Building of Informatics, Technology and Science (BITS)
Volume 8, No 1, June 2026 Page: 1−13
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v8i1.8967

Deteksi Manipulasi Citra Medis MRI Menggunakan Watermarking Least Significant Bit dengan Autentikasi SHA-256 dan ECDSA

Y Noven Dhimas Nugroho*, Wildanil Ghozi

Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Dian Nuswantoro, Semarang, Indonesia
Email: [1,*]111202214045@mhs.dinus.ac.id, [2]wildanil.ghozi@dsn.dinus.ac.id
Email Penulis Korespondensi: 111202214045@mhs.dinus.ac.id
Submitted: **17/12/2025**; Accepted: **17/04/2025**; Published**: 05/06/2026**

Abstrak−Keamanan citra medis menjadi aspek penting dalam menjaga integritas dan keaslian data, terutama pada proses transmisi dan penyimpanan digital yang rentan terhadap manipulasi. Perubahan kecil berdampak pada kesalahan diagnosis, sehingga diperlukan metode perlindungan tanpa mengganggu kualitas visual. Namun, penelitian terdahulu masih menghadapi *trade-off* antara kompleksitas sistem, efisiensi komputasi, dan kemampuan deteksi manipulasi. Penelitian ini bertujuan mengembangkan metode *watermarking* citra medis yang mampu mendeteksi perubahan pada area diagnostik secara efisien dengan distorsi minimal. Metode yang diusulkan mengintegrasikan segmentasi *Region of Interest* (ROI) otomatis berbasis *Otsu thresholding*, penyisipan *watermark* menggunakan 1-LSB pada *Region of Non-Interest* (RONI), serta autentikasi berbasis SHA-256 dan tanda tangan digital ECDSA. Kontribusi utama penelitian ini adalah penggabungan segmentasi ROI otomatis, *watermarking* berbasis 1-LSB, serta autentikasi kriptografi dalam satu kerangka kerja efisien untuk menjaga integritas citra tanpa mengorbankan kualitas visual. Hasil pengujian menunjukkan metode mampu mempertahankan kualitas citra dengan baik, dengan PSNR rata-rata sebesar 75,04 dB, MSE rendah, dan SSIM tertinggi 0,9999975. Kualitas ini dipengaruhi oleh penggunaan *payload* kecil (99 *byte*) yang hanya memodifikasi 1,21% piksel pada RONI. Dari sisi efisiensi, menunjukkan komputasi yang relatif cepat dengan waktu rata-rata *embedding* dan ekstraksi masing-masing 0,14 detik dan 0,095 detik pada citra 256×256 piksel dengan perangkat uji AMD Ryzen 5 5600H dan RAM 16 GB. Sistem mampu mendeteksi manipulasi ROI, mengenali kerusakan *payload*, dan tetap valid pada perubahan RONI, namun masih terbatas terhadap manipulasi besar akibat sifat *fragile* LSB.

Kata Kunci: Watermarking LSB; ECDSA; Integritas Citra Medis; Deteksi Manipulasi; Region of Interest (ROI); SHA-256

Abstract−Medical image security is a crucial aspect of maintaining the integrity and authenticity of diagnostic data, particularly during digital transmission and storage processes that are vulnerable to manipulation. Minor modifications to pixels can lead to misdiagnosis; thus, protection methods are required to verify integrity without compromising visual quality. However, previous studies still face a trade-off between system complexity, computational efficiency, and tamper detection capabilities. This research aims to develop a medical image watermarking method capable of efficiently detecting changes in diagnostic areas with minimal distortion. The proposed method integrates automated Region of Interest (ROI) segmentation based on Otsu thresholding, 1-LSB watermark embedding in the Region of Non-Interest (RONI), and authentication based on SHA-256 and ECDSA digital signatures. The primary contribution of this study is an integrated framework that combines automated segmentation and cryptographic authentication to maintain image integrity without sacrificing clinical information. Experimental results demonstrate that the method maintains high image quality, with an average PSNR of 75.04 dB, low MSE, and the highest SSIM of 0.9999975. This performance is achieved through a small payload (99 bytes) that modifies only 1.21% of pixels in the RONI. In terms of efficiency, the method exhibits relatively fast computational performance with average embedding and extraction times of 0.14 seconds and 0.095 seconds, respectively, on 256×256 pixel images using an AMD Ryzen 5 5600H and 16 GB RAM. The system is capable of detecting ROI manipulation, identifying global payload damage, and remains valid under RONI changes, although it remains limited against large-scale manipulation due to the fragile nature of the LSB technique.

Keywords: LSB Watermarking; ECDSA; Medical Image Integrity; Tamper Detection; Region of Interest (ROI); SHA-256

1. PENDAHULUAN

Pencitraan medis merupakan teknologi yang digunakan untuk menghasilkan representasi visual dari bagian tubuh manusia melalui perangkat seperti CT-scan, MRI, dan PET-scan. Teknologi ini telah menjadi pilar utama dalam sistem pendukung keputusan klinis yang memungkinkan deteksi penyakit pada tahap awal secara *non-invasif*. Keakuratan representasi visual dari anatomi tubuh manusia ini menjadi sangat krusial karena kesalahan interpretasi sekecil apa pun dapat berakibat fatal pada perencanaan pengobatan pasien [1]. Namun, seiring dengan masifnya digitalisasi dan adopsi sistem *e-health*, rumah sakit kini memproduksi data citra dalam skala besar yang menuntut efisiensi tinggi dalam penyimpanan dan transmisi. Tantangan juga muncul ketika citra medis harus dikirimkan melalui jaringan publik yang tidak aman, di mana risiko intersepsi oleh pihak yang tidak berwenang menjadi ancaman nyata terhadap privasi pasien [2]. Selain masalah privasi, kerentanan citra medis terhadap manipulasi ilegal sering kali tidak terdeteksi secara visual, namun secara drastis dapat mengubah nilai diagnostik. Modifikasi piksel selama proses transmisi dapat merusak integritas dan keaslian data, yang secara langsung berpotensi menyebabkan kesalahan diagnosis dan membahayakan keselamatan pasien [3].

Berbagai pendekatan telah banyak dipelajari, seperti kriptografi, steganografi, dan teknik *watermarking*. Ketiga pendekatan ini bertujuan untuk memastikan kerahasiaan, integritas, dan autentikasi citra medis [4]. *Watermarking* banyak diterapkan pada citra medis untuk penyisipan informasi ke dalam citra tanpa mengganggu kualitas visual, sehingga dapat dimanfaatkan untuk autentikasi sumber dan deteksi manipulasi [5]. Citra medis memiliki dua area utama, yakni *Region of Interest* (ROI) dan *Region of Non-Interest* (RONI). ROI merupakan bagian yang mengandung informasi diagnostik penting dan harus tetap utuh, sedangkan RONI dapat dimanfaatkan untuk

Building of Informatics, Technology and Science (BITS)
Volume 8, No 1, June 2026 Page: 1−13
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v8i1.8967

penyisipan *watermark* tanpa memengaruhi hasil analisis [6]. Oleh karena itu, penyisipan *watermark* hanya dapat dilakukan pada wilayah RONI agar tidak mengganggu akurasi hasil analisis medis. Selain itu, citra medis harus menjamin keaslian dan integritas sejak penyimpanan, transmisi, hingga penggunaan kembali untuk keperluan medis. Citra yang dimodifikasi tanpa izin dapat mengubah informasi penting dan menurunkan kepercayaan terhadap sistem medis digital [7].

Sejumlah penelitian telah dilakukan untuk meningkatkan keamanan citra medis. Segmentasi berbasis *thresholding* memiliki performa baik dalam memisahkan struktur penting pada citra MRI sehingga efektif digunakan untuk identifikasi ROI secara otomatis, Namun masih menghadapi tantangan pada kompleksitas citra medis seperti noise dan variasi intensitas [8]. Penelitian lain mengusulkan penggunaan algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) pada citra medis dan menghasilkan nilai PSNR lebih tinggi serta waktu proses enkripsi–dekripsi lebih cepat dibandingkan teknik kriptografi lainnya [9]. ECDSA juga dikenal memiliki sensitivitas tinggi terhadap perubahan data sehingga efektif dalam menjaga integritas citra [10]. Sementara itu, metode *Least Significant Bit* (LSB) merupakan salah satu teknik *watermarking* yang memiliki kompleksitas komputasi rendah dan kemampuan mempertahankan kualitas visual citra dengan nilai PSNR lebih baik, Namun memiliki kelemahan berupa rendahnya ketahanan terhadap manipulasi signifikan [11].

Selain itu, sejumlah penelitian lebih spesifik yang berkontribusi dalam mengembangkan teknik *watermarking* untuk keamanan dan autentikasi citra medis. R. Ch *et al.* [12] mengusulkan teknik *watermarking* medis berbasis ECDSA, SHA-256, IWT–DCT pada citra otak. Hasil menunjukkan kualitas citra tetap tinggi setelah proses *embedding*, dengan nilai PSNR sebesar 68,67 dB, MSE 0,96, dan SSIM 0,98, serta mampu mendeteksi *tampering* melalui perubahan *hash* dan kegagalan verifikasi tanda tangan digital, namun memiliki kompleksitas komputasi yang tinggi dan belum optimal dalam efisiensi *payload*. Ravichandran *et al.* [13] mengusulkan metode ROI *based watermarking* menggunakan *Integer Wavelet Transform* (IWT), *chaotic embedding*, dan SHA-256 untuk mendeteksi serta memulihkan bagian ROI yang dimanipulasi. Hasil penelitian menunjukkan tingkat deteksi tinggi dengan MSE nol, yang menandakan kemampuan pemulihan tanpa kehilangan data, Tetapi metode ini memiliki keterbatasan pada ketergantungan terhadap *recovery* bit berukuran besar dan proses *embedding* yang kompleks.

