



Tren dan Inovasi dalam Image Hiding untuk Keamanan Informasi Medis: Tinjauan Literatur

Maliatul Fitriyasari

Fakultas Ilmu Komputer, Universitas Jember

maliatul.fitriyasari@gmail.com

Abstrak

Pertukaran dan penyimpanan data medis digital, seperti citra hasil MRI, CT-scan, dan X-ray, telah menjadi kebutuhan utama dalam pelayanan kesehatan modern. Namun, meningkatnya volume data medis berbasis jaringan memunculkan ancaman serius terhadap privasi dan keamanan informasi pasien. Salah satu solusi yang banyak dikembangkan adalah image hiding atau steganografi citra, yang memungkinkan penyisipan informasi rahasia ke dalam citra medis tanpa mengurangi kualitas visualnya secara signifikan. Artikel ini menyajikan tinjauan literatur terkini mengenai tren dan inovasi dalam image hiding untuk aplikasi keamanan informasi medis. Studi ini menganalisis berbagai pendekatan steganografi, meliputi teknik berbasis domain spasial dan domain transformasi, serta metode berbasis pembelajaran mesin seperti Generative Adversarial Networks (GAN). Selain itu, tinjauan ini membahas metrik evaluasi yang umum digunakan, seperti Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), dan kapasitas payload. Hasil kajian menunjukkan bahwa integrasi algoritma optimisasi dan teknik deep learning mampu meningkatkan performa steganografi dalam hal kapasitas, kualitas citra stego, dan ketahanan terhadap deteksi. Artikel ini juga merumuskan tantangan penelitian serta arah pengembangan masa depan dalam bidang keamanan informasi medis berbasis image hiding.

Kata kunci: image hiding, steganografi, citra medis, keamanan informasi, Generative Adversarial Networks (GAN), PSNR, SSIM

1. Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah membawa dampak signifikan dalam berbagai bidang, termasuk sektor kesehatan. Transformasi digital di bidang kesehatan mendorong penggunaan Rekam Medis Elektronik (RME) dan citra medis digital seperti CT-scan, MRI, dan X-ray. Penerapan teknologi ini tidak hanya meningkatkan efisiensi layanan medis, tetapi juga memungkinkan proses pertukaran informasi pasien secara cepat antar fasilitas layanan kesehatan. Meski demikian, digitalisasi ini juga memunculkan tantangan besar terkait privasi, integritas, dan keamanan data medis yang bersifat sangat sensitif. Menurut laporan World Health Organization (WHO), kasus kebocoran data medis terus meningkat dalam beberapa tahun terakhir, di mana sebagian besar insiden tersebut terjadi saat proses transmisi dan penyimpanan data digital [1]. Data medis mencakup informasi penting tentang identitas pasien, hasil diagnosis, serta riwayat penyakit yang jika disalahgunakan dapat menimbulkan risiko etik, hukum, maupun sosial. Oleh karena itu, diperlukan metode pengamanan data yang andal untuk melindungi kerahasiaan informasi medis dari akses tidak sah dan potensi modifikasi.

Salah satu teknik keamanan informasi yang banyak digunakan adalah kriptografi, yang berfungsi mengenkripsi data agar tidak dapat dibaca pihak tidak berwenang. Meskipun kriptografi sangat efektif dalam menjaga kerahasiaan, metode ini tetap memiliki kelemahan dalam hal mendeteksi upaya modifikasi data dan kerentanannya terhadap serangan brute force di lingkungan jaringan yang tidak aman [2]. Untuk itu, steganografi hadir sebagai metode pelengkap, dengan cara menyembunyikan informasi sensitif ke dalam media digital seperti gambar, audio, maupun video tanpa mengubah tampilan atau kualitas media tersebut secara signifikan. Dalam konteks medis, teknik steganografi khususnya image hiding menjadi salah satu solusi potensial untuk mengamankan pertukaran citra medis. Melalui metode ini, informasi pasien dapat disisipkan langsung ke dalam file gambar medis tanpa mengganggu kualitas visual yang diperlukan dalam proses diagnosis. Selain meningkatkan keamanan, metode ini juga mendukung regulasi perlindungan data pasien, seperti Health Insurance Portability and Accountability Act (HIPAA) di Amerika Serikat dan General Data Protection Regulation (GDPR) di Eropa [3].

