Penyisipan *Watermark* Menggunakan Metode LSB (*Least Significant Bit*) untuk Autentikasi Citra Medis

Albin Alveda
S1 Teknik Elektro, Fakultas Teknik, Universitas Negeri Surabaya
Email : albin.18010@mhs.unesa.ac.id

Lusia Rakhmawati, Rr. Hapsari Peni Agustin Tjahyaningtijas, Unit Three Kartini
S1 Teknik Elektro, Fakultas Teknik, Universitas Negeri Surabaya
Email : lusiarakhmawati@unesa.ac.id, hapsaripeni@unesa.ac.id, unitthree@unesa.ac.id

Abstrak

Kemajuan teknologi informasi telah meningkatkan kebutuhan akan keamanan dan integritas data medis, khususnya dalam konteks telemedis. Data medis, termasuk gambar medis, memerlukan mekanisme perlindungan untuk memastikan bahwa informasi yang dikirimkan tetap utuh dan tidak dapat diubah. Tujuan dari penelitian ini adalah untuk mengembangkan metode *watermarking* pada citra medis menggunakan teknologi *Least Significant Bit* (LSB) sebagai langkah menuju peningkatan autentikasi dan integritas citra medis. Metode LSB dipilih karena memungkinkan informasi tambahan (*watermark*) dimasukkan ke dalam citra digital tanpa mengurangi kualitas visual gambar. Penelitian ini meliputi beberapa tahap yang dimulai dengan pemilihan citra medis yang akan digunakan, pembuatan *watermark*, dan implementasi algoritma LSB untuk menyisipkan *watermark*. Eksperimen dilakukan untuk mengukur kualitas gambar setelah *watermarking* menggunakan metrik seperti *Peak Signal-to-Noise Ratio* (PSNR) dan *Mean Squared Error* (MSE). Selain itu, penelitian ini juga menguji ketahanan *watermark* terhadap berbagai serangan *noise*, seperti penambahan *Gaussian Noise*, *Speckle Noise*, dan *Salt & Pepper Noise*. Hasil penelitian menunjukkan bahwa metode LSB dapat menyisipkan *watermark* dengan kapasitas yang cukup besar tanpa mempengaruhi kualitas citra medis secara signifikan. Nilai PSNR dan MSE yang diperoleh menunjukkan bahwa kualitas citra medis tetap sangat baik bahkan setelah dilakukan *watermarking*. Selain itu, *watermark* yang disisipkan juga menunjukkan ketahanan yang sangat baik terhadap berbagai jenis serangan *noise*, membuktikan efektivitas metode ini dalam menjaga keamanan dan keandalan gambar medis. Oleh karena itu, metode LSB dapat digunakan sebagai solusi autentikasi dan perlindungan data dalam aplikasi telemedis.
Kata Kunci: *Watermarking*, *Least Significant Bit*, Citra Medis, Keamanan Data, Telemedis.

Abstract

Advances in information technology have increased the need for security and integrity of medical data, particularly in the context of telemedicine. Medical data, including medical *image*s, requires a protection mechanism to ensure that the transmitted information remains intact and cannot be altered. The purpose of this research is to develop a *watermarking* method on medical *image*s using *Least Significant Bit* (LSB) technology as a step towards improving the authentication and integrity of medical *image*s. The LSB method was chosen because it allows additional information (*watermark*) to be inserted into a digital *image* without reducing the visual quality of the *image*. This research includes several stages starting with the selection of the medical *image* to be used, the creation of the *watermark*, and the implementation of the LSB algorithm to insert the *watermark*. Experiments are conducted to measure the *image* quality after *watermarking* using metrics such as Peak Signal-to-*Noise* Ratio (PSNR) and Mean Squared Error (MSE). In addition, this research also tests the *watermark*'s resistance to various *noise* attacks, such as the addition of *Gaussian Noise*, *Speckle Noise*, and *Salt* & *Pepper Noise*. The results show that the LSB method can insert a *watermark* with a large enough capacity without significantly affecting the quality of the medical *image*. The obtained PSNR and MSE values show that the quality of the medical *image* remains excellent even after *watermarking*. Moreover, the inserted *watermark* also shows excellent robustness against various types of *noise* attacks, proving the effectiveness of this method in maintaining the security and reliability of medical *image*s. Therefore, the LSB method can be used as an authentication and data protection solution in telemedicine applications.
Keywords: *Watermarking*, *Least Significant Bit*, Medical *Image*s, Data Security, Telemedicine.

PENDAHULUAN

Dalam era digital ini, teknologi informasi berkembang dengan pesat dan penggunaan telemedis menjadi semakin umum dalam layanan kesehatan. Telemedis memungkinkan pengiriman data medis, termasuk citra medis, melalui jaringan internet. Namun, data yang dikirim melalui internet rentan terhadap manipulasi dan penyalahgunaan. Oleh karena itu, keamanan dan integritas data medis menjadi isu yang sangat penting. Salah satu

cara untuk memastikan keaslian dan integritas citra medis adalah dengan menyisipkan *watermark* digital ke dalam citra tersebut. *Watermark* ini berfungsi sebagai tanda pengenal yang dapat digunakan untuk memverifikasi keaslian citra medis (Gunawan dan Setiawan, 2022).

