi [13].

Berdasarkan penyisipan informasi, algoritma *watermarking* dapat diklasifikasikan sebagai domain spasial dan domain transformasi. Pada domain spasial, watermark secara langsung disematkan pada nilai piksel, sedangkan pada domain transformasi, data disematkan dengan memodulasi besarnya koefisien yang ditransformasikan. Meskipun pendekatan domain spasial menguntungkan karena kompleksitasnya rendah dan implementasi yang mudah, pendekatan domain transformasi lebih disukai karena memiliki tingkat *imperceptibility* yang tinggi dan memberikan ketahanan yang lebih baik terhadap serangan [14] - [16].

*Singular Value Decomposition* (SVD) berbasis wavelet banyak digunakan sebagai transformasi dalam *watermarking* karena sifatnya yang kuat (*robust*) [17]. Penelitian [6], [9], [18] melaporkan gabungan dari metode *Discrete Wavelet Transform* (DWT), *Discrete Cosine Transform* (DCT), dan SVD untuk memberikan kompromi yang sangat baik antara *imperceptibility* dan ketahanan terhadap beberapa serangan. Penyisipan watermark dilakukan pada *subband* frekuensi tinggi HH, yang menawarkan *invisibility* yang lebih baik, serta dekomposisi DWT hingga level ketiga memungkinkan untuk meningkatkan kekokohan sistem *watermarking* terhadap berbagai serangan. Namun, penelitian [6] hanya teruji untuk tahan terhadap serangan *noise* dan *filtering*. Penelitian [9] mengusulkan *subband* LL dari citra *host* dalam domain DWT disegmentasi menjadi blok 8×8, dan setiap blok diproses oleh transformasi DCT. Di setiap blok koefisien DCT, koefisien frekuensi tengah dipilih untuk menyusun matriks modulasi dengan transformasi SVD. Nilai singular terbesar dari SVD digunakan untuk menyematkan watermark. Citra dengan watermark dienkripsi dengan algoritma enkripsi *chaotic* untuk kerahasiaan yang lebih baik menggunakan beberapa kunci rahasia [18], sehingga dihasilkan citra dengan watermark terenkripsi. Penelitian [19] menggunakan kode koreksi kesalahan Hamming pada bit teks RME untuk mengurangi BER, sehingga memberikan pemulihan RME yang lebih baik. Penelitian [13] merancang dan mengimplementasikan skema *watermarking* berbasis DWT dan dua level SVD. Sistem otentikasi dua level digunakan untuk memastikan keamanan dan meningkatkan kapasitas. Penelitian [12] dan [17] melaporkan bahwa skema *watermarking* citra berbasis SVD yang menggunakan *chaotic map* dapat mengatasi masalah *false positif* yang terdapat pada nilai singular.

Metode *watermarking* berbasis DWT umum digunakan karena sifat lokalisasi frekuensi spatio yang sangat baik sehingga dapat membantu menemukan area di citra *host* untuk menanamkan watermark secara tidak terlihat. Namun, selama proses *downsampling* DWT, informasi citra dapat dihapus. Karena koefisien yang dibuang ini, sedikit pergeseran atau modifikasi pada citra dapat mengurangi kemungkinan pemulihan watermark dari citra *host*. Untuk menghilangkan sifat *shift variant* ini digunakan *redundant* DWT (RDWT) yang bersifat *shift invariant* [8], [20], [21]. Karakteristik RDWT ini

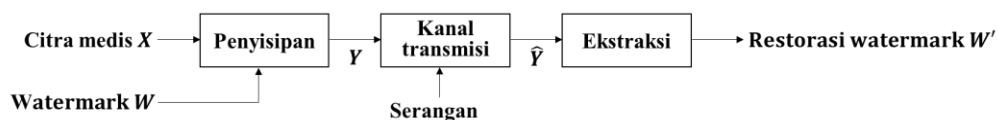
mengarah pada kekebalan yang sangat baik terhadap serangan [5]. Penelitian [5] dan [11] mengusulkan gabungan dari metode RDWT dan SVD. Penelitian [11] melaporkan metode *watermarking* berdasarkan blok citra 4×4 menggunakan RDWT dengan dekomposisi nilai singular dengan mempertimbangkan karakteristik sistem visual manusia yang dinyatakan oleh nilai entropi. Blok yang memiliki entropi lebih rendah dipilih untuk menyematkan watermark. Penelitian [5] mengusulkan komponen reflektansi citra *host* medis diperoleh dengan menggunakan *Homomorphic Transform*, dimana dekomposisi RDWT dan SVD diterapkan. Nilai singular digunakan untuk menyematkan citra watermark ke dalam citra *host*. Keamanan teknik ini dilakukan dengan mengenkripsi citra dengan watermark melalui pemetaan *Arnold Chaotic 2-D*.

Teknik *watermarking* citra medis yang diusulkan mengeksplorasi properti yang menguntungkan dari RDWT, DCT, dan SVD. Untuk menjamin keamanan, watermark diacak oleh *Arnold transform* sebelum disematkan ke dalam citra *host*. Dalam metode yang diusulkan, watermark yang diacak tidak dapat dipulihkan tanpa kunci rahasia dalam algoritma pengacakan sekalipun penyerang berhasil mengekstrak citra watermark. Tujuan utama dari skema yang diusulkan adalah untuk merancang teknik *watermarking* citra medis sedemikian rupa sehingga integritas watermark tidak rusak. Teknik *watermarking* ini menawarkan ketahanan yang baik dan *imperceptibility* dengan keamanan tinggi. Kelebihan utama dari teknik yang diusulkan adalah mencoba meminimalkan pencurian RME karena menggunakan citra medis dengan watermark untuk menjamin keamanan.

## II. METODE

Skema *watermarking* citra medis, terdiri dari dua proses, yaitu penyisipan dan ekstraksi. Pada tahap penyisipan, watermark  $W$  disembunyikan ke dalam citra medis *host* asli  $X$ , sehingga diperoleh citra dengan watermark  $Y$ . Ketika  $Y$  ditransmisikan melalui saluran transmisi maka serangan yang disengaja atau tidak disengaja dapat terjadi. Proses ekstraksi dapat menerima citra dengan watermark  $Y$  atau citra yang diserang  $\hat{Y}$ . Pada kasus ideal, ketika tidak ada serangan yang terjadi selama transmisi, maka watermark yang dipulihkan  $W'$  sama dengan watermark yang disisipkan  $W$  [22]. Gambar 1 menunjukkan skema *watermarking* citra medis secara umum.

