Masuk: 25 Agustus 2025 | Revisi: 27 September 2025 | Diterima: 29 Oktober 2025
e-SSIN: 3031-3082; DOI: https://doi.org/10.26618/hqt4ec35

JUMPTECH

Penerapan *Watermark* Tak Terlihat pada Materi Pembelajaran Digital Menggunakan QR *Code* dan *Least Significant Bit*

Arikal Khairat[1] | Titin Wahyuni[*2] | Muhyiddin AM Hayat[2]

1 Mahasiswa Program Studi Informatika, Fakultas Teknik, Universitas Muhammadiyah Makassar, Indonesia.
Email: 105841108421@student.unismuh.ac.id

2 Program Studi Informatika, Fakultas Teknik, Universitas Muhammadiyah Makassar, Indonesia.
Email: titinwahyuni@unismuh.ac.id
muhyiddin@unismuh.ac.id

Korespondensi:
*Titin Wahyuni
titinwahyuni@unismuh.ac.id

ABSTRAK

Perkembangan bahan ajar digital meningkatkan risiko pelanggaran hak cipta dan pemalsuan konten, sehingga diperlukan mekanisme perlindungan yang tidak mengganggu tampilan visual. Penelitian ini mengimplementasikan *watermarking* tak terlihat dengan menggabungkan *Quick Response* (*QR*) *Code* sebagai pembawa informasi dan *steganografi Least Significant Bit* (LSB) sebagai teknik penyisipan pada citra yang terdapat dalam dokumen. Sistem dikembangkan berbasis web dengan tiga modul utama: pembuatan *QR Code*, penyisipan *watermark*, dan validasi dokumen. Evaluasi dilakukan pada 10 dokumen berformat DOCX dan PDF dengan total 169 gambar. Kinerja *imperceptibility* diukur menggunakan *Peak Signal-to-Noise Ratio* (PSNR) dan *Mean Squared Error* (MSE). Hasil pengujian menunjukkan PSNR berada pada rentang 55,4–67,1 dB dengan MSE sangat rendah (0,02–0,19), menandakan kualitas visual citra tetap terjaga. Selain itu, seluruh *watermark* berhasil diekstraksi (100%) dan *QR Code* dapat dipindai tanpa kegagalan. Validasi integritas *payload* secara opsional menggunakan CRC32 terbukti membantu memastikan keutuhan data yang disisipkan. Temuan ini menunjukkan bahwa kombinasi *QR Code* dan LSB efektif, andal, dan efisien untuk melindungi bahan ajar digital dari penyalahgunaan tanpa menurunkan kualitas visual.

Kata Kunci: *Watermarking* tak terlihat; *QR Code*; *steganografi*; *Least Significant Bit*; bahan ajar digital.

ABSTRACT

The growth of digital teaching materials increases the risk of copyright infringement and content tampering, requiring protection mechanisms that do not degrade visual quality. This study implements an invisible watermarking scheme by combining Quick Response (QR) Code as the information carrier and Least Significant Bit (LSB) steganography for embedding within images contained in documents. A web-based system was developed with three core modules: QR Code generation, watermark embedding, and document validation. The evaluation used 10 DOCX and PDF documents comprising 169 images. Imperceptibility was assessed using Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE). Experimental results indicate PSNR values of 55.4–67.1 dB with very low MSE (0.02–0.19), confirming that visual quality is preserved. All embedded watermarks were successfully extracted (100%), and the QR Codes remained fully scannable without failure. Optional payload integrity checking using CRC32 further ensured the correctness of embedded data. Overall, the proposed QR Code–LSB combination provides a reliable and efficient approach to protect digital teaching materials against misuse while maintaining visual fidelity.

Keywords:

Invisible watermarking; QR Code; steganography; Least Significant Bit; digital teaching materials.

1 | PENDAHULUAN

Penggunaan bahan ajar digital semakin meluas dalam dunia pendidikan seiring perkembangan teknologi informasi yang menawarkan kemudahan akses, interaktivitas, serta fleksibilitas distribusi. Modul elektronik, dokumen pembelajaran, ilustrasi, dan media visual kini menjadi bagian penting dalam proses pembelajaran modern. Namun, kemudahan tersebut juga meningkatkan risiko duplikasi, modifikasi ilegal, serta penyalahgunaan konten tanpa atribusi yang jelas, sehingga berpotensi merugikan pencipta dan menurunkan kredibilitas lembaga pendidikan (Wulandari, 2024).

Permasalahan bahan ajar digital tidak hanya berkaitan dengan pelanggaran hak cipta, tetapi juga menyentuh aspek keaslian dan integritas informasi. Dalam konteks akademik, materi pembelajaran yang dimodifikasi secara tidak sah dapat menyebabkan penyampaian informasi yang keliru kepada peserta didik. Oleh karena itu, perlindungan terhadap bahan ajar digital menjadi kebutuhan mendesak untuk menjamin keaslian dokumen dan menjaga kualitas pembelajaran (Fathanudien & Maharani, 2023).

Salah satu pendekatan yang dinilai efektif untuk mengatasi permasalahan tersebut adalah teknik *watermarking*, yaitu penyisipan identitas atau informasi hak cipta langsung ke dalam media digital. *Watermarking* terbagi menjadi dua jenis, yaitu *visible* dan in*visible*. *Visible watermarking* mudah dikenali, tetapi dapat mengganggu estetika dan kenyamanan pengguna. Sebaliknya, in*visible watermarking* tidak mengubah tampilan visual secara kasat mata, sehingga lebih sesuai diterapkan pada bahan ajar digital yang menuntut kualitas visual tetap terjaga (Gultom & Suhartana, 2023). Secara konseptual, *watermarking* juga dipahami sebagai teknik penyisipan informasi ke dalam data digital untuk tujuan proteksi hak cipta, autentikasi, dan pelacakan integritas data (WIDIYONO et al., 2021).