Penggunaan telemedis membawa berbagai tantangan, salah satunya adalah keamanan data medis yang dikirimkan melalui jaringan. Informasi medis merupakan informasi yang sangat sensitif dan memerlukan perlindungan yang tinggi terhadap integritas dan kerahasiaannya. Untuk mencegah informasi pasien dan gambar medis dirusak, *watermarking* dapat digunakan untuk menyembunyikan *Electronic Patient Record* (EPR) di dalam gambar medis, sehingga mencegah penyerang mengubah citra medis atau informasi pasien dengan mudah (Rahardjo, 2019).

Penelitian ini berfokus pada pengembangan metode penyisipan *watermark* yang efektif dan *imperceptible* pada citra medis menggunakan teknik *Least Significant Bit* (LSB). Teknik ini memanfaatkan bit terakhir pada setiap piksel citra untuk menyimpan bit-bit *watermark*, sehingga *watermark* dapat disembunyikan tanpa mengganggu informasi diagnostik yang penting. Metode ini juga memungkinkan penyisipan *watermark* dengan kapasitas yang cukup besar, karena setiap piksel citra dapat menyimpan beberapa bit *watermark* (Simbolon, 2021).

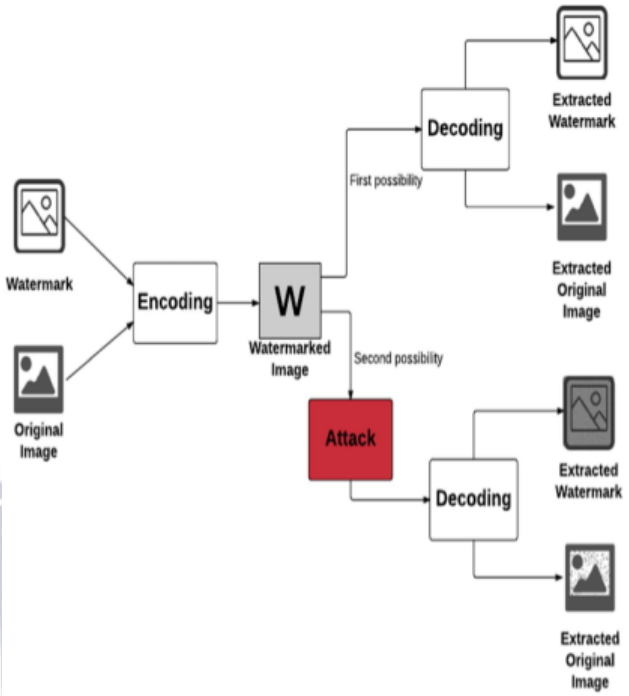
Tujuan penelitian ini adalah untuk mengembangkan dan menguji metode penyisipan *watermark* pada citra medis menggunakan teknik LSB. Penelitian ini juga bertujuan untuk mengevaluasi ketahanan *watermark* terhadap berbagai jenis serangan *noise*, seperti *Gaussian Noise*, *Speckle Noise*, dan *Salt & Pepper Noise*, serta memastikan bahwa *watermark* tetap dapat diekstraksi dengan baik meskipun ada penurunan kualitas citra akibat *noise attack* (Khilmawan dan Riadi, 2018).

Kajian teoretik dalam penelitian ini mencakup konsep dasar citra digital, teknik-teknik penyisipan *watermark*, serta metode *Least Significant Bit* (LSB) dan *Discrete Wavelet Transform* (DWT) (Fathiha, 2021). Metode LSB dipilih karena kemampuannya untuk menyisipkan *watermark* secara *imperceptible* tanpa mengurangi kualitas visual citra secara signifikan. Selain itu, penelitian-penelitian sebelumnya menunjukkan bahwa teknik *watermarking*, termasuk penggunaan tanda tangan digital yang disisipkan sebagai *watermark*, dapat meningkatkan keamanan dan kepercayaan dalam sistem telemedis (Guo dkk., 2018).

KAJIAN PUSTAKA

Watermarking

Watermarking adalah teknik yang digunakan untuk menyisipkan informasi tersembunyi ke dalam media digital seperti gambar, audio, video, atau dokumen teks. Tujuan utama *watermarking* adalah untuk melindungi hak cipta, memberikan autentikasi, dan menjaga integritas data. Dalam konteks citra digital, *watermarking* menjadi penting terutama untuk aplikasi di bidang keamanan digital dan manajemen hak digital (Nyeem dkk., 2012).