Makalah ini mengusulkan skema *watermarking* pada citra medis yang menawarkan ketahanan dan *imperceptibility* dengan keamanan tinggi. Pada teknik penyematan, citra medis *host* asli diuraikan menjadi berbagai *subband* melalui RDWT. *Subband* terpilih diproses menggunakan DCT. Penerapan DCT dapat membagi citra kedalam tiga *subband* frekuensi, yaitu frekuensi rendah (LF), frekuensi tengah (MF), dan frekuensi tinggi (HF). Pada sisi lain, citra watermark terlebih dahulu dienkripsi menggunakan transformasi *Arnold Chaotic* untuk memberikan keamanan. Kemudian, hasil enkripsi watermark diproses menggunakan RDWT dan DCT. Nilai singular dari citra dengan watermark diperoleh dari modifikasi nilai singular citra *host* dan watermark.



Gambar 1. Skema *watermarking* citra medis secara umum

A. Proses Penyisipan

Bagian ini menjelaskan penyisipan watermark dalam bentuk citra logo instansi atau RME ke dalam citra medis *host*. Untuk menjamin keamanan, watermark diacak menggunakan *Arnold transform*. Fitur dari beberapa transformasi diterapkan pada citra *host* dan watermark, dan selanjutnya disisipkan menggunakan SVD. Keluaran dari proses penyisipan adalah citra medis dengan watermark. Gambar 2 mengilustrasikan teknik penyisipan dari makalah ini.

Tahapan dari teknik penyisipan watermark ke dalam citra medis adalah sebagai berikut:

- 1) Baca citra medis *host*  $X$  dan citra watermark  $W$ .
- 2) Lakukan pengacakan pada citra watermark  $W$  menggunakan *Arnold transform*, sehingga menghasilkan citra watermark yang diubah  $\hat{W}$ . Formulasi *Arnold transform* didefinisikan sebagai berikut:

$$\begin{bmatrix} \hat{a} \\ \hat{b} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \text{mod}(n) \quad (1)$$

dengan  $(a, b)$  dan  $(\hat{a}, \hat{b})$  masing-masing adalah koordinat piksel dari citra watermark dan citra watermark yang diubah, dan  $n$  merepresentasikan urutan citra. Proses iterasi pada (1) disebut sebagai periode Arnold. Pengacakan citra dilakukan berdasarkan periode Arnold yang dapat ditentukan [7], [23].

- 3) Terapkan RDWT pada  $X$  dan  $\hat{W}$  yang menguraikan masing-masing citra menjadi empat *subband*, yaitu: LL, HL, LH, dan HH.

$$\text{RDWT}(X) = [X_{LL}, X_{HL}, X_{LH}, X_{HH}] \quad (2)$$

$$\text{RDWT}(\hat{W}) = [\hat{W}_{LL}, \hat{W}_{HL}, \hat{W}_{LH}, \hat{W}_{HH}] \quad (3)$$

Subband LL (*low-low*) memiliki informasi detail dari suatu citra. Sedangkan subband LH (*low-high*), HL (*high-low*), dan HH (*high-high*) masing-masing memiliki informasi vertikal, horizontal, dan diagonal dari citra asli.

- 4) Terapkan DCT pada  $X_{LH}$  dan  $\hat{W}_{LH}$  yang menguraikan masing-masing citra menjadi tiga area frekuensi, yaitu: frekuensi rendah (LF), frekuensi tengah (MF), dan frekuensi tinggi (HF).

$$\text{DCT}(X_{LH}) = [X_{LF}, X_{MF}, X_{HF}] \quad (4)$$

$$\text{DCT}(\hat{W}_{LH}) = [\hat{W}_{LF}, \hat{W}_{MF}, \hat{W}_{HF}] \quad (5)$$

- 5) Terapkan SVD pada  $X_{HF}$  dan  $\hat{W}_{HF}$ , sehingga masing-masing citra menghasilkan tiga matriks baru, yaitu:  $U, S,$  dan  $V$ . Formulasi SVD didefinisikan sebagai berikut:

$$\text{SVD}(X_{HF}) = U_X S_X V_X^T \quad (6)$$

$$\text{SVD}(\hat{W}_{HF}) = U_W S_W V_W^T \quad (7)$$

- 6) Nilai singular dari citra dengan watermark  $S_Y$  diperoleh dari gabungan  $S_X$  dan  $S_W$  yang dipengaruhi oleh faktor *gain*  $\alpha$ . Sisipkan watermark ke dalam citra medis menggunakan SVD, ubah nilai singular citra medis pada  $S_X$  dan watermark pada  $S_W$ . Formulasi  $S_Y$  didefinisikan sebagai berikut:

$$S_Y = S_X + (\alpha \times S_W) \quad (8)$$

- 7) Citra medis dengan watermark  $Y$  diperoleh dengan melakukan transformasi *inverse* dari SVD, DCT, dan RDWT pada  $S_Y$ .

B. Proses Ekstraksi

Bagian ini menguraikan tugas penting dari proses ekstraksi, yaitu pengambilan citra watermark. Secara umum, teknik ekstraksi melakukan proses balikan dari teknik penyisipan. Dalam kasus ideal, pada kondisi tidak ada serangan yang terjadi selama transmisi, maka watermark yang dipulihkan  $W'$  sama dengan watermark yang disisipkan  $W$ . Gambar 3 mengilustrasikan teknik ekstraksi dari makalah ini. Tahapan dari teknik ekstraksi watermark adalah sebagai berikut:

- 1) Baca citra medis dengan watermark  $Y$ .
- 2) Terapkan RDWT pada  $Y$ , sehingga diperoleh empat *subband* berbeda