Selanjutnya, Singh *et al.* [14] mengembangkan skema *region-based hybrid watermarking* untuk sistem *Internet of Medical Things (*IoMT*)* dengan menggabungkan *adaptive* LSB pada ROI dan DWT–SVD pada RONI. Pendekatan ini memperkuat keamanan dan ketahanan terhadap berbagai serangan seperti rotasi, filter, serta *salt & pepper noise* dengan nilai PSNR di atas 45 dB. Metode ini masih memiliki ketergantungan pada segmentasi ROI secara manual. Sementara itu, Alveda *et al.* [15] menerapkan metode LSB untuk autentikasi citra medis berbasis domain spasial, metode ini terbukti efektif menjaga kualitas visual citra dengan PSNR tinggi serta memiliki ketahanan terhadap berbagai serangan *noise* seperti *Gaussian, Speckle*, dan *Salt & Pepper*, Namun belum dilengkapi mekanisme kriptografi yang kuat. Ernawan *et al.* [16] Metode yang diusulkan menggunakan pendekatan autentikasi tiga lapis, yang meliputi *watermarking*, enkripsi, dan autentikasi berbasis tanda tangan dengan menggunakan *spiral block mapping* untuk pembuktian keaslian citra medis. Hasil penelitian menunjukkan akurasi deteksi tamper mencapai 93% dengan nilai PSNR sekitar 51 dB dan SSIM 0.994, serta ketahanan tinggi terhadap berbagai serangan. Skema ini masih memiliki keterbatasan dalam menyeimbangkan secara optimal antara kapasitas penyisipan, dan efisiensi komputasi dari algoritma pemetaan spiralnya.

Berbagai penelitian terdahulu menunjukkan bahwa skema keamanan citra medis sering kali menghadapi *trade-off* antara efisiensi komputasi dan ketahanan (*robustness*) terhadap serangan, atau memiliki deteksi yang presisi namun bergantung pada segmentasi manual dan proses *embedding* yang kompleks. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan metode *watermarking* citra medis yang berfokus pada sensitivitas deteksi manipulasi dan efisiensi proses tanpa mengintervensi area diagnostik. Metode yang diusulkan mengintegrasikan segmentasi ROI otomatis berbasis *Otsu thresholding* yang distabilkan dengan pendekatan *MSB-only*, penyisipan *watermark* menggunakan teknik 1-LSB pada wilayah *Region of Non-Interest* (RONI), serta mekanisme autentikasi berbasis *hashing* SHA-256 dan tanda tangan digital ECDSA. Kontribusi utama penelitian ini terletak pada perancangan kerangka kerja terintegrasi yang efisien dengan menggabungkan segmentasi otomatis dan teknik *watermarking* dengan *payload* kecil serta autentikasi kriptografi untuk verifikasi integritas. Pendekatan ini dirancang untuk menawarkan alternatif perlindungan data medis yang ringan secara komputasi namun tetap memiliki sensitivitas terhadap perubahan data sekecil satu bit, sehingga sesuai untuk kebutuhan transmisi medis yang mengutamakan kecepatan dan kualitas visual citra.

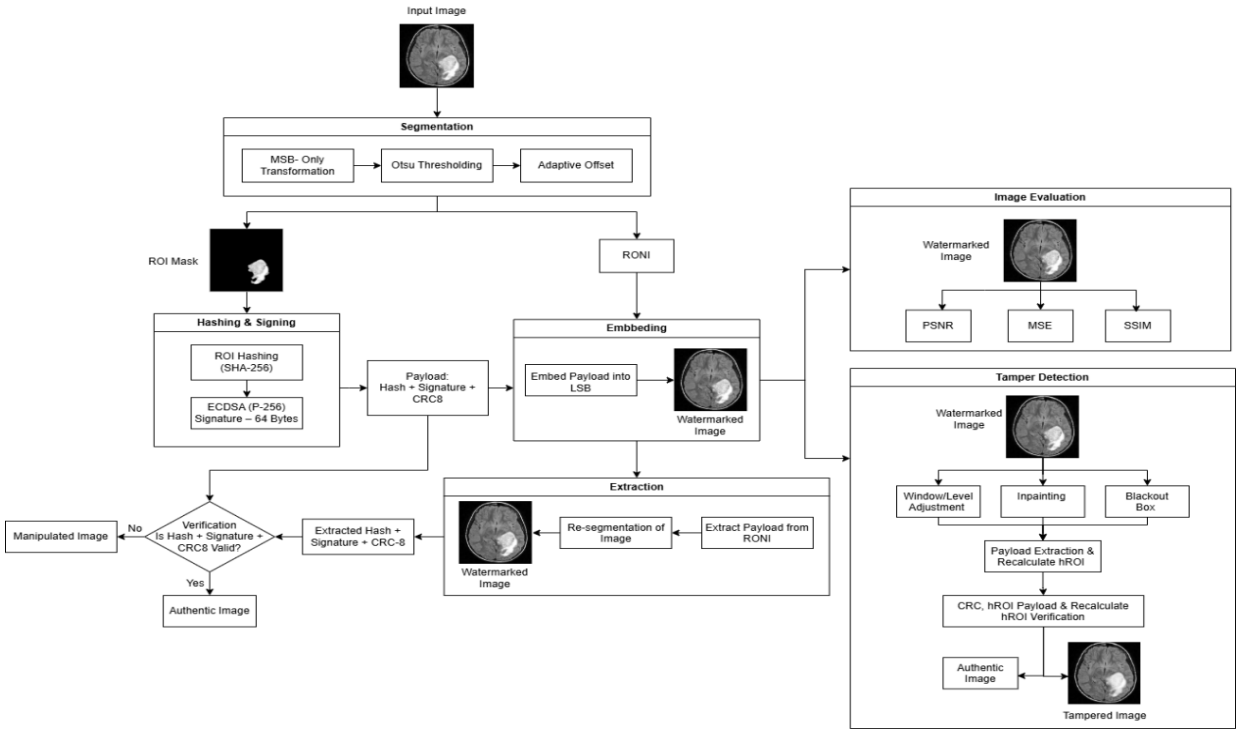
2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Penelitian ini dilakukan melalui serangkaian tahapan sistematis yang dimulai dengan segmentasi citra untuk memisahkan *Region of Interest* (ROI) dan *Region of Non-Interest* (RONI). Selanjutnya, ROI di-*hash* menggunakan SHA-256 dan ditandatangani secara digital dengan ECDSA untuk membentuk *payload*, yang kemudian disisipkan ke dalam RONI menggunakan teknik *Least Significant Bit* (LSB) sehingga dihasilkan citra *watermark*. Kualitas citra hasil penyisipan dievaluasi menggunakan PSNR, MSE, dan SSIM. Pada tahap ekstraksi dan verifikasi, *payload* diambil kembali dari RONI, ROI disegmentasi ulang, serta dilakukan pemeriksaan kecocokan *hash*, tanda tangan

Building of Informatics, Technology and Science (BITS)
Volume 8, No 1, June 2026 Page: 1−13
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v8i1.8967

digital, dan CRC-8 untuk menentukan keaslian citra. Selain itu, metode yang diusulkan diuji menggunakan beberapa skenario manipulasi, yaitu *window/level adjustment* pada keseluruhan citra, *inpainting* pada area ROI, dan *blackout box* pada area RONI. Seluruh proses eksperimen dilakukan pada perangkat dengan spesifikasi prosesor AMD Ryzen 5 5600H (3.30 GHz), RAM 16 GB, dan sistem operasi 64-bit. Pengujian juga mencakup pengukuran waktu proses *embedding* dan ekstraksi untuk mengevaluasi efisiensi komputasi dari metode yang diusulkan. Alur keseluruhan tahapan penelitian ditunjukkan pada Gambar 1.



Gambar 1. Tahapan Penelitian

2.2 Pemuatan Citra

Citra yang digunakan pada penelitian ini adalah *Citra Magnetic Resonance Imaging* (MRI) otak berukuran 256 × 256 piksel dalam format *grayscale* (8-bit). Seluruh tahapan penelitian, mulai dari segmentasi hingga penyisipan *watermark*, dilakukan sepenuhnya pada domain satu kanal ini untuk menjaga konsistensi data.

2.3 Segmentasi ROI Berbasis Otsu Thresholding

Untuk memperoleh area ROI, penelitian ini menggunakan metode Otsu *thresholding*, yang bekerja dengan menentukan nilai ambang berdasarkan distribusi intensitas piksel. Metode ini dikenal efektif untuk pemisahan objek dan latar belakang pada berbagai jenis citra [17]. Dalam konteks citra medis, Otsu juga banyak digunakan karena mampu memilih ambang secara adaptif tanpa proses manual, sehingga dapat memisahkan ROI dan RONI secara konsisten [18].

a. Transformasi MSB-Only
   Citra ditransformasikan ke bentuk MSB-only dengan mengeliminasi LSB untuk menjaga stabilitas intensitas citra. Transformasi ini menghilangkan variasi kecil akibat perubahan LSB dari proses penyisipan *watermark*, sementara bit MSB tetap dipertahankan karena memuat informasi utama citra. Dalam metode *Otsu*, perubahan kecil pada intensitas dapat memengaruhi distribusi histogram dan menggeser nilai ambang, sehingga menyebabkan segmentasi ROI yang tidak konsisten. Dengan menggunakan MSB-only, distribusi intensitas menjadi lebih stabil sehingga nilai ambang tetap konsisten dan akurasi segmentasi ROI dapat dipertahankan [19].
b. Perhitungan Ambang Otsu
   Ambang optimal k^*diperoleh dengan memaksimalkan nilai varian antar-kelas berikut:

$$\sigma_B^2(k) = \frac{[\mu_T \cdot \omega(k) - \mu(k)]^2}{\omega(k)\,[1-\omega(k)]} \tag{1}$$

   Perhitungan varians antar-kelas pada metode Otsu digunakan untuk menentukan nilai ambang optimal dengan memaksimalkan pemisahan antara dua kelompok piksel. Nilai $\sigma_b^2(t)$ menyatakan seberapa baik piksel dapat dipisahkan menjadi dua kelompok, yaitu latar belakang dan objek. Besarnya varian antar-kelas dipengaruhi oleh probabilitas kumulatif kelas pertama $\omega(t)$, rata-rata kumulatif $\mu(t)$, dan rata-rata global citra μ_T. Semakin besar nilai varians antar-kelas yang diperoleh, maka semakin baik nilai ambang tersebut dalam memisahkan ROI dan RONI.