Metode *steganografi Least Significant Bit* (LSB) merupakan salah satu teknik yang paling banyak digunakan dalam *watermarking* dan penyembunyian data digital karena kesederhanaan algoritma serta kemampuannya menjaga kualitas media penampung. Penelitian Aditya Permana & Amma (2022) menunjukkan bahwa metode LSB mampu menyisipkan data dengan tingkat *imperceptibility* yang tinggi dan distorsi visual yang minimal. Fleksibilitas metode ini juga dibuktikan melalui penerapannya pada berbagai media digital, termasuk citra dan audio (Akmal et al., 2023). Pada level prinsip, LSB bekerja dengan mengganti bit terakhir pada piksel (yang kontribusinya paling kecil terhadap nilai piksel), sehingga perubahan umumnya tidak terdeteksi oleh penglihatan manusia (Purbaningrum et al., 2023). Selain itu, penerapan LSB pada *watermarking* juga banyak digunakan untuk kebutuhan otentikasi pada citra digital, termasuk dalam skenario citra yang berpotensi mengalami manipulasi, sehingga metode ini dinilai relevan sebagai dasar penyisipan *watermark* tak terlihat (Fadlika Satria et al., 2021)

Sebagai muatan *watermark* (*payload*), *QR Code* dipilih karena kemampuannya menyimpan informasi identitas dalam format ringkas dan mudah diverifikasi, sekaligus relevan untuk kebutuhan proteksi dan keamanan data berbasis *QR Code* (Harits M et al., 2021). *QR Code* tidak hanya berfungsi sebagai penanda visual, tetapi juga dapat memuat metadata seperti identitas pembuat, kode dokumen, dan informasi verifikasi. Penelitian Alajmi et al. (2020) menunjukkan bahwa pesan terenkripsi dapat disisipkan ke dalam *QR Code* yang valid tanpa mengganggu fungsionalitas pemindaian, sementara studi lain menegaskan peran *QR Code* dalam sistem autentikasi dan verifikasi dokumen digital (Ferdiansyah et al., 2021).

Meskipun berbagai penelitian telah membahas metode LSB dan *QR Code* secara terpisah, penggabungan keduanya sebagai sistem perlindungan bahan ajar digital yang terintegrasi masih relatif jarang dikaji. Beberapa studi terkini mulai mengombinasikan *QR Code* dan LSB untuk pengamanan data, namun fokusnya belum secara spesifik diarahkan pada proteksi bahan ajar digital dalam konteks pendidikan (Putri Pebriani et al., 2025). Oleh karena itu, penelitian ini menawarkan nilai kebaruan dengan mengintegrasikan *QR Code* sebagai *payload* dan metode LSB sebagai teknik penyisipan dalam satu sistem *watermarking* tak terlihat.

Selain aspek penyisipan *watermark*, isu integritas data juga menjadi perhatian penting. Dokumen digital berpotensi mengalami perubahan selama proses distribusi, baik disengaja maupun tidak disengaja. Untuk memperkuat proses autentikasi, penelitian ini menambahkan validasi opsional menggunakan algoritma CRC32 sebagai mekanisme deteksi perubahan data. Sagala (2021) membuktikan bahwa CRC32 efektif dalam mendeteksi modifikasi pada citra digital, sehingga dapat berfungsi sebagai lapisan tambahan dalam menjaga keutuhan informasi.

Dari sisi praktis, pengembangan sistem *watermarking* berbasis *QR Code* dan metode LSB menawarkan solusi yang relatif mudah diimplementasikan oleh dosen maupun guru. Proses penyisipan *watermark* tidak memerlukan perangkat keras khusus atau keahlian teknis tingkat lanjut, sehingga dapat diterapkan secara luas dalam ekosistem pendidikan. Antarmuka berbasis web juga memudahkan pengguna dalam mengunggah dokumen, menyisipkan *watermark*, serta memvalidasi keaslian bahan ajar digital secara efisien (Faisal et al., 2020).

Perkembangan bahan ajar digital juga tidak dapat dilepaskan dari peningkatan kompetensi pendidik dalam memanfaatkan teknologi informasi. Jadi tidak hanya membuat bahan ajar digital, tetapi juga memastikan keamanan dan keaslian konten yang dihasilkan. Peningkatan kapasitas pendidik dalam mengembangkan bahan ajar digital telah menjadi fokus berbagai program pendidikan, namun aspek perlindungan konten sering kali belum menjadi perhatian utama

(Antika et al., 2022). Kondisi ini menunjukkan adanya kebutuhan akan sistem proteksi yang mudah diterapkan dan dapat diintegrasikan langsung ke dalam alur kerja pengembangan bahan ajar.

Dari perspektif teknis, pemahaman terhadap pengolahan citra digital menjadi fondasi penting dalam penerapan *steganografi* dan *watermarking*. Studi Devi & Rosyid (2022) menekankan bahwa penguasaan konsep dasar pengolahan citra, seperti representasi piksel dan manipulasi bit, sangat berpengaruh terhadap keberhasilan penyisipan data. Analisis histogram pada citra ber-*watermark* juga banyak digunakan untuk mengevaluasi perubahan distribusi piksel akibat proses penyisipan, sebagaimana ditunjukkan oleh Hasan et al. (2020), sehingga kualitas visual dan tingkat *imperceptibility* dapat diukur secara objektif.

Selain itu, pendekatan *watermarking* dan *steganografi* juga memiliki relevansi yang kuat dalam konteks sistem verifikasi dokumen digital Beberapa penelitian telah memanfaatkan *steganografi* LSB untuk verifikasi sertifikat dan dokumen resmi sebagai bukti keabsahan, yang menunjukkan bahwa teknik ini dapat diadaptasi untuk berbagai kebutuhan autentikasi (Nur Aqsal Aminullah et al., 2022). Dengan karakteristik bahan ajar digital yang serupa dengan dokumen resmi yakni mudah disalin dan didistribusikan pendekatan serupa dinilai relevan untuk diterapkan dalam dunia pendidikan sebagai upaya menjaga keaslian dan integritas materi pembelajaran.