Berbagai teknik steganografi telah dikembangkan dalam beberapa dekade terakhir. Metode yang paling sederhana adalah Least Significant Bit (LSB), di mana data rahasia disisipkan ke dalam bit paling tidak signifikan dari citra digital. Meskipun metode ini mudah diimplementasikan, ia sangat rentan terhadap kompresi dan modifikasi gambar [4]. Oleh karena itu, penelitian mulai beralih ke teknik berbasis transformasi domain, seperti Discrete Wavelet Transform (DWT) dan Discrete Cosine Transform (DCT) yang menawarkan ketahanan lebih baik terhadap berbagai serangan steganalisis.

Tren terbaru menunjukkan integrasi antara steganografi dengan teknik kriptografi serta watermarking digital guna menciptakan sistem keamanan berlapis. Pendekatan ini memungkinkan tidak hanya menyembunyikan informasi, tetapi juga memastikan integritas dan autentikasi data medis [5]. Selain itu, kemajuan dalam bidang kecerdasan buatan, khususnya Generative Adversarial Network (GAN) dan Convolutional Neural Network (CNN), telah mendorong pengembangan metode steganografi berbasis deep learning yang mampu meningkatkan kapasitas payload, ketahanan terhadap serangan, dan kualitas citra yang lebih optimal [6]. Namun demikian, sejumlah tantangan masih perlu diatasi, seperti peningkatan kapasitas penyisipan data tanpa memengaruhi kualitas visual citra medis, penguatan ketahanan terhadap berbagai jenis serangan steganalisis, serta pengembangan algoritma yang efisien untuk diaplikasikan dalam sistem telemedis berbasis internet. Oleh karena itu, diperlukan sebuah studi literatur sistematis yang merangkum tren, teknik, dan inovasi terkini dalam bidang image hiding untuk keamanan data medis, yang sekaligus dapat menjadi dasar pengembangan solusi keamanan informasi di masa depan..

2. Metode Penelitian

2.1. Desain Studi

Penelitian ini dilakukan dalam bentuk tinjauan literatur sistematis guna memetakan tren, teknik, dan inovasi terkini terkait implementasi image hiding dalam keamanan informasi medis. Studi ini menggunakan metode Systematic Literature Review (SLR) yang dirancang mengikuti pedoman Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guna memastikan proses seleksi, dokumentasi, dan analisis artikel dilakukan secara sistematis, transparan, dan dapat direplikasi [7]. Pendekatan sistematis dipilih karena dinilai mampu merangkum perkembangan penelitian secara komprehensif serta memberikan rekomendasi berbasis bukti terhadap arah riset di bidang keamanan informasi medis melalui steganografi citra.

2.2. Sumber Data dan Strategi Pencarian

Proses pencarian artikel dilakukan pada lima basis data ilmiah bereputasi, yaitu IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, dan PubMed. Basis data ini dipilih karena menyediakan artikel terkini dalam bidang keamanan informasi, teknik steganografi, dan teknologi kesehatan. Kata kunci yang digunakan dalam pencarian meliputi: "medical image steganography", "image hiding in healthcare", "secure medical data transmission", "steganography in telemedicine", "medical image security", dan "image steganography algorithms". Operator Boolean seperti AND, OR, dan NOT diterapkan untuk menyaring hasil pencarian yang lebih relevan.

2.3. Kriteria Inklusi dan Eksklusi

Agar hasil tinjauan lebih fokus dan relevan, ditetapkan kriteria inklusi dan eksklusi. Adapun kriteria inklusi meliputi:

- Studi yang membahas penerapan teknik steganografi pada data medis berbasis gambar.
- Artikel yang melaporkan hasil uji metrik kinerja seperti Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM), kapasitas payload, dan ketahanan terhadap steganalisis.
- Studi yang dipublikasikan dalam jurnal atau prosiding terindeks seperti Scopus atau Web of Science.
- Sementara itu, kriteria eksklusi terdiri dari:
- Studi yang membahas steganografi di luar domain medis.
- Artikel non-peer-reviewed atau tidak tersedia dalam full text.
- Publikasi dalam bahasa selain Inggris dan Indonesia.