Building of Informatics, Technology and Science (BITS)
Volume 8, No 1, June 2026 Page: 1−13
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v8i1.8967

c. Adaptive Offset Thresholding
Nilai ambang awal yang diperoleh dari metode Otsu kemudian disesuaikan secara adaptif dengan menambahkan *offset* intensitas untuk mengakomodasi variasi kontras pada citra MRI. *Offset* yang digunakan dalam penelitian ini adalah $\Delta \in \{0, 10, 20, 30, 40, 60\}$, yang diterapkan secara bertahap pada ambang *Otsu*. Pemilihan nilai *offset* dilakukan secara otomatis berdasarkan proporsi area ROI terhadap ukuran citra harus berada dalam rentang 5%–15%. Berdasarkan hasil pra-penelitian dan observasi terhadap karakteristik citra MRI yang digunakan, ditetapkan ambang proporsi area ROI dalam rentang 5%–15%. Batasan ini diterapkan untuk memastikan bahwa proses segmentasi mampu mengisolasi struktur lesi atau jaringan otak secara tepat tanpa menyertakan latar belakang yang berlebihan. Setiap nilai *offset* diuji secara berurutan hingga diperoleh segmentasi yang memenuhi kriteria proporsi tersebut.

d. Pembentukan ROI dan RONI
Mask ROI yang diperoleh selanjutnya diperhalus menggunakan *closing* untuk menghaluskan batas objek dan penghapusan objek kecil untuk mengurangi *noise*. Area yang termasuk dalam ROI didefinisikan sebagai wilayah dengan informasi diagnostik penting, sedangkan RONI ditetapkan sebagai komplemen dari ROI. Wilayah RONI inilah yang digunakan sebagai lokasi penyisipan *watermark*, sehingga integritas dan kualitas visual ROI tetap terjaga.

2.4 Hashing ROI Menggunakan SHA-256

SHA-256 merupakan algoritma *message digest* berukuran tetap 256-bit yang memiliki keamanan kriptografi tinggi serta efisiensi komputasi yang baik, sehingga cocok diterapkan pada sistem citra medis yang membutuhkan perlindungan integritas data [20]. SHA-256 bersifat sangat sensitif terhadap perubahan input, satu perubahan kecil pada nilai piksel akan menghasilkan *hash* yang berbeda secara signifikan, sehingga efektif digunakan untuk autentikasi dan deteksi manipulasi citra digital [21].

Pada penelitian ini, *hashing* dilakukan hanya pada piksel ROI dengan representasi MSB-only untuk memastikan bahwa nilai *hash* tidak dipengaruhi oleh watermark yang disisipkan pada bit LSB. Nilai *hash* dihitung dengan:

$$H = SHA256(R) \tag{2}$$

Hash yang dihasilkan menjadi identitas unik ROI. Perubahan apa pun pada ROI akan menghasilkan *hash* yang berbeda, sehingga integritas citra dapat diverifikasi secara langsung.

2.5 Pembangkitan dan Penandatanganan ECDSA

Elliptic Curve Digital Signature Algorithm (ECDSA) adalah skema tanda tangan digital berbasis kurva eliptik yang menyediakan keamanan tinggi dengan ukuran kunci yang lebih kecil [22]. Proses ECDSA meliputi pembangkitan kunci, *hashing* pesan, penandatanganan menggunakan kunci privat, dan verifikasi menggunakan kunci publik untuk menjamin autentikasi dan integritas data [23]. Keamanan algoritma ini bergantung pada *Elliptic Curve Discrete Logarithm Problem* (ECDLP) yang sangat sulit diselesaikan secara komputasional, sehingga ECDSA mampu menghasilkan tanda tangan yang kecil, kuat, dan mudah diverifikasi pada berbagai sistem modern [24]. Dalam penelitian ini, ECDSA berfungsi untuk memastikan keaslian sumber data dengan menandatangani *hash* ROI, sehingga melindungi sistem dari potensi pemalsuan *payload*, seperti penggantian nilai *hash* ROI oleh pihak yang tidak berwenang.

Dalam proses ini, simbol e menyatakan *hash* pesan k merupakan bilangan acak sementara, d_A adalah kunci privat pengirim, Q_A adalah kunci publik, sedangkan r dan s merupakan komponen tanda tangan digital. Proses penandatanganan diawali dengan menghitung *hash* pesan dari ROI yang telah diproses menggunakan SHA-256. *Hash* pesan tersebut dinyatakan pada Persamaan (3):

$$e = HASH(m) \tag{3}$$

Nilai hash pada Persamaan (3) kemudian dikombinasikan dengan bilangan acak k untuk menghasilkan titik pada kurva eliptik melalui perkalian dengan titik generator G. Koordinat x_1 dari titik yang dihasilkan digunakan untuk membentuk komponen pertama tanda tangan digital sebagaimana ditunjukkan pada Persamaan (4):

$$(x_1, y_1) = kG, r = x_1 \bmod n \tag{4}$$

Setelah nilai r diperoleh, komponen kedua tanda tangan dihitung menggunakan *hash* pesan, kunci privat, dan bilangan acak sementara. Perhitungan tersebut dinyatakan pada Persamaan (5):

$$s = k^{-1}(e + rd_A) \bmod n \tag{5}$$

Pasangan (r, s) yang dihasilkan menjadi tanda tangan digital ECDSA dan selanjutnya disisipkan ke dalam *payload watermark*. Pada sisi penerima, validitas tanda tangan diperiksa menggunakan *hash* pesan dan kunci publik pengirim. Tahap awal verifikasi dilakukan dengan menghitung dua nilai bantu u_1 dan u_2 sebagaimana ditunjukkan pada Persamaan (6):

Building of Informatics, Technology and Science (BITS)
Volume 8, No 1, June 2026 Page: 1−13
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v8i1.8967

$$u_1 = es^{-1} mod n, u_2 = rs^{-1} mod n \quad (6)$$

Kedua nilai pada Persamaan (6) digunakan untuk membentuk kembali titik verifikasi pada kurva eliptik menggunakan titik generator G dan kunci publik Q_A. Tanda tangan dinyatakan valid apabila nilai r yang dihitung kembali identik dengan komponen tanda tangan yang diterima, sebagaimana ditunjukkan pada Persamaan (7):

$$r \equiv (u_1 G + u_2 Q_A)_x mod n \quad (7)$$

Dengan mekanisme ini, setiap perubahan pada ROI maupun pemalsuan *payload* akan menyebabkan verifikasi tanda tangan digital gagal.

2.6 Penyisipan Watermark Menggunakan LSB pada RONI

Teknik *Least Significant Bit* (LSB) merupakan metode *watermarking* dalam domain spasial yang menyisipkan informasi pada bit paling tidak signifikan dari piksel citra. Perubahan pada bit ini sangat kecil sehingga tidak menurunkan kualitas visual citra secara nyata [25]. Karakteristik dari teknik *watermarking Least Significant* Bit (LSB) adalah memiliki karakteristik sensitif terhadap modifikasi citra [26]. Oleh karena itu, pada metode ini digunakan *payload* dengan ukuran relatif kecil untuk mengurangi risiko kerusakan *payload* akibat manipulasi, sehingga masih memungkinkan untuk diekstrak pada kondisi tertentu.
Pada metode ini *payload* watermark terdiri dari:
a. 2 byte → panjang *payload*
b. 32 byte → *hash* ROI
c. 64 byte → *signature* ECDSA
d. 1 byte → CRC-8 untuk deteksi korupsi

Total *payload* yang dihasilkan adalah 99 *byte* atau setara dengan 792 bit, di mana setiap bit disisipkan ke dalam satu piksel pada area RONI. Dengan demikian, jumlah piksel yang mengalami modifikasi adalah 792 piksel, atau hanya sebesar 1,21% dari keseluruhan piksel citra (256 × 256 = 65.536 piksel). Proporsi modifikasi yang sangat kecil ini bertujuan untuk meminimalkan perubahan visual pada citra hasil *watermarking*. Penyisipan watermark dilakukan menggunakan teknik 1-LSB, yaitu hanya pada satu bit paling rendah dari setiap piksel. Pemilihan 1-LSB bertujuan untuk meminimalkan distorsi citra sekaligus mempertahankan sensitivitas terhadap perubahan. Penyisipan watermark dilakukan hanya pada piksel-piksel RONI agar ROI tetap bebas modifikasi. Bit *payload* dikonversi menjadi *bitstream*, lalu disisipkan ke bit paling rendah dari satu piksel pada area RONI menggunakan persamaan berikut:

$$I'[i] = (I[i] \,\&\, 0xFE) \mid b_i \quad (8)$$

Pada Persamaan (8), $I'[i]$ menyatakan nilai piksel setelah proses *embedding*, $I[i]$ merupakan nilai piksel asli pada area RONI, sedangkan b_i adalah bit *payload* ke-i. Operasi AND dengan nilai $0xFE$ digunakan untuk menghapus bit paling rendah dari piksel asli. Setelah itu, operasi OR digunakan untuk menggantikan bit tersebut dengan bit *payload* yang akan disisipkan. Melalui mekanisme ini, hanya satu bit pada setiap piksel yang mengalami perubahan, sehingga perbedaan intensitas maksimum yang terjadi hanya sebesar 1. Karena penyisipan dilakukan pada area RONI dan hanya memodifikasi bit LSB, struktur diagnostik pada ROI tetap terjaga dan perubahan visual pada citra menjadi sangat kecil.