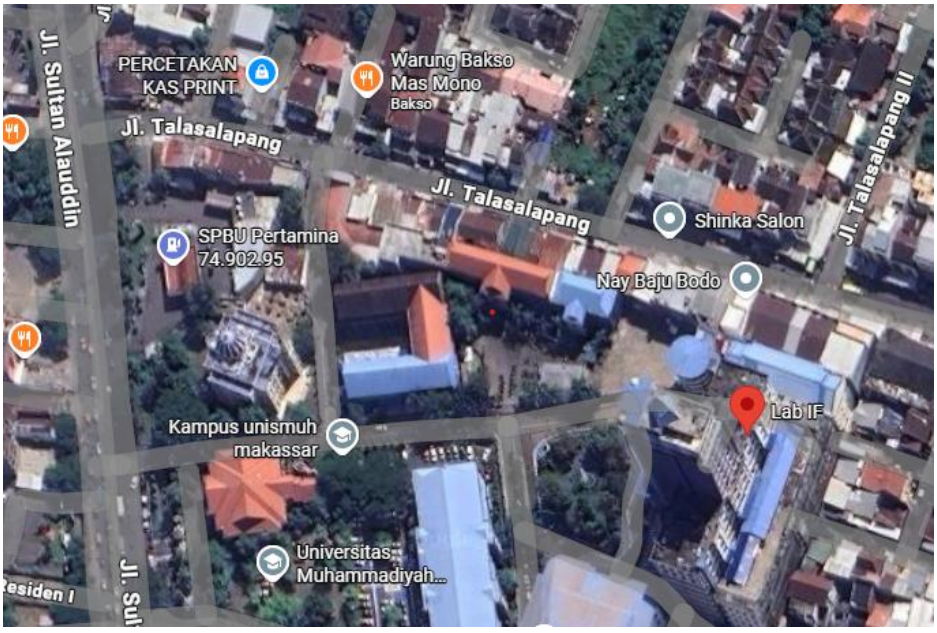
Dengan demikian, penelitian ini bertujuan untuk mengimplementasikan sistem *watermarking* tak terlihat berbasis *QR Code* dan metode LSB, serta mengevaluasi kinerjanya melalui pengujian *imperceptibility*, keberhasilan ekstraksi *watermark*, dan validasi integritas data menggunakan CRC32. Hasil penelitian diharapkan dapat memberikan kontribusi praktis bagi pendidik dan lembaga pendidikan dalam melindungi bahan ajar digital, sekaligus memperkuat budaya akademik yang menghargai karya intelektual.

2 | METODE

Metode penelitian ini dirancang untuk mengembangkan dan menguji sistem *watermarking* tak terlihat pada bahan ajar digital melalui integrasi *QR Code* sebagai informasi kepemilikan dan *steganografi* citra metode LSB sebagai teknik penyisipan. Pendekatan yang digunakan bersifat eksperimental berbasis pengembangan prototipe, dengan tahapan utama meliputi perancangan alur *embedding–extracting*, implementasi penyisipan *watermark* pada citra dalam dokumen, serta evaluasi hasil menggunakan pengujian keberhasilan ekstraksi dan pengukuran kualitas citra (MSE dan PSNR) untuk memastikan *watermark* tidak mengganggu tampilan namun tetap dapat dipulihkan secara akurat (Yanti & Budayawan, 2023).

2.1 | Lokasi Penelitian

Penelitian ini dilaksanakan di Laboratorium Informatika, Universitas Muhammadiyah Makassar, yang beralamat di Jl. Sultan Alauddin No.259, Gn. Sari, Kecamatan Rappocini, Kota Makassar, Sulawesi Selatan 90221**.** Lokasi penelitian ditampilkan pada **Gambar 1** dalam bentuk peta. Kegiatan penelitian berlangsung pada periode Juni hingga Agustus 2025.



GAMBAR 1 Peta Laboratorium Informatika Universitas Muhammadiyah Makassar

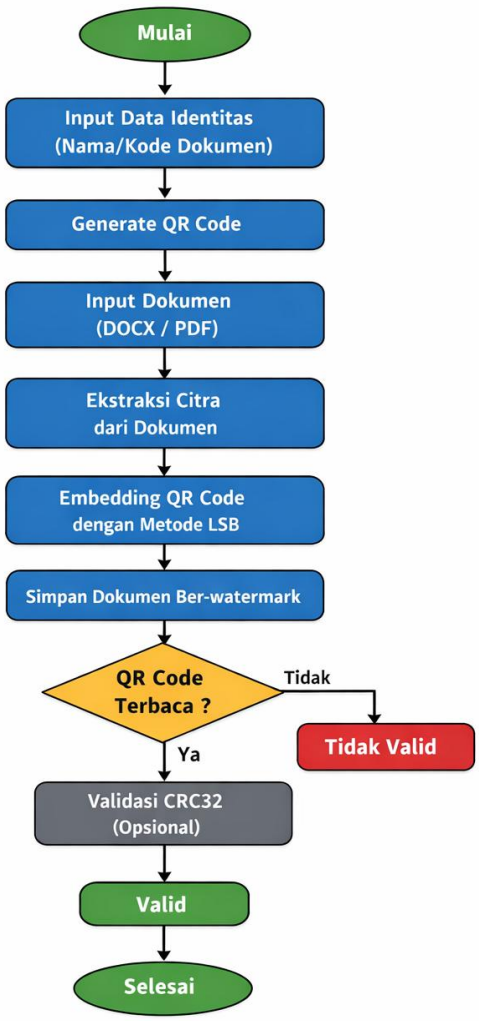
2.2 | Teknik Pengumpulan Data

Data penelitian dikumpulkan melalui pengumpulan bahan ajar digital yang digunakan sebagai objek uji dalam sistem *watermarking*. Bahan ajar tersebut diperoleh melalui dua sumber utama, yaitu guru secara langsung dan platform daring (internet). Bahan ajar yang dikumpulkan mencakup berbagai format dokumen digital yang umum digunakan dalam proses pembelajaran, seperti PDF dan DOCX. Seluruh file digital yang diperoleh dijadikan sebagai dataset pengujian dan digunakan pada proses penyisipan *watermark* serta pengujian kinerja sistem, termasuk keberhasilan ekstraksi dan kualitas citra hasil penyisipan.

2.3 | Perancangan Sistem

Rangkaian proses penelitian ini terdiri dari tiga tahap utama, yaitu *embedding*, *extraction*, dan validasi. Pengembangan dan pengujian sistem dilakukan secara komputasional menggunakan perangkat laptop dengan spesifikasi prosesor Intel® Celeron®, RAM 4 GB, dan SSD 512 GB, pada lingkungan kerja berbasis Linux Ubuntu. Implementasi sistem dikembangkan menggunakan Visual Studio Code sebagai text editor dan Python sebagai bahasa pemrograman utama.

Gambar 2 menunjukkan proses *watermarking* dokumen menggunakan *QR Code* dan metode LSB. Pengguna memasukkan identitas/kode dokumen, lalu sistem membuat *QR Code* dan menerima dokumen (DOCX/PDF). Sistem mengekstrak gambar dari dokumen, menyisipkan *QR Code* ke gambar dengan LSB, kemudian menyimpan dokumen ber-*watermark*. Terakhir, sistem mengecek apakah *QR Code* dapat dibaca; jika tidak terbaca maka dokumen dinyatakan tidak valid, sedangkan jika terbaca (opsional dicek CRC32) maka dokumen dinyatakan valid.