2.4. Proses Seleksi Studi

Seleksi artikel dilakukan melalui tiga tahap, yaitu:

1. Tahap Identifikasi: Semua artikel hasil pencarian dikumpulkan dan didokumentasikan dalam spreadsheet.
2. Tahap Penyaringan: Artikel duplikat dihapus. Selanjutnya, judul dan abstrak artikel ditelaah untuk menilai relevansi terhadap topik.

3. Tahap Kelayakan: Artikel yang tersisa dianalisis secara penuh untuk memastikan kesesuaiannya dengan kriteria inklusi.

2.5. Ekstraksi dan Sintesis Data

Dari artikel yang memenuhi kriteria, dilakukan ekstraksi data meliputi:

- Jenis teknik steganografi yang digunakan (LSB, DWT, DCT, GAN, Autoencoder).
- Jenis citra medis yang digunakan (CT-scan, MRI, X-ray, Ultrasound).
- Metrik evaluasi seperti PSNR, SSIM, payload capacity, dan robustness.
- Integrasi algoritma keamanan lainnya seperti kriptografi dan watermarking.

Data hasil ekstraksi kemudian dianalisis secara deskriptif dan kualitatif untuk memetakan tren, inovasi algoritma, dan tantangan penelitian. Selanjutnya, dilakukan sintesis untuk membandingkan kelebihan dan kelemahan masing-masing teknik.

2.6. Validasi dan Penilaian Kualitas

Setiap artikel yang masuk dalam tinjauan akhir dievaluasi kualitasnya menggunakan Critical Appraisal Skills Programme (CASP) untuk studi kualitatif, serta Quality Assessment Tool for Quantitative Studies untuk studi kuantitatif. Artikel dengan kualitas metodologis rendah dikeluarkan dari sintesis akhir guna menjaga validitas hasil penelitian.

3. Hasil dan Diskusi

3.1. Evaluasi Teknik Steganografi dalam Citra Medis

Steganografi merupakan teknik penting dalam melindungi kerahasiaan data medis, khususnya pada citra medis digital seperti MRI, CT scan, dan X-ray. Berdasarkan tinjauan literatur, teknik steganografi dalam citra medis umumnya terbagi menjadi dua kategori utama, yaitu domain spasial dan domain transformasi.

3.1.1. Domain Spasial

Metode domain spasial menyisipkan data langsung ke dalam nilai piksel citra. Salah satu teknik yang paling umum digunakan adalah Least Significant Bit (LSB). Teknik ini mengganti bit-bit paling tidak signifikan dari setiap piksel dengan bit data rahasia sehingga perubahan visual citra hampir tidak terlihat. Keunggulan utama metode ini terletak pada kesederhanaan implementasi dan kapasitas penyisipan data yang relatif besar. Namun, teknik LSB memiliki beberapa kelemahan yang signifikan, terutama dalam hal ketahanan terhadap manipulasi citra dan serangan statistik. Teknik ini rentan terhadap serangan seperti analisis chi-square dan RS steganalisis yang dapat mengidentifikasi keberadaan data tersembunyi. Selain itu, proses kompresi lossy seperti JPEG dapat merusak data yang disisipkan karena mengubah bit-bit LSB yang berisi pesan rahasia. Sebagai contoh, Ogundokun et al. mengembangkan modifikasi teknik LSB dengan menambahkan pergeseran sirkular dan enkripsi untuk meningkatkan keamanan penyisipan data dalam citra medis, yang berhasil memperkuat ketahanan data terhadap akses tidak sah [9]. Namun demikian, kelemahan terhadap serangan statistik tetap menjadi tantangan utama bagi metode domain spasial [10].

3.1.2. Domain Transformasi

Berbeda dengan domain spasial, teknik steganografi pada domain transformasi melakukan penyisipan data pada koefisien hasil transformasi frekuensi citra, seperti Discrete Cosine Transform (DCT) dan Discrete Wavelet Transform (DWT). Teknik ini dianggap lebih tahan terhadap kompresi dan manipulasi citra karena modifikasi dilakukan pada domain frekuensi yang lebih stabil terhadap perubahan tersebut. Murthy et al. memaparkan bahwa penyisipan data di koefisien frekuensi menengah hasil DCT mampu menjaga kualitas visual citra medis dengan nilai PSNR yang tinggi, sambil memastikan keamanan data yang disisipkan [11]. Selain itu, Simanungkalit et al. membuktikan efektivitas teknik DWT dalam menyembunyikan data pada sub-band frekuensi tanpa mengurangi kualitas diagnostik citra medis [12]. Kelemahan utama teknik ini adalah kompleksitas komputasi yang lebih tinggi dan kapasitas penyisipan data yang lebih kecil dibandingkan domain spasial. Namun, keuntungan dalam hal kualitas dan ketahanan citra stego membuat metode ini lebih cocok untuk aplikasi medis yang membutuhkan integritas citra tinggi.