Gambar 1. Kerangka umum *watermarking* citra digital (Sumber Fkirin dkk., 2021)

Watermarking pada citra digital dapat dikategorikan menjadi dua jenis utama berdasarkan domain tempat *watermark* disisipkan: teknik domain spatial dan teknik domain frekuensi. Teknik domain spatial menyisipkan *watermark* langsung ke dalam piksel citra, dengan metode paling sederhana dan sering digunakan adalah teknik *Least Significant Bit* (LSB). Dalam teknik ini, bit-bit informasi *watermark* disisipkan pada bit-bit paling tidak signifikan dari piksel citra. Keunggulan teknik LSB terletak pada kesederhanaan dan kapasitas yang besar, namun teknik ini cenderung kurang tahan terhadap manipulasi. Meskipun sederhana, teknik LSB menghadapi tantangan dalam hal ketahanan terhadap serangan, karena *watermark* dapat dengan mudah dihilangkan atau dimodifikasi (Asikuzzaman dan Pickering, 2017). Di sisi lain, teknik domain frekuensi menyisipkan *watermark* ke dalam koefisien frekuensi citra setelah transformasi, seperti *Discrete Cosine Transform* (DCT) atau *Discrete Wavelet Transform* (DWT). *Watermark* yang disisipkan dalam domain frekuensi biasanya lebih tahan terhadap berbagai manipulasi dan kompresi dibandingkan dengan *watermark* yang disisipkan dalam domain spatial. Teknik-teknik seperti DCT dan DWT lebih unggul dalam hal ketahanan dan kehandalan karena *watermark* tersebar di seluruh citra, membuatnya lebih sulit untuk dihilangkan atau dimodifikasi tanpa merusak citra asli (Anand dan Singh, 2020).

Least Significant Bit

Least Significant Bit (LSB) merupakan salah satu teknik dalam Steganografi. LSB menambahkan bit data pesan yang akan disembunyikan di bit terakhir yang paling

cocok atau kurang berarti. Misalkan bit pada *image* dengan ukuran 3 piksel sebagai berikut:

$$\begin{pmatrix} 0011111 & 11101001 & 11001000 \\ 0011111 & 11001000 & 11101001 \\ 1100000 & 00100111 & 11101001 \end{pmatrix}$$

Gambar 2. Bit pada *image* dengan ukuran 3 piksel

Pesan yang akan disisipkan adalah karakter 'A' yang memiliki biner 10000001, *stego image* yang akan dihasilkan adalah:

$$\begin{pmatrix} 00111111 & 11101001\mathbf{0} & 11001000\mathbf{0} \\ 00111110 & 11001000\mathbf{0} & 11101001\mathbf{0} \\ 11000000 & 00100111\mathbf{1} & 11101001\mathbf{1} \end{pmatrix}$$

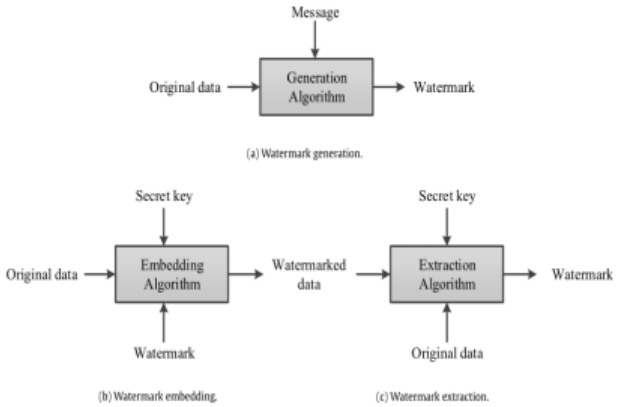
Gambar 3. Hasil stego *image*

Ada dua teknik yang dapat digunakan pada LSB, yaitu penyisipan secara sekuensial dan secara acak. Penyisipan sekuensial dilakukan berurutan sedangkan acak dilakukan dengan acak pada *image* dengan memasukan kata kunci (*stego key*) (Pakereng dkk., 2010).

Autentikasi Citra Medis

Autentikasi citra medis adalah proses untuk memastikan bahwa citra medis yang digunakan dalam diagnosis dan pengobatan adalah asli, utuh, dan belum dimodifikasi secara tidak sah. Autentikasi ini sangat penting dalam konteks medis karena integritas dan keakuratan citra medis adalah kunci untuk memberikan diagnosis yang tepat dan perawatan yang efektif. Ada beberapa metode dan teknologi yang digunakan untuk autentikasi citra medis, termasuk *watermarking* digital (Yuadi, 2020).

Metode autentikasi citra medis mencakup beberapa teknik, termasuk *watermarking* digital, kriptografi, dan teknologi *blockchain*. *Watermarking* digital adalah salah satu metode yang paling umum digunakan, di mana *watermark* yang berisi informasi penting seperti identitas pasien, waktu pengambilan gambar, dan tanda tangan digital disisipkan ke dalam citra. Setiap perubahan pada citra dapat dideteksi dengan membandingkan *watermark* yang diekstraksi dengan *watermark* asli, sehingga metode ini efektif karena *watermark* biasanya tidak mengganggu kualitas visual citra dan dapat bertahan terhadap berbagai manipulasi citra. Menurut penelitian oleh Qasim dkk. (2018), *watermark* yang disisipkan dapat mendeteksi setiap perubahan pada citra.