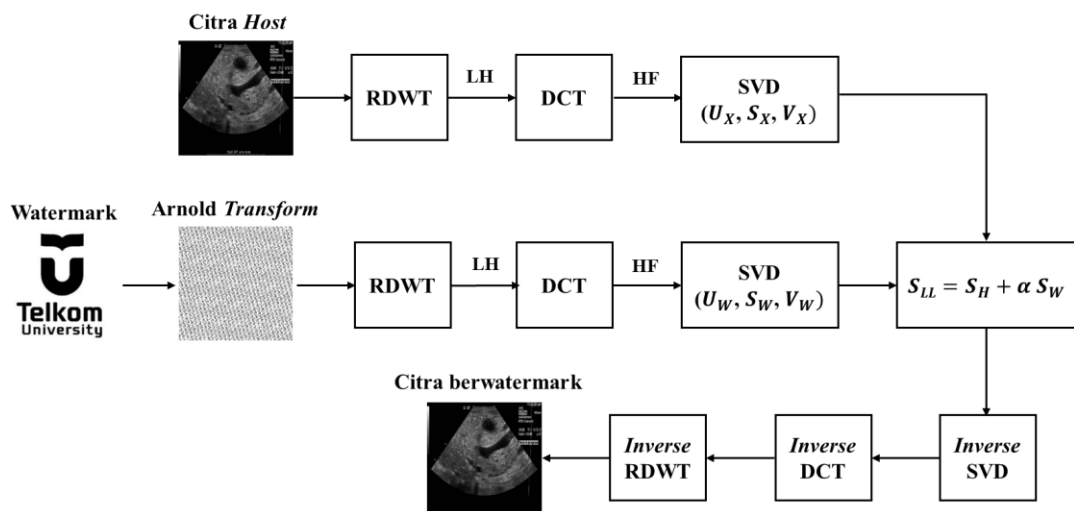
$$\text{RDWT}(Y) = [Y_{LL}, Y_{HL}, Y_{LH}, Y_{HH}] \quad (9)$$

- 3) Terapkan DCT pada  $Y_{LH}$ , sama seperti proses penyisipan.

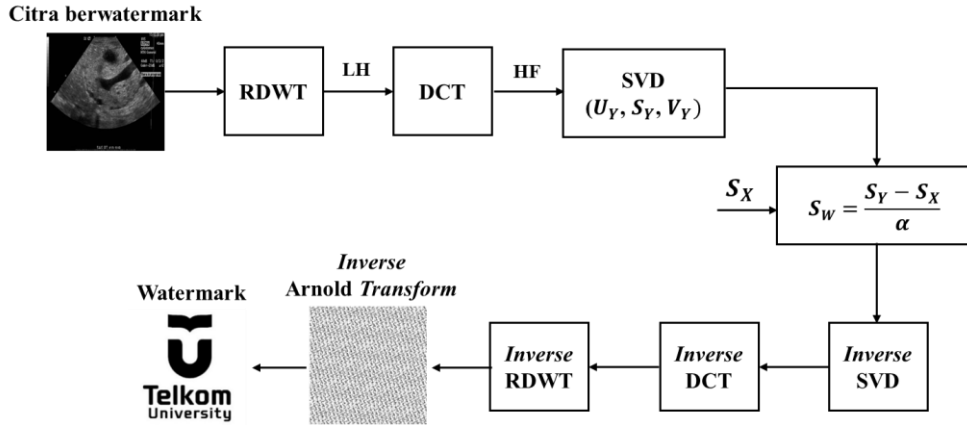
$$\text{DCT}(Y_{LH}) = [Y_{LF}, Y_{MF}, Y_{HF}] \quad (10)$$

- 4) Terapkan SVD pada  $Y_{HF}$ , sama seperti proses penyisipan.

$$\text{SVD}(Y_{HF}) = U_Y S_Y V_Y^T \quad (11)$$



Gambar 2. Proses penyisipan watermark pada skema usulan



Gambar 3. Proses ekstraksi watermark pada skema usulan

- 5) Nilai singular dari citra watermark  $S_W$  diperoleh melalui fungsi balikan (8), dengan formulasi sebagai berikut:

$$S_W = (S_Y - S_X) / \alpha \quad (12)$$

- 6) Rekonstruksi citra watermark  $\hat{W}$  dengan melakukan operasi *inverse* dari SVD, DCT, dan RDWT pada  $S_W$ .
- 7) Lakukan dekripsi terhadap  $\hat{W}$  menggunakan transformasi balikan dari (1), sehingga diperoleh citra watermark yang dipulihkan  $W'$ .

### C. Metrik Kinerja

*Peak Signal to Noise Ratio* (PSNR), dan *Structural Similarity Index Metric* (SSIM) adalah metrik yang digunakan untuk mengevaluasi ketidaktampakan persepsi (*imperceptibility*). PSNR terutama berfokus pada kesamaan visual antara citra asli dan citra yang diberi watermark. Kedua citra harus tampak sama sehingga tidak ada perbedaan besar di antara keduanya. Semakin tinggi nilai PSNR maka semakin mirip kedua citra tersebut, begitu pula sebaliknya [24], [25]. Diketahui  $X$  merupakan citra *host* asli,  $Y$  merupakan citra *host* dengan watermark, dan  $M \times N$  adalah ukuran dari citra *host*. Secara matematis, PSNR diformulasikan sebagai berikut:

$$PSNR = 10 \log \frac{255^2 \times M \times N}{\sum_{i=1}^M \sum_{j=1}^N (X-Y)^2} \quad (13)$$

SSIM adalah metrik yang mengevaluasi kesamaan struktural antara citra asli dan citra dengan watermark. Idealnya, nilai SSIM mendekati 1 yang berarti dua buah citra tersebut sama [14]. Secara matematis, SSIM dinyatakan sebagai berikut:

$$SSIM(X, Y) = \frac{(2 \mu_X \mu_Y + C_1)(2 \sigma_{XY} + C_2)}{(\mu_X^2 + \mu_Y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_2)} \quad (14)$$

dengan  $\mu_X, \mu_Y, \sigma_X, \sigma_Y$ , dan  $\sigma_{XY}$  adalah rerata lokal, simpangan baku, dan *cross covariance* untuk citra  $X$  dan  $Y$  [2].