3.2 Evaluasi Kinerja: PSNR, SSIM, dan Kapasitas Payload

Evaluasi kinerja teknik steganografi dalam citra medis menjadi aspek krusial untuk menentukan efektivitas metode yang digunakan. Tiga metrik utama yang sering dipakai dalam penilaian tersebut adalah Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), dan kapasitas payload. Masing-

masing metrik ini memberikan gambaran berbeda mengenai kualitas, kesamaan, dan kapasitas data tersembunyi dalam citra stego.

3.2.1 Peak Signal-to-Noise Ratio (PSNR)

PSNR merupakan metrik kuantitatif yang digunakan untuk mengukur kualitas citra stego dengan membandingkan perbedaan intensitas piksel antara citra asli dan citra yang sudah disisipi data. Nilai PSNR yang lebih tinggi menunjukkan bahwa citra stego lebih mirip dengan citra asli dan oleh karena itu kualitasnya lebih baik. Menurut penelitian Rashid et al., teknik steganografi berbasis domain transformasi, seperti Discrete Cosine Transform (DCT) dan Discrete Wavelet Transform (DWT), umumnya menghasilkan nilai PSNR di atas 40 dB, yang menandakan kualitas citra yang sangat baik setelah penyisipan data [9]. Sebaliknya, teknik domain spasial seperti Least Significant Bit (LSB) biasanya memiliki nilai PSNR yang lebih rendah, berkisar antara 30 sampai 35 dB, karena penyisipan data langsung ke piksel rentan menyebabkan penurunan kualitas visual [9]. Studi oleh Murthy et al. juga memperlihatkan bahwa teknik DCT mampu mempertahankan kualitas citra medis dengan PSNR di atas 40 dB, sehingga cocok untuk aplikasi medis yang menuntut kualitas citra diagnostik tetap tinggi meskipun data tambahan disisipkan [11]. Hal ini menegaskan bahwa penggunaan teknik transformasi dapat meminimalkan degradasi citra akibat proses steganografi.

3.2.2 Structural Similarity Index Measure (SSIM)

SSIM adalah metrik yang mengukur kesamaan struktural antara citra asli dan citra stego berdasarkan luminansi, kontras, dan struktur. Berbeda dengan PSNR yang hanya mengukur perbedaan numerik piksel, SSIM lebih sesuai untuk menilai persepsi visual manusia terhadap kualitas citra. Nilai SSIM berkisar dari 0 hingga 1, dengan nilai mendekati 1 menunjukkan kesamaan struktur yang tinggi. Beberapa studi menunjukkan bahwa teknik berbasis domain transformasi dan algoritma berbasis pembelajaran mesin, seperti Generative Adversarial Networks (GAN), mampu mencapai nilai SSIM yang lebih tinggi dibandingkan teknik tradisional seperti LSB. Menurut Simanungkalit et al., implementasi DWT pada steganografi citra medis dapat menghasilkan nilai SSIM yang mendekati 0,99, yang berarti struktur citra asli hampir tidak berubah [12]. Sedangkan metode berbasis GAN, yang mulai banyak digunakan, mampu mengoptimalkan penyisipan data dengan menjaga kesamaan struktural sekaligus meningkatkan ketahanan terhadap serangan [13].

3.2.3 Kapasitas Payload

Kapasitas payload mengacu pada jumlah maksimum data rahasia yang dapat disisipkan ke dalam citra stego tanpa menurunkan kualitas citra secara signifikan. Teknik domain spasial seperti LSB biasanya memiliki kapasitas payload yang tinggi karena data disisipkan langsung ke bit-bit piksel. Namun, kapasitas yang tinggi ini sering kali menjadi kompromi terhadap kualitas citra dan ketahanan terhadap serangan [9]. Sebaliknya, teknik domain transformasi dan metode berbasis pembelajaran mesin cenderung memiliki kapasitas payload yang lebih rendah, karena penyisipan data dilakukan secara selektif pada koefisien frekuensi atau melalui optimasi model generatif. Meski demikian, mereka menawarkan kualitas citra dan ketahanan yang lebih baik, yang sangat penting dalam aplikasi medis di mana integritas citra harus terjaga [11], [13].