Gambar 4. Model dasar metode *digital watermarking*

Teknik kriptografi, seperti tanda tangan digital dan enkripsi, juga digunakan untuk autentikasi citra medis. Tanda tangan digital memastikan bahwa citra belum diubah sejak ditandatangani, sementara enkripsi melindungi data selama transmisi. Penelitian oleh Dey dkk. (2016) mengembangkan sistem autentikasi berbasis kriptografi untuk citra medis dalam lingkungan telemedicine, menunjukkan peningkatan dalam keamanan dan kepercayaan. Selain itu, teknologi *blockchain* menawarkan solusi baru untuk autentikasi data medis dengan menyediakan catatan transaksi yang tidak dapat diubah dan diverifikasi secara independen. Setiap perubahan pada data medis dicatat dalam *blockchain*, memastikan transparansi dan integritas data. Penggunaan *blockchain* dalam autentikasi data medis dapat meningkatkan keamanan dan kepercayaan terhadap data yang digunakan dalam diagnosis medis, seperti yang diungkapkan oleh Ahmed (2017).

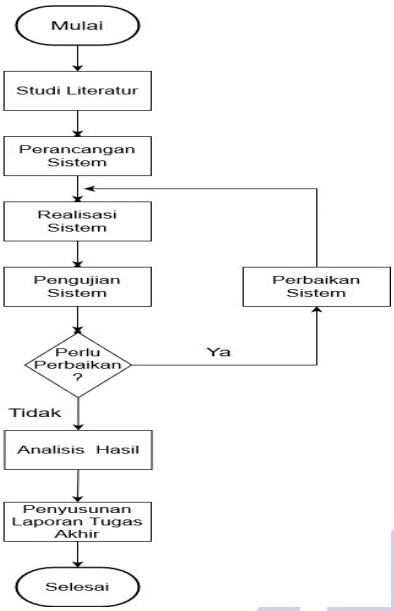
METODE

Pendekatan Penelitian

Penelitian ini menggunakan metode eksperimental untuk mengembangkan dan menguji efektivitas metode penyisipan *watermark* menggunakan teknik LSB (*Least Significant Bit*) pada citra medis. Proses penelitian dimulai dengan pengumpulan dataset citra medis yang relevan, seperti citra MRI atau CT scan, yang kemudian akan digunakan sebagai objek penelitian. Setiap citra akan melalui tahap pra-pemrosesan untuk memastikan keseragaman dalam hal resolusi dan format.

Perancangan Penelitian

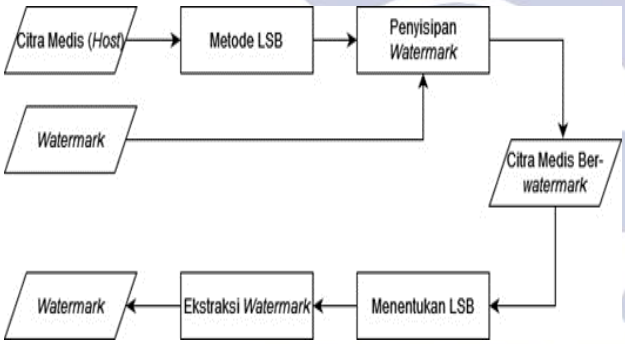
Umumnya, penelitian disusun dalam beberapa fase. Tahapan-tahapan tersebut dibagi menjadi tinjauan literatur dan kemudian dikembangkan perancangan sistem sehingga perangkat lunak dapat dirancang dalam MATLAB. Berikut ini adalah bagian penelitian dari tahap awal hingga tahap akhir. Tahap desain penelitian dijelaskan pada Gambar 5.



Gambar 5. Flowchart langkah-langkah penelitian

Desain Sistem

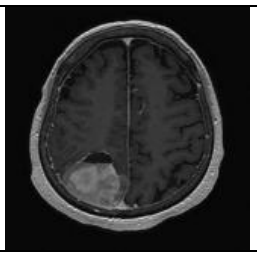
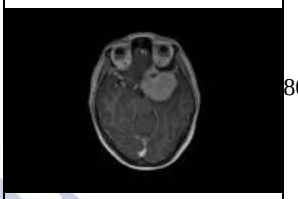
Sistem dirancang untuk dapat melakukan proses penyisipan *watermark* ke dalam sebuah citra medis kemudian mengekstraksi *watermark* tersebut. Sistem perangkat lunak *watermark* ini akan melakukan proses penyisipan dan pengekstrakan *watermark* pada citra medis menggunakan 3 inputan, yaitu citra medis yang berupa citra *grayscale* dengan format JPEG (.jpeg) sebagai citra *host* dan *watermark* yang berupa citra logo dengan format PNG (.png) dan data teks dengan format TXT (.txt). Secara umum arsitektur sistem yang dibangun pada proses *watermarking* dapat dilihat pada Gambar 6.



Gambar 6. Arsitektur *proses watermarking*

Untuk citra medis yang akan diuji adalah 3 buah citra *grayscale* tumor otak seperti yang ditampilkan pada Tabel 1.

