Journal : Jurnal Rekayasa Sistem Informasi dan Teknologi (JRSIT)
Publisher : Yayasan Nuraini Ibrahim Mandiri
ISSN : e-ISSN 3025-888X
Volume / Issue / Year/ Page : Vol. 4 No. 1 (2026): Agustus/ Hal 53-66

IMPLEMENTASI *PASSWORD-BASED SCRAMBLING* DAN METODE *LEAST SIGNIFICANT BIT* (LSB) UNTUK AUTENTIKASI KEASLIAN CITRA DIGITAL

Angeli Khairunissa Aulia Rahma [1]*, Bagus Satrio Waluyo Poetro [2],
[1,2]Universitas Islam Sultan Agung, Indonesia
[1]angelkhrnss@gmail.com, [2]bagusswp@unissula.ac.id
*coresponding author

Info Artikel

Pengajuan : 27-07-2026
Peninjauan : 05-08-2026
Revisi : 15-08-2026
Diterima : 25-08-2026
Diterbitkan : 31-08-2026

Kata Kunci:
Autentikasi Citra, *Fragile Watermarking*, *Password-Based Scrambling*, *Least Significant Bit*

Abstrak

Kemudahan distribusi citra dokumentasi melalui kanal digital meningkatkan risiko pengunggahan ulang tanpa identitas sumber serta manipulasi yang sulit dikenali secara visual. Kondisi tersebut menyebabkan penerima sulit memastikan apakah citra masih sama dengan citra yang pertama kali diterbitkan. Penelitian ini bertujuan menerapkan kombinasi Password-Based Scrambling dan Least Significant Bit (LSB) dengan pendekatan fragile watermarking untuk membantu autentikasi citra digital. Password diproses menggunakan SHA-256 untuk menghasilkan seed bagi pseudo-random number generator (PRNG). Urutan deterministik yang dihasilkan PRNG digunakan pada Fisher-Yates Shuffle untuk mengacak piksel watermark dan menentukan lokasi penyisipan pada kanal LSB. Pengujian dilakukan menggunakan 12 citra sampul RGB dan satu watermark grayscale berukuran 320 × 320 piksel pada kondisi tanpa manipulasi serta setelah kompresi JPEG, cropping, dan resizing. Proses penyisipan menghasilkan rata-rata MSE 0,0635, PSNR 62,78 dB, dan SSIM 0,9995, yang menunjukkan perubahan visual sangat kecil. Tanpa manipulasi, watermark berhasil direkonstruksi dengan BER 0 dan NC 1. Setelah manipulasi, rata-rata BER meningkat menjadi 0,4974 dan NC menurun menjadi 0,5941 sehingga watermark tidak dapat dikenali. Pada kompresi, PSNR tetap lebih dari 40 dB meskipun ekstraksi watermark gagal. Hasil tersebut menunjukkan bahwa sistem sensitif terhadap seluruh manipulasi yang diuji, tetapi belum dapat menentukan jenis dan lokasi manipulasi secara otomatis.

How to Cite *:* Rahma, A. K. A., & Poetro, B. S. W. (2026). Implementasi *password-based scrambling* dan metode *least significant bit* (LSB) untuk autentikasi keaslian citra digital. *Jurnal Rekayasa Sistem Informasi dan Teknologi (JRSIT), 4*(1), 53–66.

DOI : 10.70248/jrsit.v4i1.4565

PENDAHULUAN

Citra dokumentasi kegiatan Sekretariat Daerah Provinsi Jawa Tengah digunakan sebagai sumber informasi publik dan didistribusikan melalui berbagai kanal digital. Kemudahan penyalinan dan pengunggahan ulang menyebabkan citra dapat terpisah dari keterangan, sumber, atau identitas pemiliknya. Selain itu, isi citra dapat diubah tanpa selalu menghasilkan perbedaan visual yang mudah dikenali. Kondisi tersebut menimbulkan permasalahan autentikasi karena pemilik sulit memastikan apakah citra yang diperoleh masih sama dengan citra yang pertama kali diterbitkan atau telah mengalami manipulasi. Permasalahan serupa menjadi perhatian dalam penelitian autentikasi citra karena perubahan digital dapat memengaruhi integritas informasi yang disampaikan (Adi et al., 2023; Vaidya et al., 2025).