2.7 Ekstraksi dan Verifikasi Tanda Tangan

Proses verifikasi pada sisi penerima dimulai dengan melakukan segmentasi ulang untuk memisahkan area ROI dan membentuk kembali area RONI. Langkah selanjutnya adalah melakukan ekstraksi bit *payload* yang tertanam pada bit terakhir (LSB) di wilayah RONI. Data yang berhasil diekstraksi kemudian dipisahkan ke dalam komponen-komponen penyusunnya, yang meliputi informasi panjang *payload*, nilai *hash* ROI asli, tanda tangan digital ECDSA, dan kode deteksi kesalahan CRC. Bersamaan dengan itu, dilakukan rekalkulasi *hash* pada area ROI dari citra *watermark* yang diterima menggunakan algoritma SHA-256. Tahap akhir adalah proses verifikasi integritas dan autentikasi, di mana nilai *hash* hasil rekalkulasi dibandingkan dengan *hash* hasil ekstraksi, serta validasi tanda tangan digital menggunakan kunci publik pengirim untuk memastikan keaslian sumber citra.

2.8 Uji Tampering

Uji *tampering* dilakukan untuk mengevaluasi kemampuan sistem dalam mendeteksi manipulasi pada citra medis yang telah disisipkan *watermark*. Proses pengujian dimulai dari pemuatan citra watermark, pemberian serangan manipulasi, kemudian dilakukan segmentasi ulang untuk memperoleh area *Region of Interest* (ROI) dan *Region of Non-Interest* (RONI) menggunakan metode yang sama seperti pada tahap *embedding*, yaitu transformasi MSB-only, Otsu *thresholding*, serta *offset thresholding*. Selanjutnya, *payload watermark* diekstraksi dari area RONI menggunakan teknik 1-LSB. *Payload* yang berhasil diekstraksi divalidasi menggunakan CRC-8 untuk memastikan integritas data. Jika *payload* valid, maka *hash* ROI yang tersimpan dibandingkan dengan *hash* ROI hasil rekalkulasi. Jika identik, maka ROI dinyatakan tidak berubah, namun jika berbeda, ROI dinyatakan telah dimanipulasi. Sebaliknya, apabila *payload* tidak dapat diekstraksi akibat kerusakan besar pada piksel RONI, sistem langsung mengklasifikasikan citra sebagai telah dimanipulasi tanpa melakukan verifikasi ROI. Untuk mengevaluasi performa sistem, tiga skenario manipulasi diterapkan sebagai berikut:

Building of Informatics, Technology and Science (BITS)
Volume 8, No 1, June 2026 Page: 1−13
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v8i1.8967

2.8.1 Window/Level Adjustment (WL)

Window/Level Adjustment (WL) merupakan proses yang mengubah intensitas piksel untuk menyesuaikan kontras dan kecerahan. *Window-leveling* memodifikasi distribusi *grayscale* citra sehingga nilai piksel berubah [27]. Manipulasi ini diterapkan secara *global* pada seluruh citra, sehingga perubahan tidak hanya terjadi pada RONI, tetapi juga memengaruhi ROI.

2.8.2 Inpainting pada Area Lesi

Tujuan utama *inpainting* adalah mengisi area yang hilang pada citra dengan konten yang tampak realistis dan konsisten dengan struktur sekitarnya. Teknik ini sering digunakan dalam proses penyuntingan citra, misalnya untuk menghapus objek yang tidak diinginkan dengan menghasilkan pengisian [28]. Manipulasi ini dilakukan secara langsung pada area ROI, sehingga perubahan nilai piksel akan memengaruhi hasil perhitungan *hash* ROI dan menyebabkan ketidaksesuaian pada proses verifikasi.

2.8.3 Blackout Box

Manipulasi pada area RONI dilakukan dengan menutup sebagian wilayah menggunakan kotak hitam tanpa memengaruhi area ROI. Skenario ini bertujuan untuk menguji ketahanan sistem dalam memverifikasi integritas area diagnostik (ROI) ketika area non-diagnostik mengalami modifikasi. Secara teknis, jika manipulasi kotak hitam tidak mengenai lokasi piksel yang membawa *payload watermark*, maka *payload* tetap dapat diekstraksi secara utuh. Dalam kondisi tersebut, nilai *hash* ROI hasil rekalkulasi akan tetap identik dengan *hash* yang tersimpan di dalam *payload*, sehingga integritas area ROI tetap dinyatakan valid meskipun sebagian area RONI telah berubah. Namun, apabila manipulasi tersebut merusak piksel yang mengandung bit *watermark*, sistem akan mengklasifikasikan citra sebagai telah dimanipulasi.

2.9 Evaluasi PSNR, SSIM, dan MSE

Ketiga metrik ini merupakan *full-reference metrics* yang digunakan untuk mengevaluasi kualitas citra dengan membandingkan citra hasil watermarking terhadap citra asli sebagai referensi, sehingga tingkat distorsi akibat proses penyisipan dapat diukur secara kuantitatif. PSNR dan MSE menghitung perbedaan piksel secara langsung, namun kurang merepresentasikan persepsi visual [29]. SSIM lebih sesuai untuk menilai kualitas citra karena mempertimbangkan struktur, luminansi, dan kontras [30]. Pada citra medis, PSNR dan MSE memberikan gambaran *error* global, sedangkan SSIM lebih sensitif terhadap perubahan struktur diagnostik [31].

a. Mean Squared Error (MSE)
   Mengukur rata-rata error kuadrat antara citra asli dan citra *watermark*.

$$MSE = \frac{\sum_{i=1}^{M}\sum_{i=1}^{N}[A(i,j)-B(i,j)]^2}{\text{M.N}} \tag{9}$$

   Pada Persamaan (9), $A(i,j)$ dan $B(i,j)$ masing-masing menyatakan nilai piksel citra asli dan citra *watermark*, sedangkan Mdan N menyatakan ukuran citra. Semakin kecil nilai MSE, semakin kecil perbedaan antara kedua citra.

b. Peak Signal-to-Noise Ratio (PSNR)
   PSNR menilai kualitas citra berdasarkan nilai MSE:

$$PSNR = 20.log_{10}\left(\frac{2^X-1}{\sqrt{MSE}}\right) \tag{10}$$

   Pada Persamaan (10), X menyatakan jumlah bit per piksel. Karena citra yang digunakan merupakan citra 8-bit, maka $X = 8$, sehingga nilai maksimum intensitas piksel adalah $2^8 - 1 = 255$. Nilai PSNR yang tinggi menunjukkan bahwa proses *watermarking* hanya menyebabkan perubahan yang sangat kecil pada citra.

c. Structural Similarity Index Measure (SSIM)
   Mengukur kemiripan struktur, luminansi, dan kontras antara dua citra.

$$SSIM(A,B) = \frac{(2\mu_A\mu_B+C_1)(2\sigma_{AB}+C_2)}{(\mu_A^2+\mu_B^2+C_1)(\sigma_A^2+\sigma_B^2+C_2)} \tag{11}$$

   Pada Persamaan (11), μ_A dan μ_B menyatakan rata-rata intensitas dari citra asli dan hasil *watermarking*. Simbol σ_A^2 dan σ_B^2 menyatakan variasi, sedangkan σ_{AB} menyatakan kovariansi kedua citra. Konstanta C_1 dan C_2 digunakan untuk menjaga kestabilan perhitungan. SSIM menilai apakah struktur citra tetap dipertahankan setelah proses *watermarking*. Nilai SSIM berada pada rentang 0 hingga 1. Semakin mendekati 1, semakin tinggi kemiripan struktur antara citra asli dan citra hasil *watermarking*.

3. HASIL DAN PEMBAHASAN

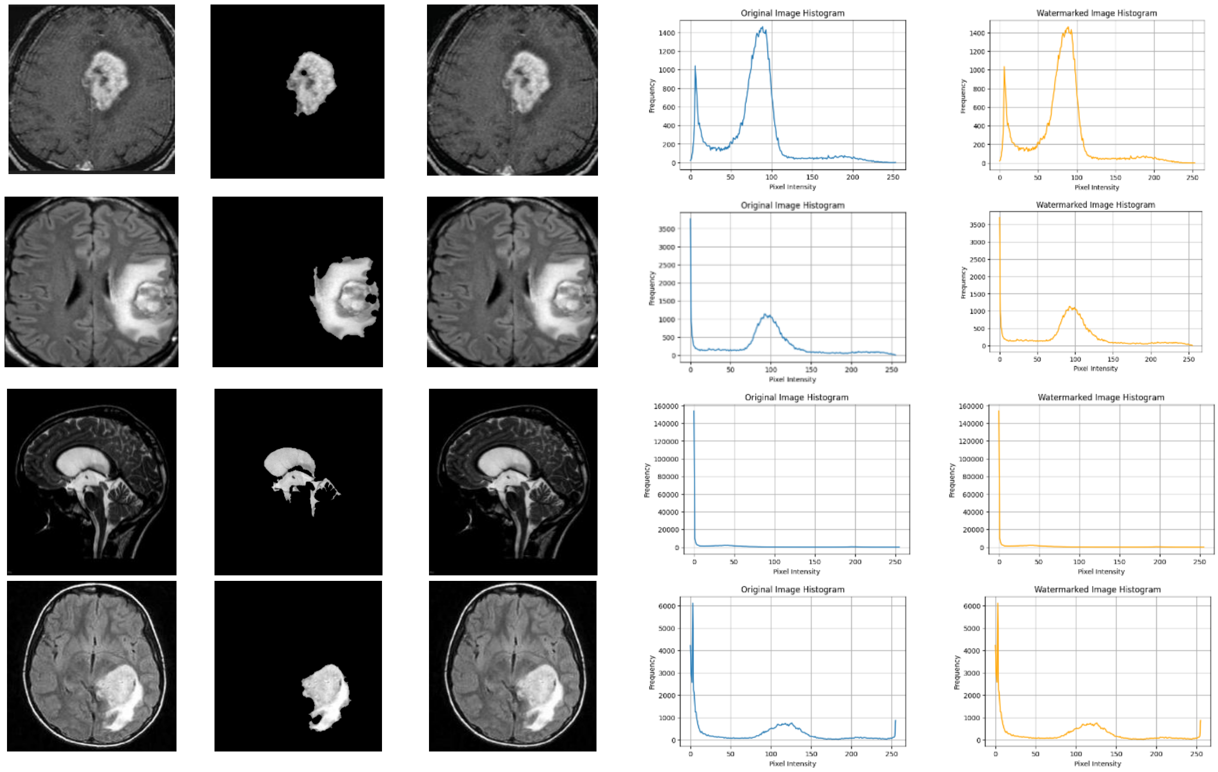
Bagian ini menyajikan hasil penerapan metode pada citra medis MRI yang meliputi segmentasi ROI, proses *watermarking*, autentikasi, serta evaluasi kualitas dan ketahanan sistem. Pembahasan mencakup hasil *segmentasi* dan