GAMBAR 2 Flowchart Perancangan Sistem

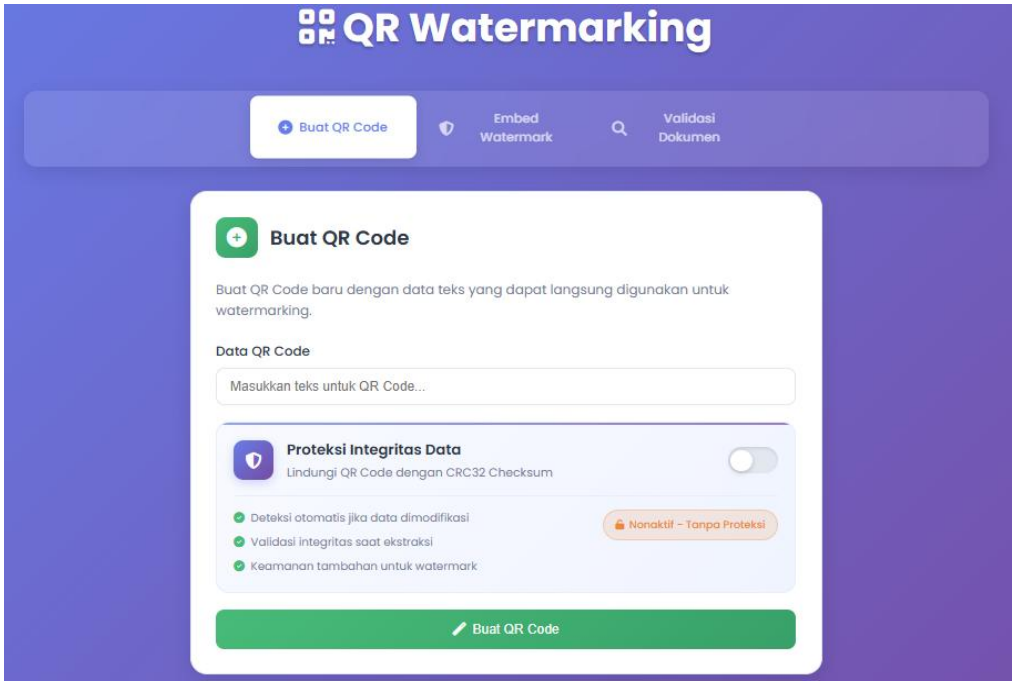
3 | HASIL

Penelitian ini menyajikan hasil implementasi sistem *watermarking* tak terlihat pada bahan ajar digital dengan mengintegrasikan *QR Code* sebagai identitas dokumen dan metode LSB sebagai teknik penyisipan pada citra. Hasil yang diperoleh menunjukkan

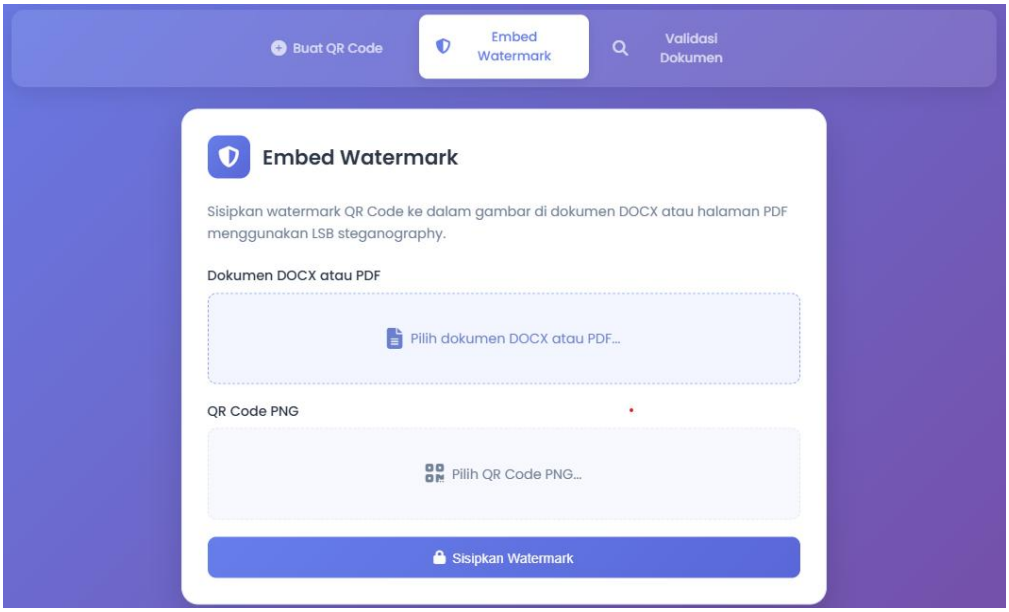
bahwa *watermark* dapat ditanamkan ke dalam dokumen (PDF/DOCX) melalui proses *embedding* dan diekstraksi kembali melalui proses *extraction* tanpa menimbulkan perubahan visual yang signifikan. Penyajian hasil dilakukan secara bertahap untuk menggambarkan keluaran sistem pada setiap proses, tingkat keberhasilan pembacaan *QR Code*, serta kualitas citra hasil penyisipan yang dievaluasi menggunakan parameter MSE dan PSNR, termasuk verifikasi tambahan menggunakan CRC32 untuk memastikan konsistensi data *watermark* yang dipulihkan.