Permasalahan tersebut belum dapat diselesaikan hanya melalui pemeriksaan visual. Perubahan kecil pada nilai maupun posisi piksel tidak selalu dapat dikenali oleh

mata manusia, sedangkan identitas yang dicantumkan melalui nama berkas, metadata, atau keterangan unggahan dapat hilang ketika citra disalin dan didistribusikan kembali. Oleh karena itu, diperlukan informasi autentikasi yang melekat pada data citra dan dapat diperiksa kembali. *Digital watermarking* menyediakan mekanisme tersebut dengan menyisipkan informasi ke dalam citra. Pada pendekatan *fragile watermarking*, informasi yang disisipkan dirancang sensitif terhadap perubahan, sehingga kerusakan atau kegagalan rekonstruksi *watermark* dapat digunakan sebagai indikator bahwa integritas citra tidak lagi terjaga (Aminuddin & Ernawan, 2022a; Adi et al., 2023).

Kebutuhan untuk mempertahankan tampilan citra sekaligus memperoleh sensitivitas terhadap manipulasi menjadi dasar pemilihan *Least Significant Bit* (LSB). Metode ini bekerja pada domain spasial dengan mengganti bit berbobot paling rendah, sehingga perubahan nilai pada setiap kanal piksel relatif kecil. Penelitian Setiawati et al. (2023) menunjukkan bahwa penyisipan menggunakan LSB dapat mempertahankan kemiripan visual antara citra asli dan citra ter-*watermark*. Namun, posisi LSB mudah berubah akibat kompresi *lossy*, interpolasi, dan perubahan geometris. Karakteristik tersebut berbeda dari metode domain frekuensi, seperti *Discrete Cosine Transform* (DCT) dan *Discrete Wavelet Transform* (DWT), yang umumnya digunakan ketika *watermark* diharapkan tetap bertahan setelah pengolahan citra. Dalam penelitian autentikasi ini, sensitivitas LSB dimanfaatkan sebagai penanda terjadinya perubahan, bukan sebagai kelemahan sistem (Makhrib & Karim, 2022; Senol et al., 2023).

Sejumlah penelitian telah mengembangkan *watermarking* untuk autentikasi dan deteksi manipulasi. Aminuddin dan Ernawan (2022a) menggunakan pergeseran LSB dalam skema *fragile watermarking* untuk autentikasi dan pemulihan mandiri citra. Adi et al. (2023) menerapkan pengurutan *Dyadic Walsh* untuk menghasilkan bit autentikasi dan mendeteksi perubahan pada citra. Pada domain frekuensi, Senol et al. (2023) menggabungkan pengacakan dan pemrosesan blok bagian dalam-luar untuk membedakan pengolahan yang dapat ditoleransi dari manipulasi berbahaya. Selanjutnya, Vaidya et al. (2025) mengintegrasikan DWT dan dekomposisi Schur untuk mendeteksi, melokalisasi, dan memulihkan bagian citra yang dimanipulasi; pengujiannya melaporkan tingkat deteksi manipulasi 100% pada serangan yang diuji serta PSNR 45 dB pada citra ter-watermark. Temuan-temuan tersebut memperlihatkan bahwa watermarking dapat digunakan tidak hanya untuk menyisipkan identitas, tetapi juga untuk mengevaluasi integritas citra.

Meskipun demikian, pendekatan berbasis transformasi dan pemrosesan blok umumnya memerlukan tahapan yang lebih kompleks, sedangkan penyisipan LSB yang dilakukan secara berurutan memiliki lokasi yang lebih mudah diperkirakan. Penelitian ini menggunakan kombinasi SHA-256 dan Fisher-Yates Shuffle sebagai *key-dependent permutation* untuk mengurangi keteraturan tersebut. *Password* dipetakan oleh SHA-256 menjadi nilai hash 256-bit yang digunakan sebagai *seed pseudo-random number generator* (PRNG). Urutan deterministik dari PRNG selanjutnya mengendalikan pengacakan piksel *watermark* dan pemilihan lokasi kanal LSB. *Password* yang sama menghasilkan urutan yang sama pada penyisipan dan ekstraksi, sedangkan *password* berbeda menghasilkan permutasi yang berbeda. Fisher-Yates Shuffle versi komputasional Durstenfeld dipilih karena membentuk permutasi tanpa elemen hilang atau ganda. Penelitian Ma et al. (2021) juga menunjukkan penerapan Fisher-Yates untuk mengendalikan pengacakan posisi piksel citra menggunakan urutan pseudoacak. Dengan demikian, seluruh piksel *watermark* tetap memiliki pemetaan yang konsisten (Durstenfeld, 1964; Ma et al., 2021).