*Bit Error Rate* (BER) dan *Normalized Correlation* (NC) adalah metrik yang digunakan untuk mengevaluasi ketahanan (*robustness*) suatu teknik *watermarking* citra medis yang diusulkan dalam menghadapi serangan. Teknisnya, BER mengukur tingkat kesalahan bit setelah proses ekstraksi watermark. Jika nilai BER mendekati 0 maka tingkat kesalahan bit sedikit, dan demikian sebaliknya. Idealnya, nilai BER harus bernilai nol [25]. Jika  $DB$  adalah jumlah bit yang salah di decode dan  $NB$  adalah jumlah total bit watermark secara keseluruhan, maka secara matematis BER diformulasikan sebagai berikut [8]:

$$BER = \frac{DB}{NB} \quad (15)$$

Secara matematis, NC dapat dihitung sebagai berikut:

$$NC = \frac{\sum_{i=1}^M \sum_{j=1}^N W \times W'}{\sum_{i=1}^M \sum_{j=1}^N W^2} \quad (16)$$

Jika nilai NC mendekati 0 maka ketahanan sistem *watermarking* bersifat rapuh. Sebaliknya, apabila NC bernilai 1 maka sistem *watermarking* dapat dikatakan *robust*. Semakin besar nilai NC maka semakin tinggi korelasi antara watermark asli  $W$  dan watermark yang dipulihkan  $W'$ . Nilai NC harus di atas 0,9 agar skema dapat menahan serangan [5].

Kapasitas muatan (*payload capacity*) dari setiap sistem *watermarking* dapat didefinisikan sebagai jumlah informasi watermark yang dimasukkan ke dalam media *host*. Dalam makalah ini, kapasitas muatan (PC) dihitung menggunakan persamaan berikut [2]:

$$PC = \frac{\text{ukuran watermark}}{\text{ukuran host}} \quad (17)$$

Kapasitas muatan dapat dihitung dengan sejumlah bit yang tertanam dalam piksel *host* atau rasio ukuran watermark dengan ukuran media *host*.

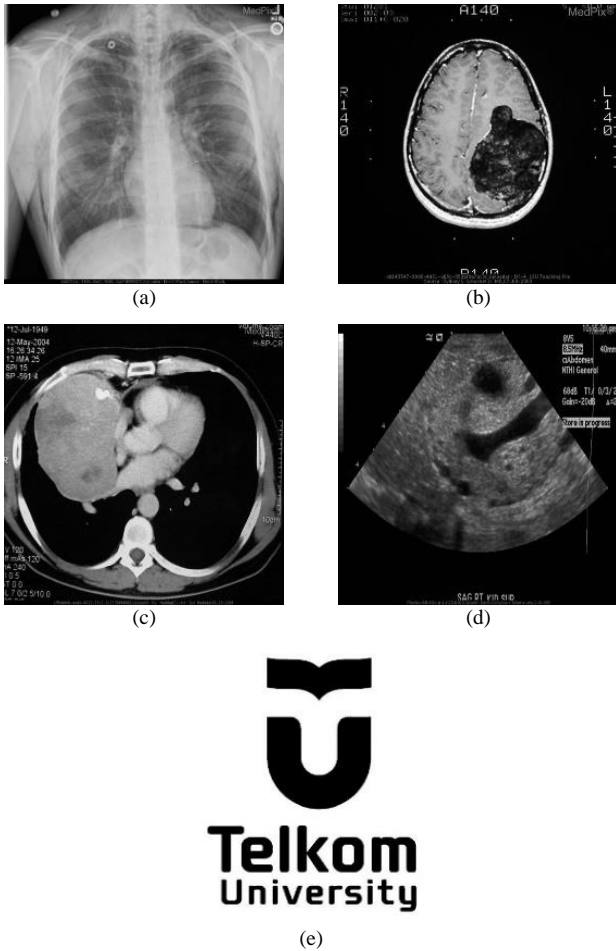
## III. HASIL DAN PEMBAHASAN

Bagian ini membahas kinerja teknik yang diusulkan. Pengujian teknik ini menggunakan citra *host* medis berformat *grayscale*, dan berukuran  $512 \times 512$  piksel. Sebanyak sepuluh citra diambil dari empat jenis modalitas citra medis, antara lain: *Magnetic Resonance Imaging* (MRI), X-Ray, *Computed Tomography* (CT), dan *Ultrasound* (US) diperoleh dari MedPix™ *Medical Image Database*. Empat modalitas tersebut umum dan banyak digunakan oleh peneliti dalam bidang *medical image watermarking*. Sedangkan citra logo Tel-U dipilih sebagai watermark berukuran  $512 \times 512$  piksel. Beberapa citra *host* yang digunakan ditunjukkan pada Gambar 4 (a-d), sementara citra watermark disajikan pada Gambar 4(e). Efisiensi skema yang diusulkan dievaluasi secara menyeluruh baik dari sisi parameter dari teknik yang digunakan maupun ketahanan *watermarking* dalam menghadapi berbagai serangan.

### A. Pengujian Parameter

#### 1) Level dan Subband RDWT

Pada bagian ini dilakukan pengujian *subband* RDWT terhadap kinerja *watermarking*. Terdapat empat *subband* keluaran RDWT, yaitu: LL, LH, HL, dan HH. Metrik kinerja *watermarking* berupa PSNR, SSIM, dan BER pada pengujian *subband* RDWT ditampilkan pada Tabel I.



Gambar 4. Citra uji (a-d) citra medis *host* (X-ray, MRI, CT, dan US) dan (e) watermark

TABEL I. HASIL KINERJA TERHADAP JENIS *SUBBAND* RDWT

<i>Subband</i>	PSNR (dB)	SSIM	BER
LL	56,436	0,9994	0,1133
LH	65,7323	1	0
HL	65,2507	0,9999	0
HH	64,2919	0,9999	0

Hasil dari pengujian jenis *subband* RDWT pada Tabel I menunjukkan bahwa nilai metrik PSNR yang dicapai cukup signifikan karena lebih besar dari 50 dB untuk semua *subband* wavelet. Pada *subband* LH, metrik SSIM dan BER mencapai nilai ideal, yaitu SSIM bernilai 1 dan BER bernilai 0. SSIM bernilai 1 berarti kesamaan struktural yang baik antara citra *host* asli dan yang diberi watermark. Ketidaktampakan persepsi untuk pendekatan yang diusulkan ditandai dengan menghitung PSNR yang jauh di atas 30 dB. Pada *subband* LH diperoleh nilai rata-rata PSNR adalah 65,7323 dB yaitu hampir 66 dB. Rasio kesalahan bit setelah proses ekstraksi watermark dihitung menggunakan BER. Nilai BER bernilai 0 yang berarti watermark berhasil dipulihkan di sisi penerima. Oleh karena itu, dipilih jenis *subband* LH karena menghasilkan kinerja *watermarking* yang paling baik diantara *subband* lainnya.