Building of Informatics, Technology and Science (BITS)
Volume 8, No 1, June 2026 Page: 1−13
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v8i1.8967

watermarking, *hashing* dan verifikasi tanda tangan digital, serta evaluasi kualitas citra dan efisiensi proses. Selain itu, dilakukan uji *tampering* untuk menganalisis respons sistem terhadap berbagai skenario manipulasi pada ROI, RONI, dan secara *global*. Seluruh pengujian dilakukan pada perangkat dengan spesifikasi AMD Ryzen 5 5600H dan memori 16 GB RAM sebagai representasi lingkungan implementasi. Dengan demikian, bagian ini bertujuan untuk memberikan analisis terukur terhadap kinerja metode yang diusulkan dalam mempertahankan kualitas citra medis.

Tabel 1. Hasil Segmentasi dan Watermarking

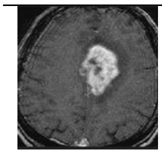
Citra Medis	ROI Mask	Watermark	Original Histogram	Watermark Histogram



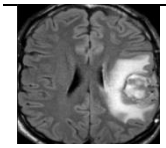
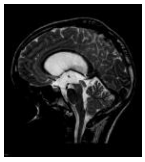
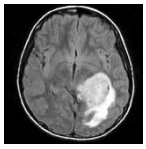
Tabel 1 menyajikan rangkaian hasil segmentasi ROI dan proses *watermarking* untuk empat citra medis MRI. Secara keseluruhan, metode segmentasi berbasis Otsu *Thresholding* terbukti mampu memisahkan area lesi pada seluruh citra uji, ditandai dengan terbentuknya ROI *mask* yang jelas pada area diagnostik penting. Hal ini menunjukkan bahwa pendekatan MSB, Otsu, *adaptive offset*, *closing* efektif dalam menstabilkan penentuan nilai ambang Otsu sehingga pemisahan area lesi (ROI) dan latar belakang (RONI) dapat dilakukan secara konsisten pada variasi kontras berbeda secara otomatis tanpa segmentasi manual. Proses *watermarking* menggunakan teknik *Least Significant Bit* (LSB) pada area RONI menghasilkan citra yang secara visual tetap mempertahankan struktur dan kualitas citra asli. Penyisipan yang dilakukan hanya pada RONI memastikan bahwa area ROI tidak mengalami perubahan, sehingga informasi diagnostik tetap terjaga.

Analisis histogram menunjukkan bahwa kurva distribusi intensitas piksel citra *watermarked* berhimpit secara presisi dengan citra asli. Perubahan nilai LSB pada 1,21% piksel tidak menyebabkan pergeseran distribusi yang teramati secara visual, yang mengonfirmasi bahwa karakteristik statistik citra tetap terjaga. Hasil ini menunjukkan bahwa metode yang diusulkan mampu melakukan segmentasi ROI secara konsisten serta menyisipkan *watermark* tanpa memengaruhi kualitas visual citra secara signifikan. Analisis menggunakan metrik PSNR, MSE, dan SSIM disajikan pada tabel 3 dan 4 untuk memberikan evaluasi yang lebih objektif terhadap kualitas citra hasil *watermarking*.

Tabel 2. Hashing dan Verifikasi Tanda Tangan Digital

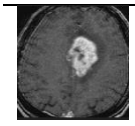
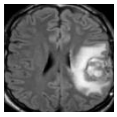
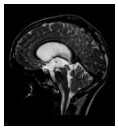
Citra Medis	*Hash* ROI Rekalkulasi	Signature	Hash ROI Ekstrak	Signature Ekstrak	Verifikasi
	47ece78423e96 ce53ef35527ef6 69ccbe86d187f0 6b643df43f9567 b37070288	c6b619fbd95c02ceb 8c8035b84bf43cfcd a5b50a401effcc48a 9fbae5cba65b03add ce4537bbef74828d 3d2e27d9a7211fb8 035f207c54ea4145 311ec88a4544	47ece78423e96 ce53ef35527ef6 69ccbe86d187f0 6b643df43f9567 b37070288	c6b619fbd95c02ceb 8c8035b84bf43cfcd a5b50a401effcc48a 9fbae5cba65b03add ce4537bbef74828d 3d2e27d9a7211fb8 035f207c54ea4145 311ec88a4544	Citra Otentik

Building of Informatics, Technology and Science (BITS)
Volume 8, No 1, June 2026 Page: 1−13
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v8i1.8967

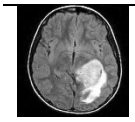
Citra Medis	*Hash* ROI Rekalkulasi	Signature	Hash ROI Ekstrak	Signature Ekstrak	Verifikasi
	ea3de7f01dde26b609f59c22947ecebe7bb4dc1e7f657b6ac0609d984162d81b	bf57bc29844150b5a29e7a70e32d4948e1aaf4c92a20ad76a90f94da48450d3aba44876eba1fd2da9b1f285b17514c6e6643cd923c538c4ae1c4b2d2bf5af8d4	ea3de7f01dde26b609f59c22947ecebe7bb4dc1e7f657b6ac0609d984162d81b	bf57bc29844150b5a29e7a70e32d4948e1aaf4c92a20ad76a90f94da48450d3aba44876eba1fd2da9b1f285b17514c6e6643cd923c538c4ae1c4b2d2bf5af8d4	Citra Otentik
	292eb0d5edf9c63bea0e07b547f509f8225b63b2e96f208dfabee93c670e5056	34fdaa6d22615f582e06c82087ae07099f1b041d03c5937f5b5ac73c2107a1c6e02a952016d6ad244cdaec98fb415f72e3482b53c9e2a167fd1edbb999adcd74	292eb0d5edf9c63bea0e07b547f509f8225b63b2e96f208dfabee93c670e5056	34fdaa6d22615f582e06c82087ae07099f1b041d03c5937f5b5ac73c2107a1c6e02a952016d6ad244cdaec98fb415f72e3482b53c9e2a167fd1edbb999adcd74	Citra Otentik
	e5381e0ecdbae6007d41786804382c80800e7f8c577343f9057e298a2a21764b	9b57341194ebb004b31cb711fe92b967e959701b7a376b215b9b2fbdaed8f4b49f70c75cf69304ba2f6b840842345024ef6c0bfa1bcba4683b071f16a186149e	e5381e0ecdbae6007d41786804382c80800e7f8c577343f9057e298a2a21764b	9b57341194ebb004b31cb711fe92b967e959701b7a376b215b9b2fbdaed8f4b49f70c75cf69304ba2f6b840842345024ef6c0bfa1bcba4683b071f16a186149e	Citra Otentik

Tabel 2 menyajikan hasil proses autentikasi yang mencakup pembangkitan *hash* ROI menggunakan SHA-256, penandatanganan digital ECDSA, serta ekstraksi *watermark* untuk verifikasi. Seluruh citra uji menunjukkan bahwa nilai hash ROI hasil ekstraksi identik dengan hash ROI hasil rekalkulasi pada sisi penerima. Hal ini membuktikan bahwa informasi diagnostik pada ROI tidak mengalami modifikasi selama proses *embedding* maupun ekstraksi kembali. Mengingat sifat SHA-256 yang sangat sensitif, di mana perubahan satu bit saja akan menghasilkan nilai *hash* yang berbeda secara signifikan, keberhasilan ini menegaskan bahwa metode yang diusulkan mampu menjaga integritas data ROI secara utuh. Selain itu, tanda tangan digital ECDSA yang diekstraksi terbukti valid saat diverifikasi terhadap *hash* ROI pada semua sampel. Validitas ini menunjukkan bahwa tanda tangan digital yang disisipkan sesuai dengan kunci publik pengirim, sekaligus mengonfirmasi keterhubungan antara identitas sumber dan integritas data ROI. Kestabilan ini mengindikasikan bahwa proses penyisipan 1-LSB pada wilayah RONI mampu membawa *payload* kriptografi sebesar 99 *byte* secara utuh tanpa kehilangan data. Kolom verifikasi menunjukkan status "Citra Otentik" untuk seluruh pengujian, yang menandakan keberhasilan sistem dalam menjalankan verifikasi pada kondisi tanpa gangguan. Hasil pada Tabel 2 merepresentasikan kinerja sistem dalam menjaga keaslian sumber dan integritas data sebelum dilakukan pengujian terhadap berbagai skenario manipulasi.