Journal : Jurnal Rekayasa Sistem Informasi dan Teknologi (JRS
Publisher : Yayasan Nuraini Ibrahim Mandiri
ISSN : e-ISSN 3025-888X
Volume / Issue / Year/ Page : Vol. 4 No. 1 (2026): Agustus/ Hal 53-66

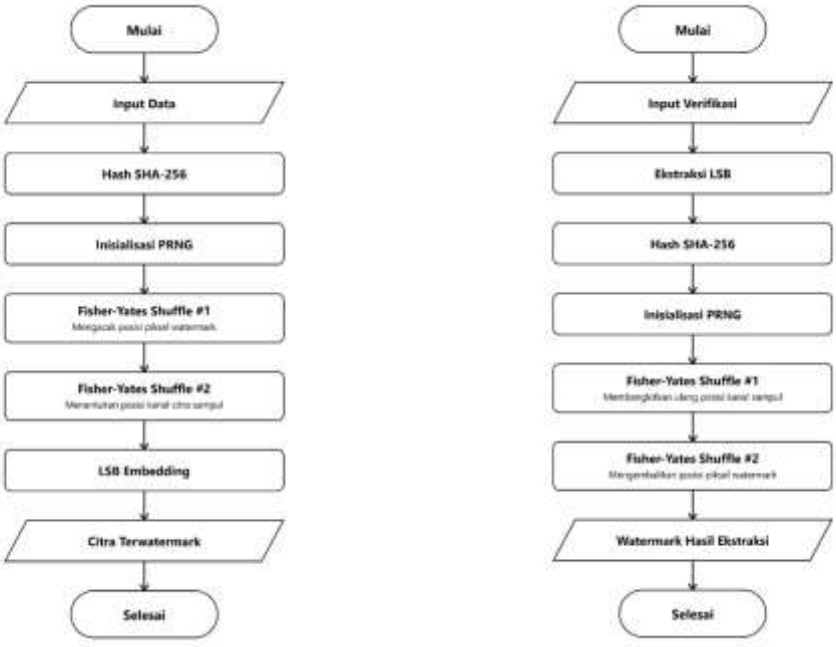
Berdasarkan penelitian terdahulu, evaluasi *watermarking* masih banyak diarahkan pada kualitas visual citra, ketahanan *watermark*, atau kemampuan lokalisasi dan pemulihan. Kualitas visual yang tinggi belum secara langsung menunjukkan bahwa *watermark* dapat diekstraksi setelah citra dimanipulasi. Oleh sebab itu, rumusan masalah penelitian ini adalah bagaimana menerapkan *Password-Based Scrambling* dan LSB untuk menghasilkan citra ter-*watermark* dengan perubahan visual yang kecil sekaligus memberikan indikator manipulasi melalui kegagalan ekstraksi *watermark*.

Penelitian ini bertujuan mengembangkan skema autentikasi citra dokumentasi berbasis *password* serta mengevaluasi dua aspek secara terpisah, yaitu kualitas citra menggunakan *Mean Squared Error* (MSE), *Peak Signal-to-Noise Ratio* (PSNR), dan *Structural Similarity Index Measure* (SSIM), serta kesesuaian *watermark* menggunakan *Bit Error Rate* (BER) dan *Normalized Cross-Correlation* (NC). Pengujian dilakukan pada kondisi tanpa manipulasi dan setelah manipulasi, seperti kompresi JPEG, *cropping*, serta *resizing* untuk mengetahui batas kemampuan sistem dalam mendeteksi perubahan nilai piksel maupun perubahan spasial.

METODE PENELITIAN

Pengujian terdiri atas dua tahap utama, yaitu penyisipan dan ekstraksi *watermark*. Pada tahap penyisipan, kualitas citra ter-*watermark* dibandingkan dengan citra sampul asli menggunakan MSE, PSNR, dan SSIM. Selanjutnya, pada tahap ekstraksi, kesesuaian antara *watermark* asli dan *watermark* hasil ekstraksi diukur menggunakan BER dan NC. Pengujian ekstraksi dilakukan pada kondisi tanpa manipulasi serta setelah kompresi JPEG 50% dan 70%, cropping 5% dan 10%, serta resizing 50% dan 75%. Seluruh tahapan diimplementasikan menggunakan Python pada Google Colab, sedangkan hubungan antartahap ditunjukkan pada Gambar 1.