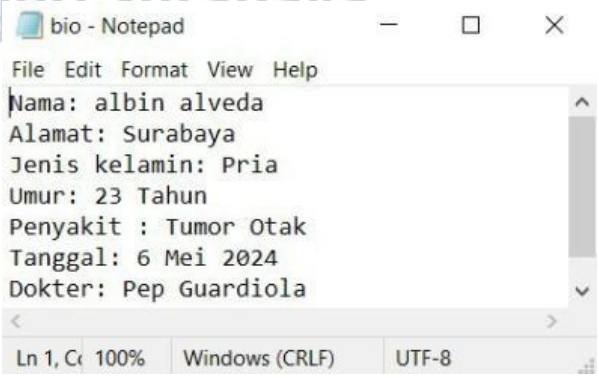
Tabel 1. Citra Medis

Nama File	Citra Medis	Dimensi	Format
CM1		512 x 512 piksel	jpeg
CM2		800 x 529 piksel	jpeg
CM3		475 x 300 piksel	jpeg

Gambar logo yang digunakan sebagai *watermark* adalah citra RGB 24 bit dengan format PNG (*.png) berukuran 200 x 200 piksel seperti yang ditampilkan pada Gambar 7.

Gambar 7. Logo *watermark*

File teks (*.txt) yang digunakan sebagai *watermark* berisi 22 karakter yang ditunjukkan pada Gambar 8.



Gambar 8. Teks *watermark*

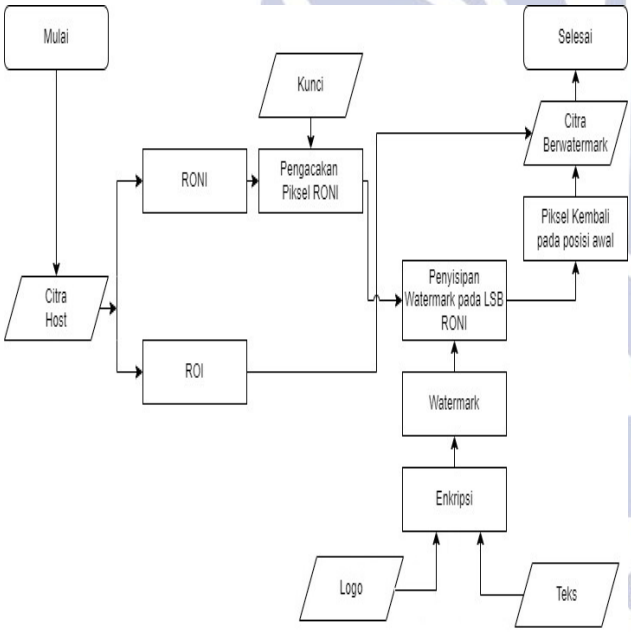
Ukuran *watermark* yang dihasilkan dan diterapkan dalam pengujian simulasi ini ditunjukkan pada Tabel 2.

Tabel 2. Ukuran dan Jenis Setiap *Watermark*

Watermark	Ukuran	Konversi Biner	Total (bit)
Logo	64x64 (*grey*)	4096 (bitmap)	4096
Teks	22 (*char*)	22 x 8	176

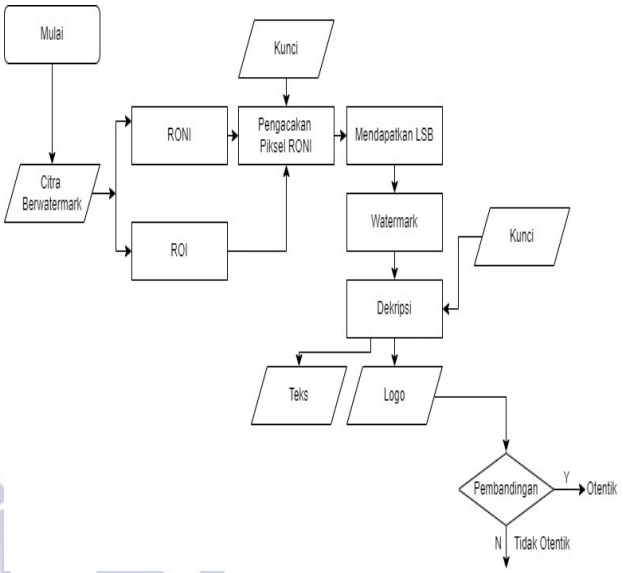
Rancang Bangun Perangkat Lunak

Sistem *watermarking* yang akan dijelaskan bertujuan untuk membangun suatu sistem pada citra digital yang efisien. Dalam sistem yang diusulkan, selama fase penyisipan, *watermark* dibuat dari dua entitas yang berbeda. *Watermark* ini kemudian disematkan pada LSB RONI dari gambar asli menggunakan metode yang diusulkan. *Watermark* yang digunakan adalah informasi yang dapat digunakan untuk autentikasi, seperti identitas pasien dan logo institusi medis. Penyisipan *watermark* dilakukan dengan mengubah bit paling tidak signifikan dari setiap piksel dalam citra medis, sehingga *watermark* dapat disisipkan tanpa merusak kualitas visual citra secara signifikan (Gaata dan Al-Hassani, 2022).



Gambar 9. Proses penyisipan *watermark*

Pada tahap ekstraksi, *watermark* yang telah disematkan akan diekstraksi, dengan proses ini sebagai kebalikan dari penyisipan. Logo yang diekstraksi kemudian dibandingkan dengan logo yang telah diketahui oleh detektor untuk otentikasi subjektif. Untuk otentikasi objektif, nilai PSNR dihitung seperti pada saat penyisipan dan dibandingkan dengan citra yang ber-*watermark* untuk memverifikasi integritas gambar (Dey dkk., 2016).