3.3 Inovasi Terkini: Pembelajaran Mesin dan Optimisasi

Perkembangan pesat dalam bidang pembelajaran mesin (machine learning) dan teknik optimisasi telah membuka peluang baru dalam inovasi steganografi untuk citra medis. Pendekatan-pendekatan modern ini berfokus pada peningkatan kualitas stego image, ketahanan terhadap serangan, dan kapasitas penyisipan data secara adaptif, sekaligus menjaga integritas informasi medis yang sangat sensitif.

3.3.1 Pembelajaran Mesin dalam Steganografi

Teknik steganografi tradisional sering kali menggunakan metode statis yang kurang mampu beradaptasi terhadap karakteristik citra medis yang kompleks. Dengan kemunculan pembelajaran mesin, khususnya jaringan saraf dalam (deep neural networks), model-model steganografi menjadi lebih adaptif dan efisien dalam menyisipkan serta mengekstraksi data tersembunyi.

Salah satu pendekatan populer adalah penggunaan Generative Adversarial Networks (GANs). GAN mampu menghasilkan citra stego yang sangat realistis dengan meminimalkan distorsi visual dan meningkatkan keamanan data tersembunyi. Menurut Zhang et al., GAN-based steganografi menunjukkan peningkatan signifikan dalam hal kualitas citra dan ketahanan terhadap deteksi steganalisis dibandingkan metode konvensional [13]. Model ini belajar secara otomatis fitur optimal untuk menyembunyikan data dan dapat menyesuaikan tingkat embedding berdasarkan konten citra medis. Selain GAN, Convolutional Neural Networks (CNNs) juga digunakan untuk optimasi proses penyisipan dan ekstraksi data. CNN memungkinkan identifikasi area-area citra yang paling toleran terhadap perubahan, sehingga penyisipan data dapat dilakukan secara selektif untuk menjaga kualitas diagnostik citra medis [14].

3.3.2 Teknik Optimisasi untuk Steganografi

Optimisasi matematis dan algoritma metaheuristik seperti Particle Swarm Optimization (PSO), Genetic Algorithm (GA), dan Ant Colony Optimization (ACO) mulai diintegrasikan ke dalam proses steganografi untuk meningkatkan performa secara otomatis. Misalnya, PSO digunakan untuk mencari posisi terbaik di citra medis guna menyisipkan bit data dengan meminimalkan distorsi dan memaksimalkan kapasitas payload. Studi oleh Li et al. melaporkan bahwa teknik steganografi berbasis PSO mampu meningkatkan PSNR hingga 42 dB dan mempertahankan nilai SSIM di atas 0,98, jauh lebih baik dibandingkan metode tradisional [15]. Pendekatan GA juga efektif dalam mengoptimalkan pola penyisipan data dengan mempertimbangkan batas toleransi diagnostik citra. Selain itu, integrasi teknik optimisasi dengan pembelajaran mesin dapat menciptakan sistem hybrid yang adaptif, meningkatkan efisiensi dan keamanan transmisi informasi medis [16].

3.3.3 Tantangan dan Peluang

Meskipun pembelajaran mesin dan optimisasi menawarkan banyak keuntungan, terdapat beberapa tantangan yang harus dihadapi. Pertama, kebutuhan akan dataset besar dan berkualitas tinggi untuk melatih model pembelajaran mesin secara efektif, terutama dalam domain medis yang sensitif terhadap privasi dan regulasi seperti HIPAA. Kedua, kompleksitas komputasi yang tinggi dari model deep learning dan algoritma optimisasi memerlukan sumber daya komputasi yang besar, yang mungkin membatasi penerapan di lingkungan klinis dengan keterbatasan perangkat keras.

Meski begitu, inovasi ini membuka peluang besar dalam pengembangan steganografi cerdas yang tidak hanya menyembunyikan data secara efektif tetapi juga adaptif terhadap jenis dan kondisi citra medis. Penggabungan pembelajaran mesin dan optimisasi diyakini akan menjadi tren utama di masa depan untuk menjamin keamanan dan privasi informasi medis digital [17].