Tahapan Penelitian



(a) *Flowchart* penyisipan *watermark* (b) *Flowchart* ekstraksi *watermark*

Gambar 1. *Flowchart* Tahapan Penelitian

Journal : Jurnal Rekayasa Sistem Informasi dan Teknologi (JRS
Publisher : Yayasan Nuraini Ibrahim Mandiri
ISSN : e-ISSN 3025-888X
Volume / Issue / Year/ Page : Vol. 4 No. 1 (2026): Agustus/ Hal 53-66

Berdasarkan Gambar 1, proses penyisipan diawali dengan memasukkan password (P). Sistem mengolah *password* tersebut menggunakan SHA-256 untuk menghasilkan nilai hash (h). Nilai hash merupakan deretan karakter yang berfungsi sebagai identitas matematis dari *password*. Perubahan satu karakter pada *password* akan menghasilkan nilai hash yang berbeda. Dalam program, nilai hash ditampilkan dalam bentuk 64 karakter heksadesimal, yaitu kombinasi angka 0–9 dan huruf a–f. PRNG (*Pseudo-Random Number Generator*) membutuhkan bilangan sebagai nilai awal pengacakan atau *seed*. Oleh karena itu, nilai hash yang masih berbentuk heksadesimal dikonversi menjadi bilangan bulat (s). Proses tersebut dinyatakan pada Persamaan (1).

$$h = SHA - 256(P), \text{s=int(h,16)} \quad (1)$$

Pada Persamaan (1), (P) merupakan *password*, (h) merupakan nilai hash yang dihasilkan oleh SHA-256, dan (s) merupakan *seed* untuk PRNG Mersenne Twister. Angka 16 pada int(h,16) menunjukkan bahwa nilai hash dibaca sebagai bilangan berbasis heksadesimal. Proses konversi ini diperlukan agar nilai hash dapat digunakan sebagai *seed*. *Password* yang sama selalu menghasilkan *seed* dan urutan pengacakan yang sama. Dengan demikian, susunan pengacakan pada proses penyisipan dapat dibentuk kembali saat proses ekstraksi (Firmansyah & Tahir, 2026).

Setelah *seed* diperoleh, sistem menggunakannya untuk mengacak susunan piksel *watermark* menggunakan Fisher-Yates Shuffle. Sebelum diacak, piksel *watermark* yang semula tersusun dalam baris dan kolom diubah menjadi satu urutan. Sebagai contoh, empat piksel dengan nilai W=[10,20,30,40] dapat diacak berdasarkan urutan indeks π=[2,0,3,1]. Hasil pengacakannya menjadi W′=[30,10,40,20]. Secara matematis, proses tersebut dinyatakan pada Persamaan (2).

$$W'_i = W_{\pi(i)}, \; 0 \le i < N \quad (2)$$

Pada Persamaan (2), W'_i merupakan piksel pada urutan ke-i setelah pengacakan, sedangkan $W_{\pi(i)}$merupakan piksel asli yang dipilih berdasarkan urutan indeks hasil Fisher-Yates Shuffle. Simbol N menyatakan jumlah seluruh piksel *watermark*. Setiap indeks hanya digunakan satu kali sehingga pengacakan hanya mengubah urutan piksel tanpa menghilangkan atau menggandakan piksel.

Piksel *watermark* yang telah diacak kemudian diubah menjadi deretan bit yang terdiri atas angka 0 dan 1. Deretan ini disebut *bitstream*. Sistem selanjutnya menentukan lokasi kanal citra sampul yang akan digunakan untuk menyimpan setiap bit. Penentuan lokasi dilakukan menggunakan PRNG yang sama sehingga lokasi penyisipan bergantung pada *password*. Setiap bit *watermark* disisipkan ke bagian LSB atau bit terakhir dari nilai kanal citra sampul. Proses penyisipan dinyatakan pada Persamaan (3).

$$C'(q_i) = [C(q_i) \wedge 254] \vee b_i, \quad 0 \le i < L \quad (3)$$

Pada Persamaan (3), $C(q_i)$ merupakan nilai kanal citra sampul pada lokasi penyisipan ke-i, sedangkan b_i merupakan bit *watermark* yang akan disisipkan. Nilai kanal setelah penyisipan dinyatakan sebagai $C'(q_i)$. Operasi dengan nilai 254 terlebih dahulu membuat bit terakhir kanal menjadi 0. Setelah itu, bit terakhir tersebut diisi dengan bit *watermark*, yaitu 0 atau 1. Proses ini hanya dapat mengubah nilai kanal sebesar satu tingkat sehingga perubahan pada citra sulit dikenali secara visual.