### 2) Jumlah Iterasi *Arnold Transform*

Pada bagian ini dilakukan pengujian jumlah iterasi pada *Arnold transform* terhadap kinerja *watermarking*. Jumlah iterasi yang diujikan, yaitu: 10, 30, 50, 70, dan 90. Metrik kinerja *watermarking* untuk pengujian iterasi *Arnold transform* ditampilkan pada Tabel II.

TABEL II. HASIL KINERJA PADA JUMLAH ITERASI *ARNOLD TRANSFORM*

Iterasi	PSNR (dB)	SSIM	BER
10	64,4338	0,9999	0
30	61,2377	0,9998	0
50	63,1691	0,9999	0
70	63,4564	0,9999	0
90	65,7323	1	0

*Arnold transform* digunakan dalam tahapan pemrosesan awal dari metode yang diusulkan. Tujuan penerapan *Arnold transform* adalah untuk memberikan keamanan ekstra pada watermark yang disematkan. Berdasarkan Tabel II, pada iterasi ke-10, skema yang diusulkan telah menghasilkan kinerja SSIM yang mendekati 1. Nilai PSNR sangat tinggi, yaitu di atas 60 dB. Semakin banyak jumlah iterasi dari *Arnold transform* maka nilai SSIM dan BER semakin baik. Namun, nilai PSNR yang dihasilkan cenderung fluktuatif. Metode *Arnold transform* mengacak posisi piksel dari citra watermark untuk menghasilkan citra yang kacau. Watermark yang kacau ini tidak dapat dipulihkan tanpa informasi yang tepat tentang algoritma pengacakan, bahkan jika penyerang berhasil mengekstrak watermark dari citra *host*.

### 3) Faktor *Gain* $\alpha$

Pada bagian ini dilakukan pengujian faktor *gain* ( $\alpha$ ) terhadap kinerja *watermarking*. Nilai  $\alpha$  yang diujikan rentang 0,01 hingga 0,09. Metrik kinerja *watermarking* untuk pengujian faktor *gain* ( $\alpha$ ) ditampilkan pada Tabel III.

TABEL III. HASIL KINERJA TERHADAP *GAIN* FACTOR ( $\alpha$ )

<i>Subband</i>	PSNR (dB)	SSIM	BER
0,01	65,7323	1	0
0,03	54,7375	0,9991	0
0,05	50,2951	0,9974	0
0,07	47,4758	0,9951	0
0,09	45,3802	0,9923	0

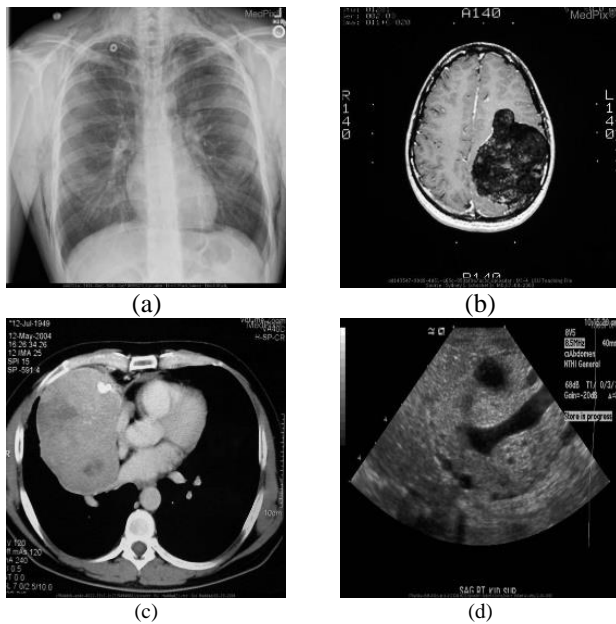
Nilai faktor *gain*  $\alpha$  menentukan kekuatan penyisipan watermark ke dalam citra medis *host*. Pada proses penyisipan, parameter  $\alpha$  diterapkan di (8) dan (12). Berdasarkan Tabel III, semakin rendah nilai  $\alpha$  yang digunakan, maka semakin tinggi nilai PSNR dan SSIM yang dihasilkan. Pada  $\alpha = 0,01$  diperoleh nilai rata-rata PSNR adalah 66 dB, metrik SSIM dan BER mencapai nilai ideal, yaitu SSIM bernilai 1 dan BER bernilai 0. Faktor *gain* memperkecil nilai singular dari citra watermark, sehingga *imperceptibility* dari citra medis *host* untuk pendekatan yang diusulkan lebih dominan. Metrik kinerja untuk empat citra medis saat tanpa serangan ditabulasikan pada Tabel IV. Sedangkan hasil citra dengan watermark ditampilkan pada Gambar 5.

TABEL IV. HASIL KINERJA PADA BERBAGAI CITRA MEDIS

Citra medis	PSNR (dB)	SSIM	BER	NC
X-ray	65,7323	1	0	1
MRI	65,2790	1	0	1
CT	65,7304	1	0	1
US	65,9443	1	0	1
Rata-rata	65,6715	1	0	1

Berdasarkan Tabel IV, metrik kinerja *watermarking* yang diusulkan untuk empat citra medis *host* mencapai nilai ideal, yaitu SSIM dan NC bernilai 1, dan BER bernilai 0 pada kondisi tanpa serangan. SSIM bernilai 1 yang berarti terdapat kesamaan struktural yang baik antara citra *host* asli dan yang diberi watermark. Nilai BER yang dihasilkan 0 berarti saat proses ekstraksi tidak terdapat kesalahan bit pada watermark. NC

bernilai 1 yang berarti ketahanan dari pendekatan yang diusulkan terhadap serangan sangat baik. Rerata PSNR yang dihasilkan untuk empat citra sebesar 65,6715 dB. Nilai metrik PSNR yang dicapai cukup signifikan karena lebih besar dari 60 dB untuk semua citra medis.



Gambar 5. Hasil citra dengan watermark (a) X-ray, (b) MRI, (c) CT, dan (d) US

Pada Gambar 5, kualitas secara visual dari citra dengan watermark yang dihasilkan mirip dengan citra medis *host* asli. Dengan demikian, skema *watermarking* yang diusulkan pada makalah ini memiliki *imperceptibility* dan ketahanan yang sangat baik.