Tabel 3. Evaluasi Kualitas Citra dan Waktu Proses

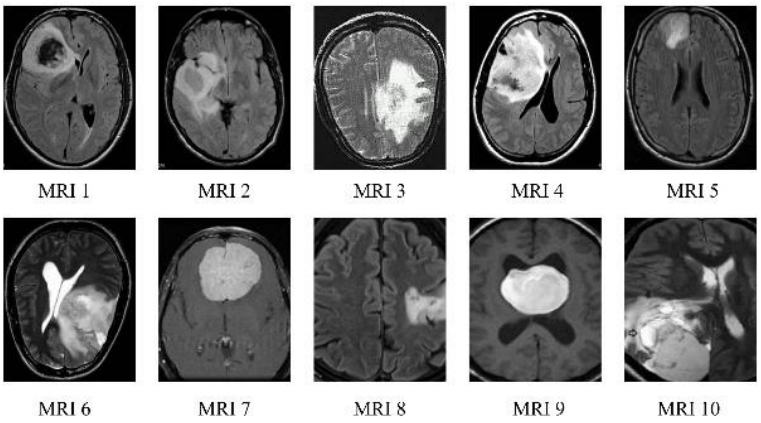
Citra Medis	PSNR	MSE	SSIM	Embedding Time	Extraction Time
	73.87 dB	0.002670	0.9999970461	0.088 s	0.061 s
	73.75 dB	0.002741	0.9999923241	0.134 s	0.058 s
	80.51 dB	0.000578	0.9999975797	0.195 s	0.142 s

Building of Informatics, Technology and Science (BITS)
Volume 8, No 1, June 2026 Page: 1−13
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v8i1.8967

Citra Medis	PSNR	MSE	SSIM	Embedding Time	Extraction Time
	74.41 dB	0.002354	0.9999941276	0.144 s	0.118 s

Tabel 3 menampilkan evaluasi kualitas citra setelah proses *watermarking* serta pengukuran waktu *embedding* dan ekstraksi untuk setiap sampel citra MRI. Secara umum, seluruh hasil menunjukkan bahwa metode *watermarking* berbasis LSB 1-LSB pada wilayah RONI mampu mempertahankan kualitas visual citra medis pada tingkat yang tinggi. Hal ini terlihat dari nilai PSNR yang berada pada rentang 73.75–80.51 dB. Nilai PSNR tersebut menandakan bahwa perubahan intensitas piksel akibat proses penyisipan *watermark* sangat kecil sehingga tidak menghasilkan distorsi visual yang dapat mengganggu proses diagnosis. Sementara itu, nilai MSE (*Mean Squared Error*) yang diperoleh berada pada rentang 0.000578 hingga 0.002741, mendekati nol, yang semakin memperkuat bahwa perbedaan antara citra asli dan citra *watermarked* berada pada tingkat yang sangat rendah. Hal ini konsisten dengan karakteristik metode LSB yang hanya memodifikasi bit paling rendah dari piksel dan dilakukan pada area RONI, sehingga tidak memengaruhi struktur utama citra.

Selain itu, nilai SSIM yang diperoleh berada dekat dengan 1, yaitu pada rentang 0.9999923241 hingga 0.9999975797, yang menunjukkan bahwa struktur, kontras, dan luminansi citra tetap terjaga setelah proses *watermarking*. Hal ini disebabkan oleh proporsi perubahan piksel yang sangat kecil dibandingkan total piksel citra sebesar 99 byte (792 bit) yang disisipkan membuat jumlah piksel RONI yang dimodifikasi hanya sekitar 792 piksel. Jika dibandingkan dengan total piksel citra berukuran 256 × 256 (65.536 piksel), jumlah piksel yang berubah hanya sebesar 1,2%. Proporsi perubahan yang sangat kecil ini menyebabkan struktur citra tetap stabil sehingga nilai SSIM tetap sangat tinggi. Dari sisi efisiensi, waktu *embedding* berada pada rentang 0.088–0.195 detik, sedangkan waktu ekstraksi berada pada rentang 0.058–0.142 detik. Hal ini menunjukkan bahwa metode yang diusulkan memiliki kompleksitas komputasi yang rendah. Efisiensi ini membuktikan bahwa metode yang diusulkan memiliki kompleksitas rendah karena bekerja langsung pada domain spasial tanpa melibatkan transformasi matematika yang berat, sehingga dapat untuk diimplementasikan pada alur kerja klinis yang menuntut kecepatan proses.



Gambar 2. Sepuluh Citra Tambahan

Selain empat citra utama, pengujian kualitas *watermarking* juga dilakukan pada sepuluh citra MRI tambahan untuk mengevaluasi konsistensi performa metode pada citra yang berbeda, sebagaimana ditunjukkan pada Gambar 2. Hasil evaluasi kuantitatif terhadap kualitas citra setelah proses penyisipan *watermark* disajikan pada Tabel 4 melalui pengukuran nilai PSNR, MSE, dan SSIM.

Tabel 4. Evaluasi PSNR, MSE dan SSIM

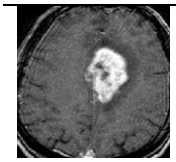
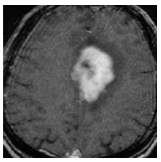
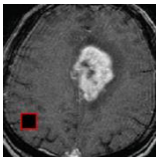
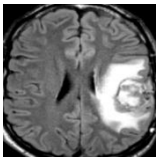
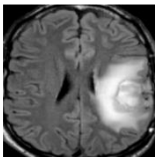
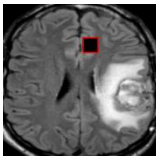
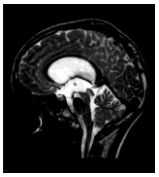
Citra MRI	PSNR	MSE	SSIM
MRI 1	75.69 dB	0.001753	0.9999931559
MRI 2	75.67 dB	0.001763	0.9999925249
MRI 3	75.72 dB	0.001742	0.9999962006
MRI 4	75.85 dB	0.001693	0.9999927921
MRI 5	75.41 dB	0.001872	0.9999943193
MRI 6	74.61 dB	0.001787	0.9999920365
MRI 7	73.34 dB	0.002184	0.9999873339
MRI 8	73.80 dB	0.002711	0.9999961878
MRI 9	74.09 dB	0.002538	0.9999955569
MRI 10	73.84 dB	0.002686	0.9999945046

Building of Informatics, Technology and Science (BITS)
Volume 8, No 1, June 2026 Page: 1−13
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v8i1.8967

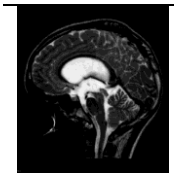
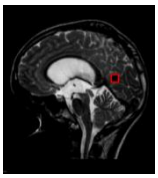
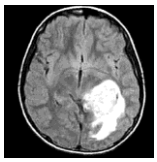
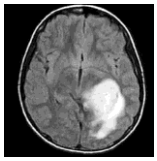
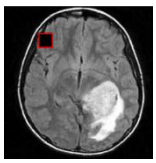
Tabel 4 menyajikan hasil evaluasi kualitas citra setelah proses *watermarking* pada sepuluh citra MRI tambahan. Secara umum, nilai PSNR, MSE, dan SSIM yang diperoleh menunjukkan pola konsisten dengan hasil pada empat citra utama sebelumnya, sehingga memperkuat kesimpulan bahwa metode yang digunakan memiliki tingkat *imperceptibility* yang baik. Nilai PSNR seluruh citra berada pada rentang 73.34 hingga 75.85 dB, dengan rata-rata 74.80 dB, yang termasuk kategori tinggi untuk citra medis. PSNR sebesar ini mengindikasikan bahwa perubahan piksel akibat proses penyisipan *watermark* sangat kecil dan tidak menimbulkan *noise* atau artefak yang dapat terlihat secara visual. Nilai MSE pada seluruh sampel juga sangat rendah, berada pada rentang 0.001693 hingga 0.002711, yang menunjukkan bahwa perbedaan antara citra asli dan citra *watermarked* hampir tidak signifikan. Seluruh citra menunjukkan nilai SSIM yang mendekati 1,0000, yang mengindikasikan bahwa struktur diagnostik citra tetap terjaga secara utuh.

Nilai SSIM pada seluruh citra berada pada rentang 0,9999873339 hingga 0.9999962006, yang menunjukkan bahwa struktur, kontras, dan luminansi citra tetap terjaga setelah proses *watermarking*. Nilai SSIM yang tinggi ini konsisten dengan karakteristik metode LSB, di mana perubahan hanya terjadi pada bit intensitas paling rendah sehingga tidak memengaruhi kesamaan struktural citra. Konsistensi nilai PSNR, MSE, dan SSIM pada seluruh citra MRI tambahan menunjukkan bahwa metode *watermarking* yang digunakan mampu bekerja secara stabil pada berbagai variasi citra. Secara keseluruhan, hasil pada Tabel 4 mengonfirmasi bahwa penyisipan watermark tidak menyebabkan degradasi kualitas citra yang signifikan, baik secara visual maupun berdasarkan metrik kuantitatif.

Tabel 5. Uji Tampering

Citra	Jenis Serangan	Area	Hash ROI Payload	Hash ROI (Recalc)	Status	Keterangan
	Window/Level	Global	Tidak tersedia/ rusak	ca235cc04a61f8 aa3debc0856f0e 9cb95ef49f6263 64ac19cbd2dc9 fb109306e	Tampered	Payload rusak akibat serangan global
	Inpainting	ROI	47ece78423e96ce 53ef35527ef669c cbe86d187f06b6 43df43f9567b37 070288	b8f6fe69be7916 e649743385909 3bc0bb304e4b3 19a8920a7cfa8 63771ebb1b7	ROI Tampered	ROI dimodifikasi, hash berubah
	Blackout Box	RONI	47ece78423e96ce 53ef35527ef669c cbe86d187f06b6 43df43f9567b37 070288	47ece78423e96ce 53ef35527ef669c cbe86d187f06b6 43df43f9567b37 070288	ROI Valid	Perubahan hanya pada RONI, ROI tetap
	Window/Level	Global	Tidak tersedia/ rusak	8a9067b3e4b6323 c88485b3431b3f1 5033c43d1e898a 8b762d6f491079 c2dd46	Tampered	Payload rusak akibat serangan global
	Inpainting	ROI	ea3de7f01dde26b 609f59c22947ece be7bb4dc1e7f657 b6ac0609d98416 2d81b	677fdcfa5e7db93c fba10f26fab0b4b 800e8aeb8a0892 1720ab29f33788 6775a	ROI Tampered	ROI dimodifikasi, hash berubah
	Blackout Box	RONI	ea3de7f01dde26b 609f59c22947ece be7bb4dc1e7f657 b6ac0609d98416 2d81b	ea3de7f01dde26b 609f59c22947ece be7bb4dc1e7f657 b6ac0609d98416 2d81b	ROI Valid	Perubahan hanya pada RONI, ROI tetap
	Window/Level	Global	Tidak tersedia/ rusak	cb350b0aa548de5 3def366e7fb2715 daf3b9cd6d4ac02 817f2c1afc7e3f2 2504	Tampered	Payload rusak akibat serangan global