Pada proses ekstraksi, sistem menggunakan *password* yang sama untuk menghasilkan kembali urutan pengacakan dan lokasi penyisipan yang sama. Bit *watermark* diambil dari LSB setiap lokasi, disusun kembali menjadi piksel, kemudian dikembalikan ke urutan sebelum pengacakan. Apabila *password* yang dimasukkan berbeda, urutan dan lokasi yang dihasilkan juga berbeda sehingga *watermark* tidak

Journal : Jurnal Rekayasa Sistem Informasi dan Teknologi (JRS
Publisher : Yayasan Nuraini Ibrahim Mandiri
ISSN : e-ISSN 3025-888X
Volume / Issue / Year/ Page : Vol. 4 No. 1 (2026): Agustus/ Hal 53-66

dapat direkonstruksi dengan benar.

Dataset Penelitian

Setelah mekanisme penyisipan dan ekstraksi ditetapkan, tahap berikutnya adalah menyiapkan dataset penelitian. Dataset berupa foto dokumentasi resmi kegiatan pemerintah yang dikelola oleh Humas Sekretariat Daerah Provinsi Jawa Tengah tahun 2026. Data terdiri atas 12 citra sampul RGB dan satu logo resmi sebagai *watermark* berukuran 320 × 320 piksel. Apabila *watermark* masih berformat RGB, sistem mengonversinya menjadi *grayscale* menggunakan transformasi luminansi pada Persamaan (4).

$$Y = 0{,}299R + 0{,}587G + 0{,}114B \quad (4)$$

Pada Persamaan (4), R, G, dan B merupakan intensitas kanal merah, hijau, dan biru, sedangkan Y merupakan intensitas *grayscale* yang dihasilkan. Konversi tersebut menghasilkan satu kanal 8-bit sehingga data yang disisipkan lebih ringkas tanpa mengubah *watermark* menjadi citra biner. Sampel dataset ditunjukkan pada Tabel 1.

Tabel 1. Sampel Citra Sampul dan Citra Watermark

Nama File	Citra Sampul	Dimensi
CS2		4160 x 2773 piksel
CS3		1280 x 853 piksel
CS4		950 x 650 piksel
CS5		2490 x 1567 piksel
Citra *watermark*		320 x 320 piksel

Journal : Jurnal Rekayasa Sistem Informasi dan Teknologi (JRS
Publisher : Yayasan Nuraini Ibrahim Mandiri
ISSN : e-ISSN 3025-888X
Volume / Issue / Year/ Page : Vol. 4 No. 1 (2026): Agustus/ Hal 53-66

Parameter Evaluasi

Setelah data disiapkan, hasil penyisipan dan ekstraksi dievaluasi melalui dua kelompok metrik, yaitu kualitas citra dan tingkat kemiripan *watermark* hasil ekstraksi. Kriteria umum untuk menafsirkan MSE, PSNR, dan SSIM dirangkum pada Tabel 2.

Tabel 2. Parameter Kualitas Citra

Kondisi	MSE	PSNR	SSIM	Interpretasi
Kemiripan tinggi	Mendekati 0	> 40 dB	Mendekati 1	Perubahan sangat kecil
Kemiripan rendah	Relatif besar	< 20 dB	Menjauhi 1	Perubahan cukup besar

Berdasarkan Tabel 2, evaluasi kualitas dimulai dengan menghitung *Mean Squared Error* (MSE), yaitu rata-rata kuadrat selisih nilai piksel antara citra sampul asli dan citra ter-*watermark*. Untuk citra berukuran M × N dengan C kanal, perhitungan MSE ditunjukkan pada Persamaan (5).

$$MSE = \frac{1}{3MN}\sum_{c=1}^{3}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xyc} - C_{xyc}\right)^2 \quad (5)$$

Pada Persamaan (5), M dan N menyatakan tinggi dan lebar citra, 3 merupakan jumlah kanal warna, sedangkan S(xyc) dan C(xyc) adalah nilai piksel pada posisi dan kanal yang sama. Selisih setiap nilai piksel antara kedua citra dikuadratkan, dijumlahkan, lalu dibagi dengan jumlah seluruh nilai piksel. MSE yang mendekati 0 menunjukkan perubahan yang sangat kecil. Nilai MSE tersebut selanjutnya digunakan untuk menghitung PSNR melalui Persamaan (6).