Parameter penting lainnya dalam algoritma *watermarking*, yaitu kapasitas muatan. Ukuran citra medis *host* dan watermark, keduanya yaitu 512×512 piksel. Besar kapasitas muatan dihitung menggunakan (17), sehingga diperoleh PC bernilai 1. Skema *watermarking* citra yang diusulkan memiliki kapasitas muatan yang tinggi, karena citra *host* dapat menampung informasi watermark yang ukurannya sama dengan citra medis *host*.

## B. Hasil Ketahanan *Watermarking* pada Berbagai Serangan

Bagian ini mengevaluasi seberapa kokoh skema yang diusulkan terhadap berbagai serangan. Jenis serangan yang diberikan yaitu: kompresi JPEG, penambahan *noise*, penapisan citra, geometri, dan serangan pengolahan sinyal lainnya.

### 1) Kompresi JPEG.

Kompresi JPEG adalah salah satu serangan kompresi umum yang paling banyak digunakan oleh pengguna. Setiap watermark yang efektif harus *robust* sampai tingkat kompresi tertentu. Skema yang diusulkan diuji terhadap kompresi JPEG dengan mengubah nilai faktor kualitas (QF). Nilai QF berada dalam kisaran [0, 100]. Semakin kecil nilai QF maka kualitas citra lebih rendah, namun kompresi citra lebih besar. Demikian sebaliknya. Gambar 6(b-d) menampilkan hasil watermark yang dipulihkan untuk serangan kompresi JPEG dengan QF=10, 20, dan 30. Peningkatan pemulihan kualitas watermark sebanding dengan peningkatan faktor kualitas kompresi JPEG. Nilai NC mendekati 1 yang berarti skema yang diusulkan tahan terhadap serangan kompresi JPEG.

### 2) Penambahan *Noise*

Serangan non-geometris yang paling banyak dibahas dalam pemrosesan sinyal adalah penambahan *noise*. Skema yang diusulkan diujicobakan terhadap *salt and pepper*, *speckle* dan *Gaussian noise*. *Salt and pepper noise* disebabkan oleh kesalahan piksel pada saat pengiriman data. Modifikasi nilai piksel ini memberikan tampilan seperti *salt and pepper* pada citra, dimana kerapatan *noise* dihitung dengan mengubah persentase piksel [2].

Metode ini diuji terhadap *salt and pepper noise* dengan tiga kerapatan *noise* yang berbeda, seperti yang disajikan pada Gambar 6(e) dan Tabel V. Hasil pengujian menunjukkan bahwa skema yang diusulkan dapat memulihkan citra watermark dengan sedikit kesalahan piksel. Nilai NC mendekati 1 yang berarti skema yang diusulkan tahan terhadap serangan *salt and pepper noise*.

*Speckle noise* merupakan derau yang timbul karena pengaruh sensor pencitraan saat akuisisi citra [8]. Metode ini diuji terhadap *noise speckle* pada tiga varian *noise* yang berbeda. Citra watermark restorasi yang dimanipulasi oleh *speckle noise* dengan varians=0,005 ditampilkan pada Gambar 6(f). Dari Tabel V, dapat dilihat bahwa pemulihan kualitas logo watermark ditingkatkan dengan pengurangan varians *noise*. Nilai NC dari pemulihan watermark menunjukkan proporsionalitas terbalik dengan varian citra *speckle noise*.

*Gaussian noise* adalah salah satu operasi pemrosesan *noise* statistik yang umum digunakan. Efek *noise* bergantung pada besar variansnya dengan mean nol. Untuk menguji ketahanan, *noise* statistik ini ditambahkan ke citra dengan watermark dari metode ini. Citra watermark restorasi yang dimanipulasi dan NC dari *Gaussian noise* dengan varians=0,005 ditampilkan pada Gambar 6(g) dan Tabel V. Nilai NC mendekati 1 menunjukkan bahwa skema yang diusulkan tahan terhadap serangan *Gaussian noise*.

### 3) Penapisan Citra

Jenis serangan penapisan citra yang diujikan pada bagian ini adalah: *median filter*, *Gaussian low pass filtering (LPF)*, dan *mean filter*. Dalam aplikasi peningkatan citra umum, *median filter* sering digunakan untuk proses pengurangan *noise*. Pada dasarnya, *median filter* memodifikasi nilai piksel tengah dari *window* dengan nilai tengah dari nilai piksel yang diurutkan. Skema yang diusulkan diuji terhadap serangan *median filter* dengan ukuran *window* [3×3]. Logo watermark yang dipulihkan saat *median filter* [3×3] ditampilkan pada Gambar 6(h). Nilai NC dan citra watermark yang dihasilkan mengkonfirmasi kemantapan skema ini terhadap serangan *median filter*.

Operasi penapisan citra *lowpass* digunakan untuk menghilangkan *noise* frekuensi tinggi dari sinyal. Untuk membuktikan kekokohan dari teknik yang diusulkan terhadap LPF, serangan *Gaussian LPF* dengan parameter ukuran [3×3] diterapkan pada citra uji. Logo watermark restorasi yang dimodifikasi di bawah serangan *Gaussian LPF* [2×2] disajikan pada Gambar 6(i). Nilai NC untuk serangan *Gaussian LPF* mendekati 1 berarti bahwa metode yang diusulkan ini tahan dari serangan *Gaussian LPF*.

*Mean filtering* atau *average filtering* adalah salah satu serangan teknik peningkatan kualitas citra yang terkenal serta salah satu serangan *denoising*. *Mean filtering* diterapkan untuk menggantikan setiap sampel citra yang diberi watermark dengan nilai rata-rata dari kumpulan piksel tetangga  $W \times W$  atau ukuran jendela  $W$ . Skema ini diverifikasi terhadap serangan

*mean filtering*, ditunjukkan pada Gambar 6(j). Nilai NC dari *recovery* data watermark yang mendekati 1 menunjukkan bahwa skema yang diusulkan tahan terhadap serangan *mean filtering*.