3.4 Tantangan dan Arah Penelitian Masa Depan

Walaupun kemajuan dalam teknik steganografi untuk citra medis telah menunjukkan hasil yang menjanjikan, masih terdapat berbagai tantangan penting yang harus diatasi guna memastikan keamanan dan keandalan penyimpanan serta transmisi informasi medis yang tersembunyi. Tantangan ini berkaitan dengan keseimbangan kapasitas penyisipan dan kualitas citra, ketahanan terhadap berbagai jenis serangan, serta perlunya standarisasi metode evaluasi. Selain itu, arah penelitian masa depan memerlukan pengembangan pendekatan yang lebih adaptif, efisien, dan kompatibel dengan kebutuhan dunia medis digital.

3.4.1 Keseimbangan antara Kapasitas dan Kualitas

Salah satu permasalahan utama dalam steganografi citra medis adalah trade-off antara kapasitas penyisipan data (payload capacity) dan kualitas citra stego. Semakin besar jumlah data yang disisipkan dalam citra, maka kemungkinan besar kualitas visual citra akan menurun, yang berisiko mengganggu fungsi diagnostik citra medis tersebut. Sebagian besar penelitian saat ini masih berusaha mencari titik keseimbangan optimal agar data medis dapat disisipkan tanpa mengorbankan kualitas citra secara signifikan.

Menurut studi yang dilakukan oleh Li et al., peningkatan kapasitas payload pada metode Least Significant Bit (LSB) dapat menurunkan nilai PSNR dan SSIM, yang pada akhirnya memengaruhi kualitas visual citra medis [15]. Oleh karena itu, penelitian ke depan perlu difokuskan pada teknik steganografi adaptif, yang secara otomatis menyesuaikan kapasitas penyisipan berdasarkan area atau fitur citra yang toleran terhadap perubahan.

3.4.2 Ketahanan terhadap Serangan

Ketahanan terhadap berbagai jenis serangan, baik serangan statistik maupun manipulasi citra (seperti kompresi JPEG, cropping, scaling, atau filtering), menjadi tantangan signifikan dalam steganografi citra medis. Citra medis seringkali melalui berbagai proses pengolahan sebelum sampai ke pihak yang berwenang, sehingga metode steganografi yang digunakan harus mampu menjaga keberadaan dan integritas data tersembunyi di berbagai kondisi.

Seperti yang disampaikan oleh Zhang et al., metode berbasis domain transformasi seperti Discrete Wavelet Transform (DWT) dan Discrete Cosine Transform (DCT) cenderung lebih tahan terhadap kompresi dan noise dibandingkan metode spasial [13]. Namun, metode ini masih rentan terhadap serangan kompleks, seperti serangan steganalisis berbasis deep learning yang dapat mendeteksi pola penyisipan data secara akurat. Oleh sebab itu, pengembangan metode steganografi yang lebih aman dan dinamis menggunakan teknik pembelajaran mesin serta optimisasi adaptif menjadi prioritas penelitian ke depan.

3.4.3 Standarisasi dan Evaluasi

Saat ini, belum terdapat standar evaluasi yang baku untuk mengukur kinerja dan keamanan metode steganografi citra medis. Setiap penelitian biasanya menggunakan metrik dan dataset yang berbeda, sehingga menyulitkan perbandingan objektif antar-metode. Hal ini diakui sebagai salah satu kendala utama dalam pengembangan metode steganografi medis yang dapat diterapkan secara luas.

Menurut Chen et al., pengembangan benchmark dataset citra medis dengan anotasi penyisipan data yang jelas dan protokol evaluasi terstandarisasi dapat membantu komunitas peneliti melakukan perbandingan kinerja secara lebih objektif dan sistematis [17]. Selain itu, diperlukan pedoman etika dan regulasi yang lebih jelas terkait steganografi medis untuk memastikan perlindungan privasi pasien tetap terjaga.

3.4.4 Arah Penelitian Masa Depan

Arah penelitian masa depan dalam steganografi citra medis berpotensi menggabungkan teknik pembelajaran mesin, optimisasi evolusioner, serta pengembangan sistem steganografi adaptif berbasis konteks citra. Implementasi steganografi berbasis deep learning, seperti Generative Adversarial Networks (GAN) dan Variational Autoencoders (VAE), diyakini mampu menghasilkan metode penyisipan data yang lebih aman, adaptif, dan memiliki ketahanan tinggi terhadap berbagai serangan steganalisis modern.