Building of Informatics, Technology and Science (BITS)
Volume 8, No 1, June 2026 Page: 1−13
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v8i1.8967

Citra	Jenis Serangan	Area	Hash ROI Payload	Hash ROI (Recalc)	Status	Keterangan
	Inpainting	ROI	292eb0d5edf9c63bea0e07b547f509f8225b63b2e96f208dfabee93c670e5056	ae2b32762638eff0b4e17d68d43ea419d491145166b5cadbcf369a3c2f34a66d	ROI Tampered	ROI dimodifikasi, hash berubah
	Blackout Box	RONI	292eb0d5edf9c63bea0e07b547f509f8225b63b2e96f208dfabee93c670e5056	292eb0d5edf9c63bea0e07b547f509f8225b63b2e96f208dfabee93c670e5056	ROI Valid	Perubahan hanya pada RONI, ROI tetap
	Window/Level	Global	Tidak tersedia/ rusak	6286865a5e8949e6fb13d90affa12ef153484069af5f5c241e4799886a6c9e8a	Tampered	Payload rusak akibat serangan global
	Inpainting	ROI	e5381e0ecdbae6007d41786804382c80800e7f8c577343f9057e298a2a21764b	4fff47cbb2be7b4a438f70a28acc8da61a904637af1dc685a8a5b0c2c65534c3	ROI Tampered	ROI dimodifikasi, hash berubah
	Blackout Box	RONI	e5381e0ecdbae6007d41786804382c80800e7f8c577343f9057e298a2a21764b	e5381e0ecdbae6007d41786804382c80800e7f8c577343f9057e298a2a21764b	ROI Valid	Perubahan hanya pada RONI, ROI tetap

Tabel 5 menyajikan hasil pengujian tampering pada beberapa citra MRI dengan tiga skenario manipulasi, yaitu *window/level adjustment* (global), *inpainting* (ROI), dan *blackout box* (RONI). Secara umum, hasil menunjukkan bahwa sistem mampu membedakan dampak manipulasi berdasarkan lokasi perubahan serta kondisi *payload* watermark yang diekstraksi.

Pada skenario manipulasi global (*window/level*), seluruh citra menunjukkan bahwa nilai *hash* ROI yang tersimpan dalam *payload* tidak dapat diekstraksi (tidak tersedia/rusak). Hal ini terjadi karena perubahan intensitas secara *global* memengaruhi bit LSB pada area RONI, sehingga *payload watermark* menjadi korup. Dalam kondisi ini, sistem mengklasifikasikan citra sebagai ”Tampered”. Namun, karena tidak terdapat *hash* pembanding dari *payload*, integritas ROI tidak dapat diverifikasi secara langsung. Oleh karena itu, status yang dihasilkan merefleksikan adanya manipulasi pada citra, tetapi tidak secara spesifik menyimpulkan apakah ROI mengalami perubahan atau tidak. Pada skenario manipulasi ROI melalui teknik *inpainting*, seluruh citra menunjukkan perbedaan antara *hash* ROI hasil ekstraksi *payload* dan *hash* ROI hasil perhitungan ulang. Perbedaan ini mengindikasikan bahwa terjadi perubahan langsung pada area ROI, sehingga sistem secara konsisten mengklasifikasikan kondisi ini sebagai ”ROI Tampered”. Dengan demikian, sistem menunjukkan sensitivitas yang baik dalam mendeteksi perubahan pada area diagnostik utama.

Sebaliknya, pada skenario manipulasi RONI menggunakan *blackout box*, nilai *hash* ROI hasil ekstraksi dan hasil perhitungan ulang tetap identik pada seluruh citra uji. Hal ini menunjukkan bahwa perubahan yang terjadi terbatas pada area RONI dan tidak memengaruhi ROI. Sistem kemudian mengklasifikasikan kondisi ini sebagai ”ROI Valid”, yang menandakan bahwa integritas ROI tetap terjaga. Kondisi ini sejalan dengan desain metode di mana *payload* disisipkan hanya pada wilayah RONI, sehingga manipulasi pada area tersebut tidak memengaruhi nilai piksel pada ROI. Meskipun teknik LSB bersifat sensitif (*fragile*) terhadap perubahan, keberhasilan ekstraksi *payload* pada skenario ini dimungkinkan oleh penggunaan *payload* minimal sebesar 99 byte yang hanya menempati sebagian kecil area RONI. Rendahnya proporsi piksel yang membawa informasi autentikasi ini menyebabkan manipulasi seperti *blackout box* memiliki probabilitas rendah untuk merusak bit *watermark*, sehingga proses verifikasi integritas ROI tetap dapat dilakukan. Sistem mampu mengidentifikasi perubahan pada ROI dan tetap mempertahankan status valid ketika perubahan hanya terjadi pada RONI, serta mendeteksi kerusakan *watermark* pada manipulasi global meskipun verifikasi ROI tidak dapat dilakukan secara langsung.

Building of Informatics, Technology and Science (BITS)
Volume 8, No 1, June 2026 Page: 1−13
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v8i1.8967

Tabel 6. Komparasi Penelitian Terdahulu

Pendekatan (Penelitian)	Kriptografi / Keamanan	Avg. PSNR	Waktu (E/X)	Deteksi Tamper	Kelebihan
R. Ch et al. (2024) (Hybrid IWT-DCT)	ECDSA	68.67 dB	2.16 s E / 1.03 s X	Ya	Robust & aman
D. Ravichandran et al. (2021) (Transform IWT)	Chaotic *Embedding*	≈48.83 dB	8.37 s (Total)	Ya	Recovery ROI lossless
F. Ernawan et al. (2022) (Spatial Fragile LSB)	Otentikasi Tiga Lapisan	51.29 dB	Tidak rinci	Ya	Autentikasi berlapis
P. Singh et al. (2022) (Hybrid DWT-SVD)	Huffman & ECDSA PRK (DAC+MT)	≈45.93 dB	≈0.16 s E / ≈0.03 s X	Ya	Robust & efisien
Albin Alveda et al. (2024) (Spatial LSB Murni)	Tidak disebutkan	≈52.60 dB	Tidak rinci	Ya	PSNR tinggi & tahan Berbagai Serangan
Metode yang Diusulkan	ECDSA	75.04 dB	0.140 s E / 0.095 s /X	Ya	PSNR tinggi & efisien

Tabel 6 menunjukkan metode yang diusulkan menunjukkan keunggulan dalam efisiensi komputasi, kualitas citra, dan keamanan sistem, dengan nilai rata PSNR yang tertinggi yaitu 75.04 dB, serta waktu *embedding* dan ekstraksi yang relatif cepat. Selain itu, penggunaan SHA-256 dan ECDSA memberikan jaminan integritas dan autentikasi yang lebih kuat dibandingkan metode lain. Namun demikian, penelitian sebelumnya juga memiliki keunggulan masing-masing, seperti metode Singh et al. [14] yang lebih robust terhadap berbagai serangan, serta metode Ravichandran et al. [13] yang mampu melakukan *recovery* ROI secara *lossless*. Dengan demikian, metode yang diusulkan dapat memberikan solusi untuk skenario yang memprioritaskan integritas data diagnostik yang presisi, distorsi minimal, dan kecepatan proses yang tinggi.

4. KESIMPULAN

Berdasarkan hasil penelitian, metode yang diusulkan mampu mengintegrasikan segmentasi ROI otomatis, *watermarking* berbasis LSB, serta mekanisme autentikasi menggunakan SHA-256 dan ECDSA untuk menjaga integritas dan keaslian citra medis. Hasil pengujian menunjukkan bahwa metode dapat mempertahankan kualitas citra dengan baik, ditandai dengan nilai PSNR yang tinggi (sekitar 75 dB), MSE yang rendah, serta SSIM yang mendekati 1. Hal ini dipengaruhi oleh ukuran *payload* yang kecil, yaitu sekitar 99 byte (792 bit), sehingga jumlah piksel yang dimodifikasi sangat terbatas dibandingkan total piksel citra yang digunakan yaitu (256 × 256 = 65.536 piksel). Selain itu, penyisipan dilakukan menggunakan teknik 1-LSB pada area RONI, sehingga perubahan hanya terjadi pada bit dengan kontribusi intensitas paling rendah dan tidak memengaruhi struktur utama citra. Kondisi ini menyebabkan perbedaan antara citra asli dan citra hasil *watermarking* sangat kecil. Dari sisi efisiensi, waktu proses *embedding* dan ekstraksi relatif singkat, yaitu masing-masing sekitar 0.14 detik dan 0.095 detik. Efisiensi ini diperoleh dari kombinasi metode yang digunakan, yaitu teknik LSB pada domain spasial serta proses *hash*ing dan tanda tangan digital yang tidak memerlukan transformasi kompleks. Dari sisi keamanan, metode ini menunjukkan kemampuan dalam mendeteksi manipulasi, khususnya pada area ROI. Sistem dapat membedakan kondisi citra yang tidak mengalami perubahan, manipulasi pada ROI, serta manipulasi global yang menyebabkan kerusakan *payload*. Hasil uji *tampering* menunjukkan bahwa perubahan pada ROI dapat terdeteksi melalui perbedaan nilai *hash*, Sementara itu, manipulasi pada area RONI tidak memengaruhi hasil verifikasi ROI selama serangan tersebut tidak merusak piksel yang membawa *payload watermark*, sehingga integritas informasi diagnostik tetap dapat dinyatakan valid meskipun area latar belakang telah dimodifikasi. Dibandingkan dengan penelitian terdahulu, metode yang diusulkan menunjukkan kinerja yang baik dalam menjaga kualitas citra dan efisiensi proses. Namun demikian, metode ini masih memiliki keterbatasan dalam ketahanan terhadap serangan manipulasi berskala besar akibat penggunaan teknik LSB yang bersifat *fragile*. Selain itu, seluruh pengujian dalam penelitian ini dilakukan hanya pada citra medis MRI otak, sehingga hasil kinerja belum dapat digeneralisasikan untuk citra medis lain yang memiliki karakteristik noise, kontras, dan tekstur yang berbeda. Perbedaan karakteristik ini berpotensi memengaruhi performa segmentasi ROI yang digunakan. Pengujian pada citra dengan resolusi yang lebih besar diperlukan untuk mengevaluasi pengaruh *payload* berukuran kecil terhadap kualitas visual serta kapasitas penyisipan *watermark*.