3.1 | Implementasi Sistem

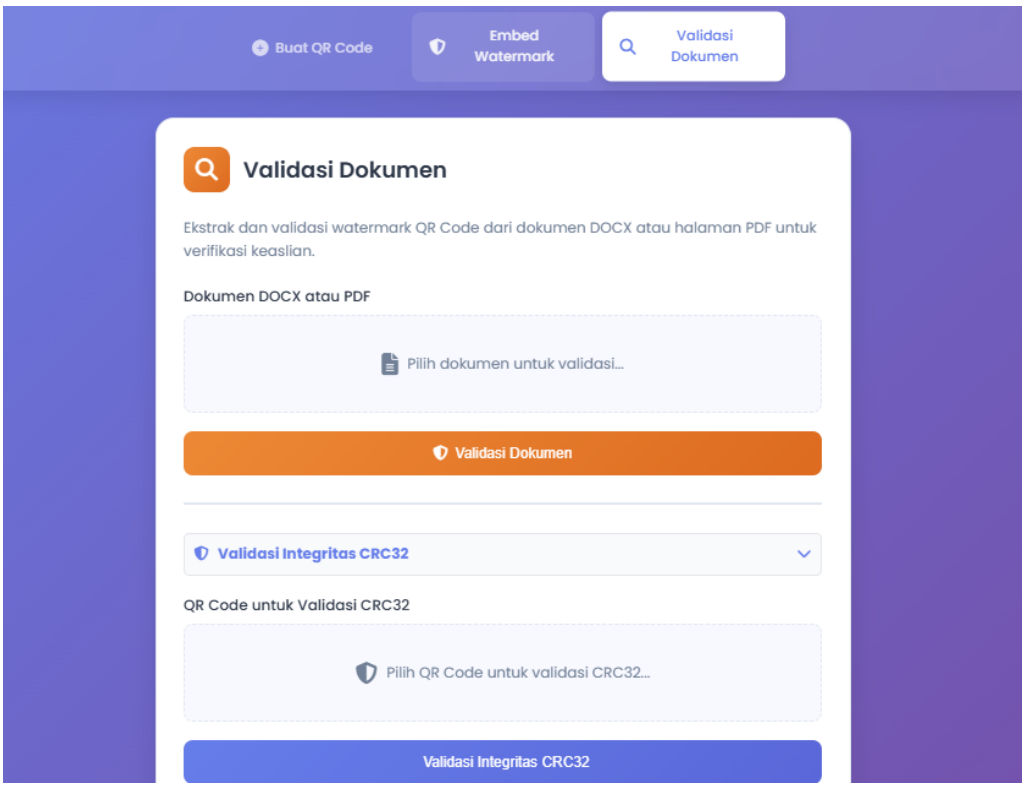
Sistem *watermarking* tak terlihat diimplementasikan dalam bentuk aplikasi berbasis web dengan tiga menu utama, yaitu *Generate QR Code*, *Embedding*, dan *Extraction*. Tampilan menu *Generate QR Code* ditunjukkan pada **Gambar 3**, yang berfungsi untuk mengubah teks identitas menjadi *QR Code* sebagai *payload*. Selanjutnya, proses penyisipan ditampilkan pada **Gambar 4** melalui menu *Embedding*, di mana *QR Code* disisipkan ke dalam citra penampung menggunakan metode *Least Significant Bit* (LSB) tanpa menimbulkan perubahan visual yang berarti. Tahap akhir ditampilkan pada **Gambar 5** melalui menu Validasi, yang berfungsi untuk mengekstraksi kembali *QR Code* dari dokumen hasil penyisipan guna dilakukan proses verifikasi; apabila fitur CRC32 diaktifkan, sistem akan menghitung nilai *checksum payload* untuk memastikan integritas data.