Selain itu, kolaborasi antar-bidang seperti keamanan informasi, teknologi medis, dan kecerdasan buatan diperlukan untuk merancang sistem steganografi medis yang tidak hanya aman, tetapi juga praktis diterapkan di lingkungan klinis yang memiliki keterbatasan perangkat keras dan waktu.

4. Kesimpulan

Berdasarkan hasil tinjauan terhadap berbagai literatur terkini, dapat disimpulkan bahwa image hiding atau steganografi citra memiliki peran yang semakin penting dalam upaya menjaga kerahasiaan dan keamanan data medis digital. Dalam konteks industri kesehatan yang saat ini mengalami digitalisasi masif melalui penerapan sistem rekam medis elektronik (Electronic Medical Record/EMR) dan pertukaran informasi medis berbasis jaringan, keamanan data menjadi isu yang krusial, terutama terkait privasi pasien. Penggunaan teknik steganografi sebagai salah satu mekanisme pendukung keamanan informasi telah terbukti mampu meningkatkan proteksi terhadap data sensitif, khususnya pada citra medis seperti MRI, CT-scan, dan X-ray. Dari hasil studi, teknik steganografi dalam citra medis secara umum terbagi menjadi dua domain utama, yaitu domain spasial dan domain transformasi. Metode domain spasial seperti Least Significant Bit (LSB) menawarkan kelebihan dalam hal kapasitas payload dan kemudahan implementasi, namun cenderung memiliki kelemahan pada aspek ketahanan terhadap kompresi maupun serangan steganalisis. Sebaliknya, metode berbasis domain transformasi seperti Discrete Cosine Transform (DCT) dan Discrete Wavelet Transform (DWT) mampu memberikan ketahanan yang lebih baik terhadap manipulasi dan perubahan citra, meskipun dengan kapasitas payload yang lebih terbatas [2], [8]. Perkembangan terbaru menunjukkan bahwa integrasi teknik pembelajaran mesin, khususnya Generative Adversarial Networks (GAN), telah berhasil meningkatkan performa steganografi citra medis baik dari aspek kualitas citra stego maupun ketahanan terhadap deteksi. Beberapa studi melaporkan bahwa penggunaan GAN dapat meningkatkan nilai Peak Signal-to-Noise Ratio (PSNR) dan Structural Similarity Index Measure (SSIM) secara signifikan, sekaligus mempertahankan kapasitas penyisipan data yang kompetitif [6], [18]. Selain itu, implementasi algoritma optimisasi seperti Particle Swarm Optimization (PSO) dan algoritma berbasis chaos juga berkontribusi dalam mengoptimalkan posisi penyisipan bit rahasia sehingga mampu meminimalisasi distorsi dan memperkuat resistensi terhadap serangan steganalisis [19]. Namun demikian, terdapat sejumlah tantangan yang perlu diperhatikan dalam pengembangan steganografi citra medis di masa depan. Beberapa di antaranya adalah kebutuhan akan keseimbangan optimal antara kapasitas payload, kualitas citra, dan ketahanan terhadap serangan. Selain itu, masih terdapat keterbatasan dalam hal standarisasi metrik evaluasi dan ketersediaan dataset benchmark khusus citra medis yang dapat digunakan secara umum. Keterbatasan ini menjadi hambatan dalam melakukan perbandingan performa antar algoritma secara objektif. Oleh karena itu, arah penelitian selanjutnya sebaiknya difokuskan pada pengembangan metode hybrid yang menggabungkan keunggulan dari berbagai pendekatan steganografi, serta integrasi lebih lanjut dengan teknologi deep learning untuk meningkatkan kemampuan deteksi adaptif dan optimasi penyisipan data. Selain itu, upaya standarisasi metrik kinerja dan penyediaan dataset terbuka untuk citra medis sangat diperlukan guna menunjang penelitian yang lebih sistematis dan komprehensif di bidang ini. Dengan demikian, image hiding atau steganografi citra tidak hanya relevan sebagai solusi keamanan informasi medis, tetapi juga berpotensi besar menjadi salah satu komponen penting dalam pengembangan sistem keamanan data berbasis digital di sektor kesehatan ke depan.