REFERENCES

[1] M. Y. M. Parvees and T. Vijayakumar, "Medical image cryptosystem using improved Quadratic Congruential Generator and logistic map," *Meas. Sensors*, vol. 24, p. 100502, Dec. 2022, doi: 10.1016/J.MEASEN.2022.100502.
[2] B. Meng, X. Yuan, Q. Zhang, C. T. Lam, and G. Huang, "Encryption-then-*embedding*-based hybrid data hiding scheme for medical images," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 36, no. 1, p. 101932, Jan. 2024, doi: 10.1016/J.JKSUCI.2024.101932.
[3] S. Jagadeesh, A. K. Parida, and K. Meenakshi, "Tamper detection, localization and self-recovery using slant transform with

Building of Informatics, Technology and Science (BITS)
Volume 8, No 1, June 2026 Page: 1−13
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v8i1.8967

DNA encoding for medical images," *Results Eng.*, vol. 27, p. 105907, Sep. 2025, doi: 10.1016/J.RINENG.2025.105907.
[4] A. Sayyouri *et al.*, "Medical image zero-watermarking algorithm based on a reversible integer quaternionic Meixner transform and a hybrid chaotic system," *Eng. Sci. Technol. an Int. J.*, vol. 71, p. 102180, Nov. 2025, doi: 10.1016/J.JESTCH.2025.102180.
[5] S. Tu, Y. Jia, J. Du, and B. Han, "Application of Zero-Watermarking for Medical Image in Intelligent Sensor Network Security," *C. - Comput. Model. Eng. Sci.*, vol. 136, no. 1, pp. 293–321, Jan. 2023, doi: 10.32604/CMES.2023.022308.
[6] M. Magdy, K. M. Hosny, N. I. Ghali, and S. Ghoniemy, "Security of medical images for telemedicine: a systematic review," *Multimed. Tools Appl.*, vol. 81, no. 18, pp. 25101–25145, Jul. 2022, doi: 10.1007/S11042-022-11956-7/TABLES/10.
[7] M. Zarour *et al.*, "Healthcare Technology Letters Ensuring data integrity of healthcare information in the era of digital health," 2021, doi: 10.1049/htl2.12008.
[8] Y. Feng, W. Liu, X. Zhang, Z. Liu, Y. Liu, and G. Wang, "An Interval Iteration Based Multilevel Thresholding Algorithm for Brain MR Image Segmentation," *Entropy*, vol. 23, no. 11, p. 1429, Oct. 2021, doi: 10.3390/e23111429.
[9] O. C. Akinduyite *et al.*, "ECC-Based Encryption with ECDSA for Medical Images," in *IEEE International Conference on Emerging and Sustainable Technologies for Power and ICT in a Developing Society, NIGERCON*, IEEE, Nov. 2024, pp. 1–5. doi: 10.1109/NIGERCON62786.2024.10927093.
[10] A. Ch, R. Ch, S. Gadamsetty, C. Iwendi, T. R. Gadekallu, and I. Ben Dhaou, "ECDSA-Based Water Bodies Prediction from Satellite Images with UNet," *Water (Switzerland)*, vol. 14, no. 14, p. 2234, Jul. 2022, doi: 10.3390/w14142234.
[11] J. Ooi, "Performance Comparison of Spatial Domain-based Watermarking Techniques," pp. 64–69, 2021, doi: 10.1109/ICSECS52883.2021.00019.
[12] R. Ch, N. Vivek K, G. Srivastava, and Reddy Gadekallu, "ECDSA-based tamper detection in medical data using a watermarking technique," *Int. J. Cogn. Comput. Eng.*, vol. 5, no. May 2023, pp. 78–87, 2024, doi: 10.1016/j.ijcce.2024.01.003.
[13] D. Ravichandran, P. Praveenkumar, S. Rajagopalan, J. B. B. Rayappan, and R. Amirtharajan, "ROI-based medical image watermarking for accurate tamper detection, localisation and recovery," *Med. Biol. Eng. Comput.*, vol. 59, no. 6, pp. 1355–1372, 2021, doi: 10.1007/s11517-021-02374-2.
[14] P. Singh, K. J. Devi, H. K. Thakkar, and K. Kotecha, "Region-Based Hybrid Medical Image Watermarking Scheme for Robust and Secured Transmission in IoMT," *IEEE Access*, vol. 10, pp. 8974–8993, 2022, doi: 10.1109/ACCESS.2022.3143801.
[15] A. Alveda, L. Rakhmawati, R. H. Peni, and A. Tjahyaningtijas, "Penyisipan Watermark Menggunakan Metode LSB (Least Significant Bit) untuk Autentikasi Citra Medis," *J. Tek. ELEKTRO*, vol. 13, no. 3, pp. 273–280, Jul. 2024, doi: 10.26740/JTE.V13N3.P273-280.
[16] F. Ernawan, A. Aminuddin, D. Nincarean, M. F. A. Razak, and A. Firdaus, "Three Layer Authentications with a Spiral Block Mapping to Prove Authenticity in Medical Images," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 4, pp. 211–223, Apr. 2022, doi: 10.14569/IJACSA.2022.0130425.
[17] Y. Guo, Y. Wang, K. Meng, and Z. Zhu, "Otsu Multi-Threshold Image Segmentation Based on Adaptive Double-Mutation Differential Evolution," *Biomimetics*, vol. 8, no. 5, 2023, doi: 10.3390/biomimetics8050418.
[18] Katherine, R. Rulaningtyas, and K. Ain, "CT scan image segmentation based on hounsfield unit values using Otsu thresholding method," *J. Phys. Conf. Ser.*, vol. 1816, no. 1, p. 012080, Feb. 2021, doi: 10.1088/1742-6596/1816/1/012080.
[19] L. Thi Bich Huong, "Watermarking Scheme Based On Most Significant Bit For Public Copyright Protection For Relational Databases," *Vinh Univ. J. Sci.*, vol. 53, no. 3A, pp. 73–79, Sep. 2024, doi: 10.56824/VUJS.2024A032A.
[20] J. Wu, J. Zhang, D. Liu, and X. Wang, "A Multiple-Medical-Image Encryption Method Based on SHA-256 and DNA Encoding," *Entropy*, vol. 25, no. 6, 2023, doi: 10.3390/e25060898.
[21] M. Hanif *et al.*, "A Novel Grayscale Image Encryption Scheme Based on the Block-Level Swapping of Pixels and the Chaotic System," *Sensors*, vol. 22, no. 16, 2022, doi: 10.3390/s22166243.
[22] T. Wellem, Y. Nataliani, and A. Iriani, "Academic Document Authentication using Elliptic Curve Digital Signature Algorithm and QR Code," *Int. J. Informatics Vis.*, vol. 6, no. 3, pp. 667–675, 2022, doi: 10.30630/joiv.6.2.872.
[23] A. Nadzifarin and A. Asmunin, "Penerapan Elliptic Curve Digital Signature Algorithm pada Tanda Tangan Digital dengan Studi Kasus Dokumen Surat – Menyurat," *J. Informatics Comput. Sci.*, vol. 4, no. 01, pp. 1–9, 2022, doi: 10.26740/jinacs.v4n01.p1-9.
[24] D. S. P. Kanakam, "ECDSA: The Virtual Signature Set of Rules of a Higher Internet," *Int. J. Eng. Comput. Sci.*, vol. 10, no. 10, pp. 25408–25412, 2021, doi: 10.18535/ijecs/v10i10.4630.
[25] A. A. Shareef and M. G. Ahmed, "Securing Digital Information Through Image Watermarking With Lsb Algorithm: a Comprehensive Overview and Implementation Using Matlab," *Eng. Technol. J.*, vol. 08, no. 05, pp. 2176–2182, 2023, doi: 10.47191/etj/v8i5.03.
[26] Z. Bin Faheem *et al.*, "Image Watermarking Scheme Using LSB and Image Gradient," *Appl. Sci.*, vol. 12, no. 9, pp. 1–12, 2022, doi: 10.3390/app12094202.
[27] A. Haque, A. Wang, and A. A. Z. Imran, "Window-Level Is a Strong Denoising Surrogate," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12966 LNCS, pp. 457–466, 2021, doi: 10.1007/978-3-030-87589-3_47.
[28] W. Quan, R. Zhang, Y. Zhang, Z. Li, J. Wang, and D. M. Yan, "Image Inpainting with Local and Global Refinement," *IEEE Trans. Image Process.*, vol. 31, no. c, pp. 2405–2420, 2022, doi: 10.1109/TIP.2022.3152624.
[29] M. Arabboev, S. Begmatov, M. Rikhsivoev, K. Nosirov, and S. Saydiakbarov, "A comprehensive review of image super-resolution metrics: classical and AI-based approaches," *Acta IMEKO*, vol. 13, no. 1, pp. 1–8, 2024, doi: 10.21014/ACTAIMEKO.V13I1.1679.
[30] U. S. Ukommi, "Review of Multimedia Communication Quality Assessment Techniques," *Niger. J. Technol.*, vol. 41, no. 2, pp. 330–338, 2022, doi: 10.4314/njt.v41i2.15.
[31] M. Dohmen, M. A. Klemens, I. M. Baltruschat, T. Truong, and M. Lenga, "Similarity and quality metrics for MR image-to-image translation," *Sci. Rep.*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-87358-0.