GAMBAR 3 Tampilan Menu *Generate* QR *Code*



GAMBAR 4 Tampilan Menu Penyisipan Watermark



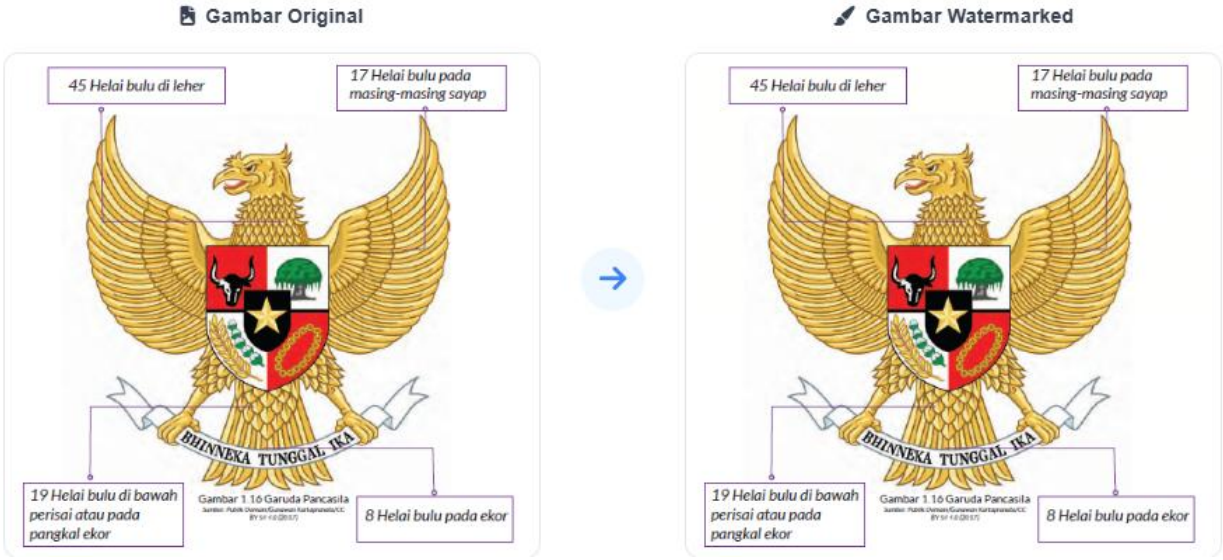
GAMBAR 5 Tampilan Menu Ekstraksi

3.2 | Hasil Pengujian

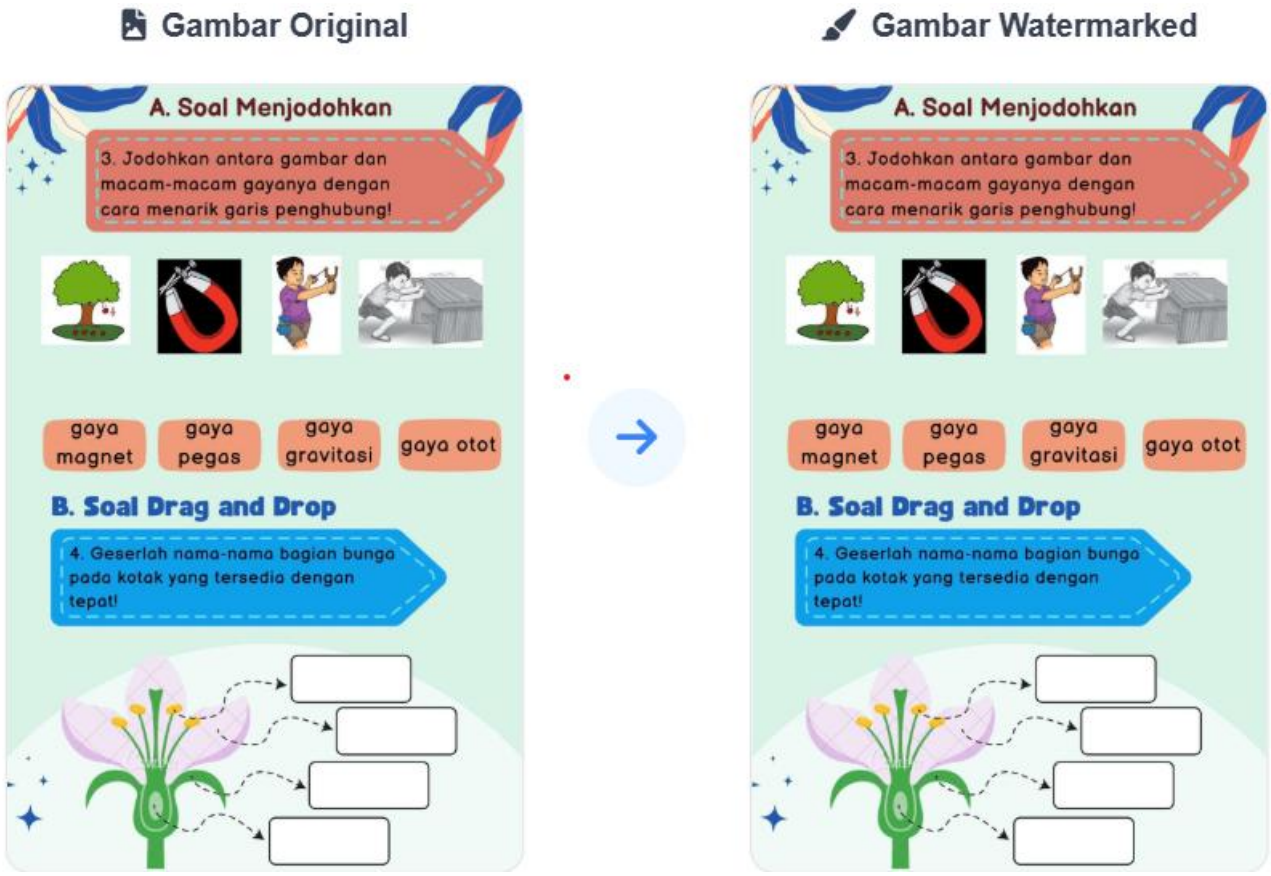
Pengujian dilakukan untuk menilai kinerja sistem *watermarking* yang dikembangkan, baik dari aspek kualitas visual dokumen maupun keberhasilan pemulihan *watermark*. Evaluasi mencakup uji *imperceptibility* untuk memastikan *watermark* tidak mengganggu tampilan, serta pengujian kuantitatif menggunakan parameter MSE dan PSNR sebagai indikator perubahan citra setelah proses penyisipan. Nilai MSE yang rendah dan PSNR yang tinggi mengindikasikan tingkat *imperceptibility* yang baik (Alveda et al., 2024). Selain itu, pengujian juga mencakup keberhasilan ekstraksi dan keterbacaan *QR Code* sebagai dasar penentuan validitas dokumen ber-*watermark*.

3.2 | Uji *Imperceptibility*

Hasil pengamatan visual menunjukkan *watermark* tidak tampak secara kasat mata. Perbandingan cover image sebelum dan sesudah penyisipan sebagaimana ditampilkan pada **Gambar 6** dan **Gambar 7** tidak memperlihatkan perubahan yang berarti, sehingga kualitas tampilan dokumen tetap terjaga.



GAMBAR 6 Perbandingan gambar sebelum dan sesudah penyisipan



GAMBAR 7 Perbandingan gambar sebelum dan sesudah penyisipan

Secara kuantitatif, pengujian pada 10 dokumen dengan total 169 gambar seperti yang ditampilkan pada **Tabel 1**, menghasilkan nilai MSE yang sangat rendah, yaitu 0,02–0,19, serta nilai PSNR yang tinggi, yakni 55,4–67,1 dB. Rentang nilai ini mengindikasikan distorsi yang sangat kecil akibat penyisipan *watermark*. Dengan demikian, metode LSB terbukti memiliki tingkat *imperceptibility* yang sangat baik pada citra dalam dokumen bahan ajar.

TABEL 1 Rata-rata Nilai MSE dan PSNR Hasil Pengujian

No	Nama Dokumen	Jumlah Gambar	MSE	PSNR	MSE (CRC32)	PSNR (CRC32)
1	Doc1.docx	23	0.18	55.6 dB	0.18	55.4
2	Doc2.docx	18	0.18	55.4 dB	0.18	55.3
3	Doc3.docx	13	0.15	56.5 dB	0.19	55.4
4	Doc4.docx	17	0.16	56.0 dB	0.18	55.6
5	Doc5.docx	11	0.17	56.7 dB	0.17	56.3
6	Doc6.pdf	18	0.19	55.4 dB	0.19	55.3
7	Doc.pdf	8	0.12	58.0 dB	0.13	57.2
8	Doc8.pdf	22	0.15	56.8 dB	0.17	56.2
9	Doc9.pdf	25	0.15	58.1 dB	0.15	57.8
10	Doc10.pdf	14	0.13	57.1 dB	0.15	56.4

3.2.2 | Uji Keberhasilan Ekstraksi

Uji ekstraksi dilakukan untuk mengambil kembali *watermark* berupa *QR Code* dari dokumen hasil penyisipan dengan membaca bit LSB pada citra, merekonstruksi *QR Code*, lalu mendekode *payload*. Pemeriksaan integritas menggunakan CRC32 bersifat opsional dan dijalankan hanya jika fitur *integrity check* diaktifkan.