4) Serangan Geometris

Jenis serangan geometris yang diujikan pada bagian ini antara lain: pencerminan (*flipping*), rotasi/ pemutaran (*rotation*), mengubah ukuran (*resizing*), dan pemotongan (*cropping*). Citra watermark restorasi yang dimanipulasi oleh serangan *flipping*, rotasi 45°, *resizing* dengan perbesaran dua kali, dan pemotongan sebesar 40% pada posisi kiri atas, ditampilkan pada Gambar 6(k-n). Nilai NC dari restorasi watermark di atas 0,9 menunjukkan bahwa skema yang diusulkan tahan terhadap serangan *flipping*, *rotation*, *resizing*, dan *cropping*.

5) Serangan Pengolahan Sinyal Lainnya

Jenis serangan pengolahan sinyal lainnya yang diujikan pada bagian ini adalah: *motion blur*, penajaman citra (*image sharpening*), dan *histogram equalization*. *Motion blur* adalah salah satu contoh penerapan LPF pada citra yang bertujuan untuk menghilangkan *noise* dari suatu citra sementara membiarkan sebagian besar citra tetap utuh. *Motion blur* sangat umum digunakan sebelum citra mengalami pemrosesan lain seperti deteksi tepi. *Image Sharpening* adalah metode yang mampu memberikan penekanan tekstur dan meningkatkan fokus citra. *Histogram equalization* adalah teknik pemrosesan yang digunakan untuk meningkatkan kontras pada citra. Logo watermark restorasi yang dimodifikasi di bawah serangan *motion blur*, penajaman citra, dan *histogram equalization*. disajikan pada Gambar 6(o-q). Nilai NC dari restorasi watermark di atas 0,9 menunjukkan bahwa skema yang diusulkan tahan terhadap serangan *motion blur*, penajaman citra, dan *histogram equalization*.



Gambar 6. Hasil restorasi watermark terhadap serangan, (a) tanpa serangan, (b-d) kompresi QF=10, 20, 30, (e) *salt&pepper noise*, (f) *speckle noise*, (g) *Gaussian noise*, (h) *median filter*, (i) *Gaussian LPF*, (j) *mean filter*, (k) *flipping*, (l) *rotation*, (m) *resizing*, (n) *cropping*, (o) *motion blur*, (p) penajaman citra, dan (q) *histogram equalization*

TABEL V. PERBANDINGAN NILAI NC DENGAN METODE SEBELUMNYA

No.	Jenis Serangan	DWT-DCT-SVD [6]	RDWT-DCT [8]	Penelitian ini
1.	Tanpa Serangan	1	1	1
2.	<i>Gaussian Noise</i> (0,003)	-	0,8458	<b>0,9070</b>
3.	<i>Median Filter</i> (3×3)	<b>0,9995</b>	0,7774	0,9651
4.	<i>Speckle Noise</i> (0,01)	<b>0,9998</b>	0,7402	0,9586
5.	<i>Speckle Noise</i> (0,03)	<b>0,9998</b>	-	0,9084
6.	<i>Speckle Noise</i> (0,005)	-	0,7878	<b>0,9925</b>
7.	<i>Salt &amp; Pepper Noise</i> (0,01)	<b>0,9998</b>	0,8531	0,9449
8.	<i>Salt &amp; Pepper Noise</i> (0,03)	<b>0,9998</b>	-	0,8379
9.	<i>Salt &amp; Pepper Noise</i> (0,001)	-	0,9663	<b>0,9717</b>
10.	<i>Histogram Equalization</i>	-	0,9588	<b>0,9615</b>
11.	Kompresi JPEG (40)	-	0,9899	<b>0,9972</b>
12.	Kompresi JPEG (50)	-	0,9909	<b>0,9985</b>
13.	Kompresi JPEG (60)	-	0,9922	<b>0,9988</b>

Skema *watermarking* berbasis RDWT dan *Arnold transform* pada citra medis telah diuji menggunakan beberapa serangan yang bertujuan untuk mengukur ketahanan skema *watermarking* yang diusulkan. Perbandingan nilai NC terhadap serangan dengan metode sebelumnya dapat dilihat pada Tabel V. *Watermarking* dapat dikatakan kuat atau *robust* apabila nilai NC lebih dari 0,7 pada berbagai serangan. Berdasarkan hasil pengujian, skema *watermarking* yang diusulkan pada penelitian ini memperoleh nilai NC lebih dari 0,9. Oleh karena itu, skema *watermarking* yang diusulkan ini dapat dikatakan *robust* terhadap berbagai serangan, memiliki kapasitas yang tinggi, dan memberikan keamanan yang ekstra pada watermark. Teknik *watermarking* citra medis yang diusulkan ini mengeksplorasi properti yang menonjol dari RDWT, DCT, dan SVD. Kemudian, sebelum disisipkan ke citra medis *host*, watermark diacak oleh *Arnold transform* untuk menjamin keamanan. RDWT bersifat *invariant* dan tanpa proses *downsampling*, sehingga informasi yang berpotensi berharga tidak dihapus untuk mereproduksi citra. DCT memiliki pemadatan energi yang sangat baik pada citra. Kemudian, teknik penyisipan dengan memanfaatkan nilai singular dari *subband* LH memberikan *imperceptibility* dan ketahanan yang lebih baik.

#### IV. PENUTUP

Metode *watermarking* citra medis berbasis RDWT, DCT, dan *Arnold transform* yang diusulkan dalam penelitian ini telah berhasil memberikan *imperceptibility*, ketahanan, dan kapasitas yang tinggi. Pengujian pada empat jenis citra medis, yaitu MRI, X-Ray, CT, dan US, serta watermark berupa logo yang berukuran sama menghasilkan rerata nilai PSNR sebesar 65,67 dB, SSIM 1, BER 0, dan NC 1. Hasil tersebut menunjukkan bahwa skema *watermarking* yang diusulkan memberikan autentikasi, *imperceptibility*, dan keamanan yang tinggi pada citra medis. *Subband* LH dari RDWT dan *subband* FH dari DCT dipilih untuk menjaga keseimbangan antara *imperceptibility* dan ketahanan. Watermark diacak menggunakan *Arnold transform* sebelum disematkan ke dalam citra *host* untuk menjamin keamanan. Nilai singular dari citra dengan watermark diperoleh dari modifikasi nilai singular citra *host* dan watermark. Pada saat citra dengan watermark dimodifikasi dan diberikan serangan, skema *watermarking* yang diusulkan mampu menghasilkan nilai NC mendekati 1. Dengan demikian, skema usulan tahan terhadap serangan kompresi JPEG, penambahan *noise* (*Salt & Pepper*, *Speckle*, dan *Gaussian Noise*), serangan penapisan citra (*Median Filter*, *Mean Filter*, dan *Gaussian LPF*), serangan geometris (*flipping*, *rotation*, *resizing*, dan *cropping*), dan serangan pemrosesan sinyal lainnya (*motion blur*, penajaman citra, dan *histogram equalization*). Penelitian mendatang dapat dilakukan teknik *watermarking* secara *blind*, menerapkan skema pada citra warna, dan watermark berupa teks.