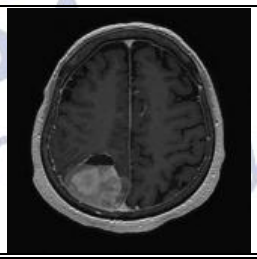
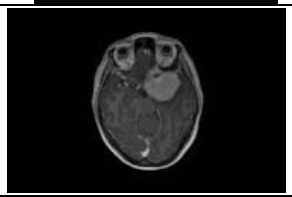
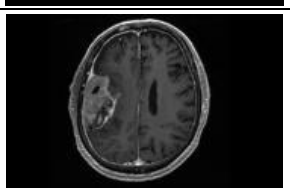
Gambar 10. Proses pengekstrakan *watermark*

HASIL DAN PEMBAHASAN

Hasil Uji Penyisipan *Watermark*

Pengujian sistem *watermarking* yang telah dirancang untuk autentikasi citra medis dilakukan dengan cara menyisipkan setiap bit dari *watermark*, yang berupa logo dan teks, ke dalam bit LSB dari area RONI (Region of Non-Interest) pada citra medis. Proses ini menghasilkan citra medis ber-*watermark*. Pengujian sistem penyisipan perangkat lunak ini dikatakan berhasil apabila proses penyisipan berhasil dilakukan. PSNR dan MSE digunakan sebagai metrik kualitas untuk mengevaluasi seberapa baik *watermark* disisipkan dan diekstrak dari citra medis. Hasil perhitungan MSE dan PSNR penyisipan *watermark* ditunjukkan pada Tabel 3.

Tabel 3. Hasil Uji Penyisipan *Watermark*

Citra Ber-*watermark*	MSE	PSNR
	0,261	53,99
	0,691	49,77
	0,163	54,04

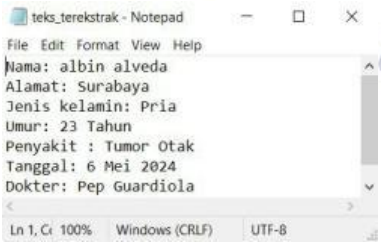
Dari hasil uji perhitungan nilai kualitas citra pada penyisipan *watermark*, degradasi yang terjadi pada citra yang diberi *watermark* dibandingkan dengan citra aslinya dievaluasi menggunakan metrik rasio sinyal-ke-*noise* (PSNR) dan mean square error (MSE). Berdasarkan perhitungan pada citra medis ber-*watermark*, ditemukan bahwa nilai MSE antara citra medis asli dengan citra medis ber-*watermark* hampir mendekati nol dan nilai kualitas citra (PSNR) medis ber- *watermark* besar. Dari hasil ini, dapat diketahui bahwa proses penyisipan *watermark* mengalami sedikit perubahan. Penilaian dari hasil perhitungan menunjukkan bahwa kualitas citra setelah proses penyisipan tidak mengalami perubahan yang signifikan. Hal ini dibuktikan dengan nilai MSE yang mendekati nol dan nilai PSNR yang lebih besar dari 30 dB, yang menunjukkan bahwa kualitas citra medis ber-*watermark* memiliki hasil yang bagus.

Hasil Uji Pengekstrakan *Watermark*

Pengujian proses ekstraksi adalah kebalikan dari proses penyematan. Karena skema yang diusulkan bersifat blind, tidak diperlukan gambar asli untuk mengekstrak *watermark* yang disisipkan. Pengujian sistem pengekstrakan perangkat lunak ini dikatakan berhasil apabila proses pengekstrakan berhasil dilakukan. Hasil dari proses ekstraksi *watermark* ditampilkan pada Gambar 11. dan Gambar 12.

Gambar 11. Citra *watermark* hasil pengekstrakan citra medis ber-*watermark*

Citra logo *watermark* yang dihasilkan dari proses pengekstrakan adalah citra biner 1 bit dengan format PNG (.png) berukuran 64 x 64 piksel.



Gambar 12. Teks *watermark* hasil pengekstrakan citra medis ber-*watermark*

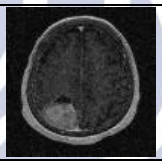
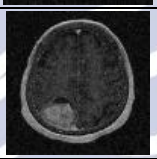
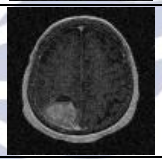
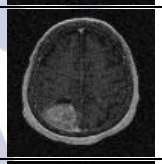
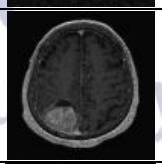
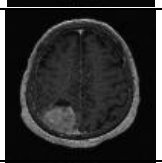
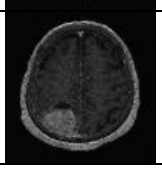
Teks *watermark* yang dihasilkan dari proses pengekstrakan adalah file teks (*.txt) yang berisi 22 karakter.