Referensi

- [1] S. Gulia, S. Mukherjee, and T. Choudhury, "An extensive literature survey on medical image steganography," *CSI Transactions on ICT*, vol. 4, no. 4, pp. 293–298, 2016.
- [2] B. A. Shtayt, N. H. Zakaria, and N. H. Harun, "A Comprehensive Review on Medical Image Steganography Based on LSB Technique and Potential Challenges," *Baghdad Science Journal*, vol. 18, no. 2(Suppl.), pp. 957–974, 2021.
- [3] H. N. AlEisa, "Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things," *Journal of Healthcare Engineering*, vol. 2022, Article ID 7528583, 2022.

- [4] A. Singh, R. Kumar, and R. Kaur, "Medical Image Steganography Using LSB and Huffman Encoding," *Procedia Computer Science*, vol. 132, pp. 1256–1263, 2018.
- [5] M. Elhoseny and A. A. Elghamrawy, "Evaluating the merits and constraints of cryptography-steganography fusion: a systematic analysis," *International Journal of Information Security*, vol. 23, no. 1, pp. 1–20, 2024.
- [6] J. Liu et al., "Recent Advances of Image Steganography with Generative Adversarial Networks," *arXiv preprint arXiv:1907.01886*, 2019.
- [7] M. Moher, D. Liberati, J. Tetzlaff, dan D. Altman, "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement," *PLoS Med.*, vol. 6, no. 7, p. e1000097, 2009.
- [8] A. Z. Abadin, R. Sulaiman, dan M. K. Hasan, "Randomization Strategies in Image Steganography Techniques: A Review," *Comput. Mater. Contin.*, vol. 80, no. 2, pp. 3139–3171, 2024.
- [9] R. O. Ogundokun, A. O. Ayodele, dan S. O. Fagbohunka, "A Safe and Secured Medical Textual Information Using an Improved LSB Image Steganography," *Int. J. Digit. Multimed. Broadcast.*, vol. 2021, pp. 1–12, 2021.
- [10] A. Rashid, M. Amjad, dan M. Hussain, "Analysis of Steganography Techniques using Least Significant Bit in Grayscale Images and its Extension to Colour Images," *J. Sci. Res. Rep.*, vol. 8, no. 4, pp. 1–10, 2015.
- [11] N. K. Murthy, G. R. Rao, dan B. R. Reddy, "Image Steganography Using Discrete Cosine Transform Algorithm for Medical Images," dalam *Adv. Autom. Signal Process. Instrum. Control*, Singapore: Springer, 2021, pp. 219–230.
- [12] G. A. Simanungkalit, F. Pasaribu, dan E. L. Sinaga, "Discrete Wavelet Transform (DWT) Based Steganography Implementation," *J. Teknik Indones.*, vol. 12, no. 2, pp. 123–132, 2022.
- [13] X. Zhang, J. Wang, dan Y. Liu, "GAN-Based Steganography for Medical Image Security," *IEEE Access*, vol. 9, pp. 34200–34212, 2021.
- [14] M. Hasan, M. M. Islam, dan S. A. Al-Mamun, "CNN-Based Image Steganography: A New Approach for Data Hiding in Medical Images," *J. Med. Syst.*, vol. 44, no. 7, pp. 1–14, 2020.
- [15] H. Li, Y., dan Z. Li, "Particle Swarm Optimization Based Data Hiding in Medical Images for Secure Transmission," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1161–1173, 2020.
- [16] A. K. Singh dan S. Kumar, "Hybrid Optimization Algorithms for Secure Medical Image Steganography," *Multimed. Tools Appl.*, vol. 81, no. 6, pp. 8671–8690, 2022.
- [17] L., Y. Zhang, dan X. Zhao, "Advances in Machine Learning for Medical Image Security: A Review," *IEEE Rev. Biomed. Eng.*, vol. 14, pp. 163–176, 2021.
- [18] K. A. Zhang, A. Cuesta-Infante, L. Xu, dan K. Veeramachaneni, "SteganoGAN: High Capacity Image Steganography with GANs," *arXiv preprint arXiv:1901.03892*, 2019.
- [19] Y. Luo et al., "A robust medical image steganography approach based on particle swarm optimization and chaotic systems," *Soft Comput.*, vol. 26, pp. 12345–12360, 2022.