#### REFERENSI

- [1] A. Sharma, A. K. Singh, and S. P. Ghrra, "Robust and Secure Multiple Watermarking for Medical Images," *Wirel. Pers. Commun.*, vol. 92, no. 4, pp. 1611–1624, 2017, doi: 10.1007/s11277-016-3625-x.
- [2] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, "An efficient medical image watermarking scheme based on FDCuT–DCT," *Eng. Sci. Technol. an Int. J.*, vol. 20, no. 4, pp. 1366–1379, 2017, doi: 10.1016/j.jestch.2017.06.001.
- [3] A. F. Qasim, F. Meziene, and R. Aspin, "Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review," *Comput. Sci. Rev.*, vol. 27, pp. 45–60, 2018, doi: 10.1016/j.cosrev.2017.11.003.
- [4] S. Kumar and R. K. Jha, "FD-based detector for medical image watermarking," 2019, doi: 10.1049/iet-ipc.2018.5485.
- [5] P. Khare and V. K. Srivastava, "A Secured and Robust Medical Image Watermarking Approach for Protection Integrity of Medical Images," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 2, p. e3918, 2021.
- [6] I. Assini, A. Badri, K. S. A. Sahel, and A. Baghdad, "A robust hybrid watermarking technique for securing medical image," *Int. J. Intell. Eng. Syst.*, vol. 11, no. 3, pp. 169–176, 2018, doi: 10.22266/IJIES2018.0630.18.
- [7] M. Hamidi, M. El Haziti, H. Cherifi, and M. El Hassouni, "Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform," *Multimed. Tools Appl.*, vol. 77, no. 20, pp. 27181–27214, 2018, doi: 10.1007/s11042-018-5913-9.
- [8] S. Roy and A. K. Pal, "A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling," *Multimed. Tools Appl.*, vol. 76, no. 3, pp. 3577–3616, 2017, doi: 10.1007/s11042-016-3902-4.
- [9] X. Bing Kang, F. Zhao, G. Feng Lin, and Y. Jun Chen, "A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength," *Multimed. Tools Appl.*, vol. 77, no. 11, pp. 13197–13224, 2018, doi: 10.1007/s11042-017-4941-1.
- [10] R. Thanki, A. Kothari, and D. Trivedi, "Hybrid and blind watermarking scheme in DCuT – RDWT domain," *J. Inf. Secur. Appl.*, vol. 46, pp. 231–249, 2019, doi: 10.1016/j.jisa.2019.03.017.
- [11] F. Ernawan and M. N. Kabir, "A block-based RDWT-SVD image watermarking method using human visual system characteristics," *Vis. Comput.*, vol. 36, no. 1, pp. 19–37, 2020, doi: 10.1007/s00371-018-1567-x.
- [12] W. H. Alshoura, Z. Zainol, J. Sen Teh, and M. Alawida, "A New Chaotic Image Watermarking Scheme Based on SVD and IWT," *IEEE Access*, vol. 8, pp. 43391–43406, 2020, doi: 10.1109/ACCESS.2020.2978186.
- [13] T. K. Araghi and A. A. Manaf, "An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD," *Futur. Gener. Comput. Syst.*, vol. 101, pp. 1223–1246, 2019, doi: 10.1016/j.future.2019.07.064.
- [14] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, "Watermarking Techniques used in Medical Images: a Survey," *J. Digit. Imaging*, vol. 27, no. 6, pp. 714–729, 2014, doi: 10.1007/s10278-014-9700-5.
- [15] D. Ariatmanto and F. Ernawan, "An improved robust image watermarking by using different embedding strengths," pp. 12041–12067, 2020.
- [16] 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.
- [17] N. M. Makbol, B. Ee, and T. H. Rasseem, "Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain," pp. 26845–26879, 2018.
- [18] S. Thakur, A. K. Singh, and S. P. Ghrra, "Multi-layer security of medical data through watermarking and chaotic encryption for telehealth applications," pp. 3457–3470, 2019.
- [19] F. N. Thakkar and V. K. Srivastava, "A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications," vol. 76, pp. 3669–3697, 2017, doi: 10.1007/s11042-016-3928-7.
- [20] J. Guo and H. Prasetyo, "Security analyses of the watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," *AEUE - Int. J. Electron. Commun.*, vol. 68, no. 9, pp. 816–834, 2014, doi: 10.1016/j.aeue.2014.03.008.
- [21] F. Ernawan, M. N. Kabir, and A. A. Scrambling, "A Blind Watermarking Technique using Redundant Wavelet Transform for Copyright Protection," 2018 *IEEE 14th Int. Colloq. Signal Process. Its Appl.*, no. March, pp. 221–226, 2018, doi: 10.1109/CSPA.2018.8368716.
- [22] A. Menendez-ortiz, C. Feregrino-uribe, and J. J. Garcia-herandez, "A Survey on Reversible Watermarking for Multimedia Content: A Robustness Overview," *IEEE Access*, vol. 7, pp. 132662–132681, 2019, doi: 10.1109/ACCESS.2019.2940972.
- [23] N. S. Utami, L. Novamizanti, S. Saidah, and I. N. A. Ramatryana, "SVD on a Robust Medical Image Watermarking based on SURF and DCT," in 2021 *IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, 2021, pp. 32–38.
- [24] S. M. Mousavi and A. Naghsh, "A robust medical image watermarking against salt and pepper noise for brain MRI images," pp. 10313–10342, 2017, doi: 10.1007/s11042-016-3622-9.
- [25] P. Apama, P. Venkata, and V. Kishore, "Biometric-based efficient medical image watermarking in E-healthcare application," vol. 13, pp. 421–428, 2019, doi: 10.1049/iet-ipc.2018.5288.