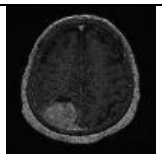
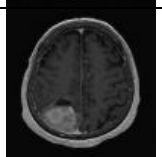
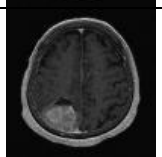
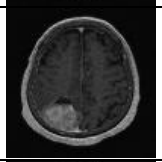
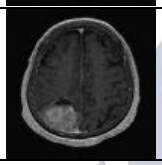
Hasil Uji *Noise* Attack terhadap *Watermark*

Dalam pengujian pengaruh *noise* attack terhadap *watermark*, citra ber-*watermark* mengalami serangan *noise* berupa *gaussian*, *speckle*, dan *salt* & *pepper*. Serangan ini diterapkan pada citra medis ber-*watermark*, kemudian dilakukan deteksi dan ekstraksi *watermark* yang telah disisipkan.

Pada eksperimen ini, citra medis ber-*watermark* yang digunakan adalah hasil dari CM1.jpeg dengan nama file CB1.png, memiliki dimensi 512x512 piksel, dan telah disisipi *watermark* logo_unesa.png dengan dimensi 200x200 piksel. Citra medis ini kemudian diberikan *noise* attack yang terdiri dari *Gaussian Noise*, *Speckle Noise*, dan *Salt* & *Pepper Noise* dengan berbagai tingkat presentase. Hasil dari pemberian *noise* attack pada citra medis ber-*watermark* disajikan dalam Tabel 4.

Tabel 4. Hasil Uji *Noise* Attack pada Citra Medis Ber-*watermark*

Jenis Serangan	Citra Hasil Serangan	Hasil Ekstraksi	MSE	PSNR
Gaussian Noise 5%			40,33	32,53
Gaussian Noise 10%			48,97	31,48
Gaussian Noise 15%			53,33	30,90
Gaussian Noise 20%			56,27	30,66
Speckle Noise 5%			8,342	38,95
Speckle Noise 10%			16,66	35,95
Speckle Noise 15%			24,92	34,20

Speckle Noise 20%			33,23	32,95
Salt & Pepper Noise 5%			12,47	37,21
Salt & Pepper Noise 10%			19,49	35,27
Salt & Pepper Noise 15%			24,93	34,20
Salt & Pepper Noise 20%			29,25	33,50

Inspeksi visual digunakan sebagai metode autentikasi subjektif. Pada Tabel 4.4, beberapa manipulasi citra dilakukan pada citra yang memiliki *watermark* menggunakan perangkat lunak MATLAB. Pertama, *Gaussian Noise*, dengan bertambahnya tingkat *noise* dari 5% hingga 20%, kualitas visual citra semakin menurun. Pada tingkat 5%, citra masih cukup jelas meskipun ada sedikit butiran *noise* yang terlihat. Namun, pada tingkat 20%, *noise* menjadi sangat dominan, menyebabkan penurunan signifikan dalam kualitas visual dan detail citra. Kedua, *Speckle Noise*, serangan *speckle noise* menghasilkan tekstur granular yang lebih terlihat pada citra. Pada tingkat 5%, efek *speckle noise* mulai terlihat tetapi masih memungkinkan untuk interpretasi visual yang baik. Namun, pada tingkat 20%, citra menjadi sangat berbutir sehingga mengganggu penglihatan detail yang lebih halus. Ketiga, *Salt* & *Pepper Noise*, serangan ini menghasilkan titik-titik putih dan hitam acak pada citra. Pada tingkat 5%, titik-titik tersebut cukup terlihat namun masih memungkinkan untuk melihat keseluruhan citra. Pada tingkat 20%, distribusi titik-titik *salt* & *pepper* menjadi sangat padat sehingga kualitas visual citra sangat terganggu.

Untuk analisis objektif, parameter MSE dan PSNR digunakan untuk melakukan autentikasi dengan membandingkan citra ber-*watermark* yang asli dan citra ber- *watermark* yang telah dimanipulasi. Berdasarkan hasil perhitungan yang tercantum dalam Tabel 4.3, nilai Mean Squared Error (MSE) dan Peak Signal-to-*Noise* Ratio (PSNR) untuk masing-masing jenis serangan dan tingkat persentase *noise* dianalisis. Pada *Gaussian Noise*, pada tingkat 5%, nilai MSE adalah 40,33 dan PSNR adalah 32,53. Pada tingkat 20%, nilai MSE meningkat menjadi 56,27 dan PSNR menurun menjadi 30,66. Hasil ini menunjukkan bahwa semakin tinggi tingkat *Gaussian Noise* yang diterapkan, semakin besar kerusakan pada citra, ditunjukkan oleh nilai MSE yang meningkat, dan semakin rendah kualitas citra, ditunjukkan oleh nilai PSNR yang menurun. Pada *Speckle Noise*, pada tingkat 5%, nilai MSE adalah 8,342 dan PSNR adalah 38,95. Pada tingkat 20%, nilai MSE adalah 33,23 dan PSNR adalah 32,95. Meskipun nilai MSE untuk *speckle noise* lebih bervariasi, pola umum tetap menunjukkan bahwa peningkatan *speckle noise* menurunkan kualitas citra. Untuk *Salt* & *Pepper Noise*, pada tingkat 5%, nilai MSE adalah 12,47 dan PSNR adalah 37,21. Pada tingkat 20%, nilai MSE adalah 29,25 dan PSNR adalah 33,50. *Salt* & *Pepper Noise* juga mengikuti hasil yang sama, dengan peningkatan tingkat *noise* yang menyebabkan nilai MSE lebih tinggi dan PSNR lebih rendah.