TABEL 2 Hasil Pengujian Ekstraksi *QR Code*

No	Nama Dokumen	Jumlah Gambar	Validasi Tanpa CRC32	Status CRC32	Validasi CRC32
1	Doc1.docx	23	Berhasil	Cocok	Berhasil
2	Doc2.docx	18	Berhasil	Cocok	Berhasil
3	Doc3.docx	13	Berhasil	Cocok	Berhasil
4	Doc4.docx	17	Berhasil	Cocok	Berhasil
5	Doc5.docx	11	Berhasil	Cocok	Berhasil
6	Doc6.pdf	18	Berhasil	Cocok	Berhasil
7	Doc7.pdf	8	Berhasil	Cocok	Berhasil
8	Doc8.pdf	22	Berhasil	Cocok	Berhasil
9	Doc9.pdf	25	Berhasil	Cocok	Berhasil
10	Doc10.pdf	14	Berhasil	Cocok	Berhasil

Berdasarkan **Tabel 2**, pengujian pada 10 dokumen (169 gambar) menunjukkan seluruh *QR Code* berhasil diekstraksi, dapat dipindai, dan menghasilkan *payload* yang identik dengan data saat penyisipan (validasi tanpa CRC32: Berhasil). Pada validasi CRC32, seluruh *checksum* hasil ekstraksi juga cocok dengan *checksum* saat penyisipan sehingga status CRC32 dan validasi CRC32 seluruhnya Berhasil. Dengan demikian, tingkat keberhasilan ekstraksi adalah 100% (169/169) dan seluruh sampel dinyatakan valid.

3.3 | Analisis Ukuran File

Perbandingan ukuran file sebelum dan sesudah penyisipan *watermark* menunjukkan adanya variasi perubahan pada setiap dokumen. Rincian ukuran file pada kondisi asli, hasil *watermark* standar, dan hasil *watermark* dengan CRC32.

TABEL 3 Perbandingan Ukuran File Sebelum dan Sesudah *Embedding*

No	Nama Dokumen	Asli	*Watermark*	*Watermark* (CRC32)
1	Doc1.docx	1.990 KB	1.591 KB	1.608
2	Doc2.docx	1.502 KB	1.206 KB	1.217
3	Doc3.docx	2.196 KB	1.661 KB	1.029
4	Doc4.docx	2.018 KB	1.661 KB	1.352
5	Doc5.docx	567 KB	1.287 KB	1.297
6	Doc6.pdf	515 KB	2.436 KB	2.436
7	Doc7.pdf	817 KB	1.970 KB	1.970
8	Doc8.pdf	789 KB	10.723 KB	10.723
9	Doc9.pdf	941 KB	14.191 KB	14.191
10	Doc10.pdf	513 KB	860 KB	860

Berdasarkan **Tabel 3**, ukuran file setelah *embedding* mengalami variasi. Pada dokumen DOCX (Doc1–Doc5), perubahan ukuran relatif kecil dan beberapa file justru menurun, kemungkinan akibat proses kompresi/*repackaging* saat penyimpanan ulang dokumen. Sebaliknya, pada dokumen PDF (Doc6–Doc10) ukuran cenderung meningkat lebih jelas, terutama Doc7–Doc9, karena mekanisme kompresi gambar dalam PDF menjadi kurang efisien setelah modifikasi bit LSB.

Selain itu, hasil pada kolom *Watermark* (CRC32) menunjukkan bahwa penggunaan CRC32 tidak memberikan pengaruh berarti terhadap ukuran file dibanding *watermark* tanpa CRC32. Secara keseluruhan, perubahan ukuran tidak mengganggu keterbacaan dokumen maupun kualitas visual.

4 | PEMBAHASAN

Hasil penelitian menunjukkan bahwa sistem *watermarking* berbasis *QR Code* dan metode LSB berhasil diimplementasikan dalam bentuk aplikasi web yang fungsional dan stabil. Tiga proses utama pembuatan *QR Code*, penyisipan *watermark*, dan validasi dapat berjalan dengan baik pada dokumen berformat DOCX maupun PDF. Penyisipan *watermark* dilakukan pada kanal biru citra menggunakan metode LSB tanpa menimbulkan perbedaan visual

yang signifikan, sehingga tetap mempertahankan kualitas tampilan bahan ajar digital.

Dari sisi kinerja visual, pengujian *imperceptibility* menghasilkan nilai PSNR yang tinggi, yaitu berada pada rentang 55,4–58,1 dB, jauh di atas ambang batas 30 dB yang umumnya digunakan sebagai indikator kualitas visual yang baik. Nilai MSE yang rendah (0,12–0,19) memperkuat temuan bahwa perbedaan antara citra asli dan citra hasil penyisipan sangat kecil. Hasil ini menegaskan bahwa metode LSB efektif dalam menyisipkan *QR Code* tanpa mengorbankan kualitas visual dokumen.

Selain itu, pengujian ekstraksi menunjukkan tingkat keberhasilan 100% pada seluruh dokumen uji. *QR Code* yang diekstraksi dapat dipindai dengan baik dan menghasilkan *payload* yang identik dengan data awal. Penerapan validasi CRC memastikan integritas data tetap terjaga, sehingga sistem tidak hanya mampu menyembunyikan informasi, tetapi juga menjamin keasliannya. Perubahan ukuran file yang terjadi setelah proses *embedding* bersifat relatif kecil dan tidak memengaruhi keterbacaan maupun fungsi dokumen. Secara keseluruhan, hasil ini menunjukkan bahwa sistem yang dikembangkan layak digunakan sebagai solusi perlindungan hak cipta bahan ajar digital.

5 | KESIMPULAN

Penelitian ini berhasil mengimplementasikan sistem *watermarking* tak terlihat berbasis kombinasi *QR Code* dan metode *steganografi Least Significant Bit* (LSB) untuk melindungi bahan ajar digital. Sistem yang dibangun dalam bentuk aplikasi web ini terbukti mampu menyisipkan identitas atau informasi hak cipta ke dalam citra pada dokumen berformat DOCX maupun PDF tanpa menurunkan kualitas visual. Hasil pengujian menunjukkan bahwa *watermark* yang disisipkan tidak terlihat secara kasat mata dengan nilai PSNR pada rentang 55,4–67,1 dB dan MSE yang rendah, menandakan kualitas citra tetap terjaga. Seluruh *watermark* berhasil diekstraksi kembali dengan tingkat keberhasilan 100% dan *QR Code* yang dihasilkan dapat dipindai dengan benar, membuktikan keandalan metode ini dalam menjaga keaslian konten. Selain itu, fitur opsional CRC32 memberikan lapisan keamanan tambahan dengan memastikan integritas *payload* tetap terjaga sepanjang proses distribusi. Meskipun terjadi variasi ukuran file setelah penyisipan, khususnya pada format PDF, perubahan tersebut tidak memengaruhi keterbacaan maupun kualitas visual dokumen. Dengan demikian, kombinasi *QR Code* dan LSB dapat dijadikan solusi praktis dan efisien dalam melindungi bahan ajar digital dari penyalahgunaan sekaligus memperkuat aspek autentikasi dan verifikasi keaslian dokumen.