PENUTUP

Simpulan

Penelitian ini menunjukkan bahwa metode *Least Significant Bit* (LSB) efektif untuk melakukan *watermarking* pada citra medis tanpa mengurangi kualitas visual. *Watermark* yang disisipkan tidak terlihat dengan mata telanjang, sehingga gambar aslinya tidak dapat terdeteksi. Mengekstraksi *watermark* dari gambar yang dimanipulasi menunjukkan bahwa *watermark* dapat berhasil diekstraksi bahkan dengan adanya *noise* seperti *noise gaussian*, *noise speckle*, dan *noise salt & pepper*. Hasil pengujian menunjukkan bahwa kualitas gambar yang diberi *watermark* mengalami penurunan. Hal ini dapat diukur dengan peningkatan nilai MSE (*Mean Squared Error*) dan penurunan nilai PSNR (*Peak Signal-to-Noise Ratio*). Namun, *watermark* masih memungkinkan untuk diekstrak dengan presisi tinggi. Oleh karena itu, metode LSB tahan terhadap berbagai jenis *noise* dan efektif dalam menjaga integritas dan keaslian gambar medis dalam aplikasi telemedis, menjamin keamanan dan keandalan data medis yang dikirimkan melalui jaringan Internet.

Saran

Evaluasi kualitas citra dengan menggunakan parameter MSE dan PSNR menunjukkan adanya perbedaan yang signifikan setelah serangan. Penelitian lebih lanjut dapat dilakukan untuk mengeksplorasi parameter evaluasi kualitas citra lainnya atau bahkan mengembangkan metode baru yang lebih sensitif terhadap perubahan kualitas citra setelah serangan.

DAFTAR PUSTAKA

Anand, Ashima dan Singh, Amit Kumar. (2020). *Watermarking techniques for medical data authentication: a survey*. Multimedia Tools and Applications.

Asikuzzaman, Md dan Pickering, Mark R. (2017). *An Overview of Digital Video Watermarking*. IEEE Transactions on Circuits and Systems for Video Technology, 1–1.

Dey, Nilanjan, Ashour, Amira S., dan Borra, Surekha. (2017). *Classification and authentication of*

biomedical data using machine learning techniques. Biomedical Information Technology, Academic Press, 375-394.

Fathiha, Verryna Adzillatul. (2021). *Implementasi Teknik Watermarking menggunakan metode discrete wavelet transform (DWT) dan singular value decomposition (SVD) pada citra digital*. Jurnal Ilmiah Teknologi Informasi Asia, 14(2), 125.

Fkirin, Alaa, Attiya, Gamal, dan El-Sayed, Ayman. (2021). *Two-level security approach combining watermarking and encryption for securing critical colored images*. Optical and Quantum Electronics, 53(6).

Gaata, Methaq Talib dan Al-Hassani, Dr. Mustafa. (2022). *Authentication and integrity of E-documents based on zero-watermarking method*. Webology, 19(1), 5058–5067.

Gunawan, D. dan Setiawan, H. (2022). *Convolutional neural network Dalam Citra Medis*. KONSTELASI: Konvergensi Teknologi Dan Sistem Informasi, 2(2).

Guo, Yijia, Su, Xinghua, dan Li, Yangyang. (2018). *A robust medical image watermarking technique for telemedicine based on DWT and LSB*. IEEE Access, 6, 43366- 43374.

Khilmawan, Muhammad Rizqi dan Riadi, Aditya Akbar. (2018). *Implementasi Pengurangan Noise pada citra Tulang Menggunakan metode median filter dan gaussian filter*. JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika), 3(2).

Nyeem, Hussain, Boles, Wageeh W., dan Boyd, Colin. (2012). *A review of Medical Image Watermarking requirements for teleradiology*. Journal of Digital Imaging, 26(2), 326–343.

Pakereng, M. A. Ineke, Beeh, Yos Richard, dan Endrawan, Sonny. (2010). *Perbandingan Steganografi metode spread spectrum Dan Least Significant Bit (LSB) Antara Waktu proses Dan Ukuran File gambar*. Jurnal Informatika, 6(2).

Qasim, Asaad F., Meziane, Farid, dan Aspin, Rob. (2018). *Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review*. Computer Science Review, 27, 45–60.

Rahardjo, Budhi. (2019). *Implementasi Kerahasiaan Informasi medis Dalam Rekam Medis Pasien (Studi Kasus di Rumah Sakit Islam at-tin husada ngawi jawa Timur)*. Jurnal Manajemen Informasi Dan Administrasi Kesehatan (JMIAK), 2(1).

Simbolon, Buha Johannes. (2021). *Steganografi penyisipan Pesan Pada file citra Dengan Menggunakan metode LSB (Least Significant Bit)*. Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI), 4(1), 1–6.

Yuadi, Firzanatusalma Rafiza. (2020). *Forensik Digital Berdasarkan citra Mikroskop Untuk Autentikasi ARSIP tercetak*. Khazanah: Jurnal Pengembangan Kearsipan, 13(2), 157.