Daftar Pustaka

Aditya Permana, A., & Amma, H. (2022). IMPLEMENTASI *STEGANOGRAFI* FILE CITRA DIGITAL MENGGUNAKAN METODE *LEAST SIGNIFICANT BIT*. *JT Jurnal Teknik*, *11*(1), 62–72.

Akmal, R. A., Furqan, Mhd. F., & Kurniawan R, R. (2023). Implementasi Metode *Least Significant Bit* Dalam Teknik *Steganografi* pada Berkas Audio Dengan Stego Citra Digital. *G-Tech: Jurnal Teknologi Terapan*, *7*(2), 543–553. https://doi.org/10.33379/gtech.v7i2.2300

Alajmi, M., Elashry, I., El-Sayed, H. S., & FaragAllah, O. S. (2020). Steganography of Encrypted Messages Inside Valid *QR Code*s. *IEEE Access*, *8*, 27861–27873. https://doi.org/10.1109/ACCESS.2020.2971984

Alveda, A., Rakhmawati, L., & Agustin Tjahyaningtijas Agustin, R. H. P. (2024). *Penyisipan Watermark Menggunakan Metode LSB (Least Significant Bit) untuk Autentikasi Citra Medis*.

Antika, T. L., Kusmana, S., & Gloriani, Y. (2022). BAHAN AJAR DIGITAL TEKS CERPEN UNTUK SMP. In *Jurnal Penelitian Pendidikan Bahasa dan Sastra* (Vol. 7, Issue 2).

Devi, P. A. R., & Rosyid, H. (2022). Pemaparan Materi Dasar Pengolahan Citra Digital untuk Upgrade Wawasan Siswa di SMK Dharma Wanita Gresik. *Jurnal Abdi Masyarakat Indonesia*, *2*(4), 1259–1264. https://doi.org/10.54082/jamsi.405

Fadlika Satria, A., Ibnu Adam, R., & carudin. (2021). Analisis Digital *Watermarking* untuk Otentikasi pada Citra Manipulasi Menggunakan Metode *Least Significant Bit*. *Edumatic Jurnal Pendidikan Informatika*, *5*(2), 204–213. https://doi.org/10.29408/edumatic.v5i2.3901

Faisal, M., Hotimah, Nurhaedah, AP, N., & Khaerunnisa. (2020). Peningkatan Kompetensi Guru Sekolah Dasar dalam Mengembangkan Bahan Ajar Digital di Kabupaten Gowa. *Jurnal Publikasi Pendidikan*, *10*(3), 266–270. http://ojs.unm.ac.id/index.php/

Fathanudien, A., & Maharani, V. (2023). Perlindungan Hukum Hak Cipta terhadap Buku Elektronik (E-Book) di Era Globalisasi. In *Jurnal Penelitian Universitas Kuningan* (Vol. 14).

Ferdiansyah, Id Hadiana, A., & Rakhmat Umbara, F. (2021). PENGGUNAAN *QR CODE* BERBASIS KRIPTOGRAFI ALGORITMA AES ADVANCED ENCRYPTION STANDARD UNTUK ADMINISTRASI REKAM MEDIS. *JOINT (Journal of Information Technology)*, *03*(2), 20–27.

Gultom, C. E., & Suhartana, K. G. (2023). Penerapan *Steganografi* dan *Visible Watermarking* Pada Gambar Digital Untuk Perlindungan Hak Cipta. *Jurnal Elektronik Ilmu Komputer Udayana*, *12*(2), 377–384.

Harits M, A. R., Ridwan, R., Hafidzin, A. P., & Taufik, M. (2021). Proteksi Keamanan Data pada *Quick Response* (QR) Code. *Jurnal Teknologi Dan Rekayasa Manufaktur*, *3*(2), 99–110. https://doi.org/10.48182/jtrm.v3i2.58

Hasan, N. F., Dengen, C. N., & Ariyus, D. (2020). Analisis Histogram *Steganografi Least Significant Bit* Pada Citra Grayscale. *Jurnal Teknologi Informasi & Komunikasi Digital Zone*, *11*, 2086–4884. https://doi.org/10.31849/digitalzone.v11i1.3413ICCS

Nur Aqsal Aminullah, M., Yusliana Bakti, R., Hayat, M. A., & Lukman. (2022). *PEMBUATAN VERIFIKASI SERTIFIKAT DIGITAL SEBAGAI BUKTI KEABSAHAN MENGGUNAKAN ALGORITMA STEGANOGRAFI DENGAN METODE LEAST SIGNIFICANT BIT INSERTION (LSB)* (Vol. 4, Issue 1).

Purbaningrum, A., Silvi Amalia, K., & Ady Saputro, I. (2023). *Penerapan Metode Least Significant Bit (LSB) dalam Menyisipkan Pesan Rahasia pada Citra Digital: Sebuah Pendekatan Steganografi*.

Putri Pebriani, D., Marwati, R., & Rachmatin, D. (2025). Implementasi Kombinasi Secret Sharing dan *Steganografi* Citra *Least Significant Bit* dengan *QR Code*. *Original Article Indonesian Journal of Applied Mathematics*, *5*(1), 33–41. https://doi.org/10.35472/indoja

Sagala, S. H. (2021). Penerapan Metode CRC32 Untuk Mendeteksi Otentikasi Citra Tanda Tangan. *Pelita Informatika : Informasi Dan Informatika*, *9*(4), 276–280.

WIDIYONO, WIBOWO, A. P., & DARMAWAN, A. S. (2021). TEKNIK *WATERMARKING* MENGGUNAKAN METODE *LEAST SIGNIFICANT BIT* PADA CITRA UNTUK PERLINDUNGAN HAK CIPTA MOTIF BATIK. *Jurnal Instek Informatika Sains Dan Teknologi*, *6*(1), 37–45.

Wulandari, F. (2024). Problematika Pelanggaran Hak Cipta di Era Digital. *Journal of Contemporary Law Studies*, *2*(2), 99–114. https://doi.org/10.47134/lawstudies.v2i2.2261

Yanti, F., & Budayawan, K. (2023). Implementasi *Steganografi* Menggunakan Metode *Least Significant Bit* (Lsb) dalam Pengamanan Informasi Pada Citra Digital. *Jurnal Vocational Teknik Elektronika Dan Informatika*, *11*(1), 63–70. http://ejournal.unp.ac.id/index.php/voteknika/index