$$\text{PSNR} = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (6)$$

Pada Persamaan (6), MAX adalah nilai intensitas maksimum citra; untuk citra 8-bit nilainya 255. PSNR dinyatakan dalam desibel (dB) dan berbanding terbalik dengan MSE. Artinya, semakin kecil kesalahan piksel, semakin tinggi PSNR dan semakin baik kualitas citra. Jika MSE bernilai 0, kedua citra identik dan nilai PSNR secara teoretis tidak terhingga. Karena MSE dan PSNR hanya bertumpu pada selisih piksel, kemiripan struktur citra juga diukur menggunakan SSIM pada Persamaan (7).

$$SSIM_{(x,y)} = [l(x,y)]^{\alpha}.[c(x,y)]^{\beta}.[s(x,y)]^{\gamma} \quad (7)$$

Pada Persamaan (7), SSIM mengevaluasi kemiripan struktur citra melalui tiga komponen utama, yaitu luminansi, kontras, dan struktur. Nilai SSIM yang mendekati 1 menunjukkan bahwa ketiga komponen pada kedua citra semakin serupa (Al Najjar, 2024). MSE, PSNR, dan SSIM menilai perubahan kualitas citra, tetapi tidak secara langsung menunjukkan apakah informasi *watermark* berhasil dipulihkan. Oleh karena itu, tingkat kemiripan *watermark* hasil ekstraksi dievaluasi dengan membandingkannya terhadap *watermark* asli. Metrik pertama adalah *Bit Error Rate* (BER), yang dihitung menggunakan Persamaan (8).

$$BER = \frac{1}{L}\sum_{i=1}^{L} b_i \oplus b'_i \quad (8)$$

Pada Persamaan (8), L menyatakan jumlah seluruh bit *watermark*, b_i merupakan bit *watermark* asli, dan b'_i merupakan bit hasil ekstraksi. Operasi XOR menghasilkan 1 apabila kedua bit berbeda dan 0 apabila sama. Jumlah perbedaan tersebut dibagi dengan L sehingga BER 0 menunjukkan tidak ada bit yang berubah, sedangkan BER yang mendekati 0,5 menunjukkan hasil ekstraksi mendekati susunan acak. Selain

Journal : Jurnal Rekayasa Sistem Informasi dan Teknologi (JRS
Publisher : Yayasan Nuraini Ibrahim Mandiri
ISSN : e-ISSN 3025-888X
Volume / Issue / Year/ Page : Vol. 4 No. 1 (2026): Agustus/ Hal 53-66

kesesuaian bit, kemiripan pola intensitas *watermark* diukur menggunakan NC pada Persamaan (9).

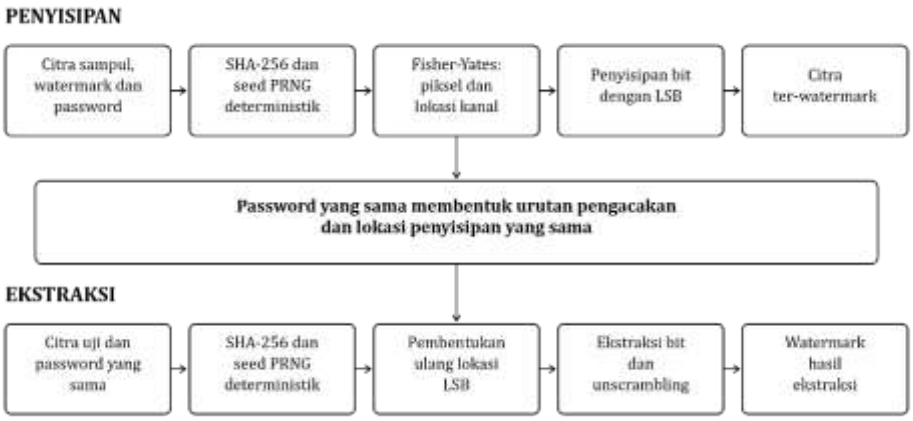
$$NC = \frac{\sum_{i=1}^{N} W_i \, W'_i}{\sqrt{(\sum_{i=1}^{N} W_i^2)(\sum_{i=1}^{N} W'^2_i)}} \quad (9)$$

Pada Persamaan (9), N adalah jumlah piksel *watermark*, W_i merupakan intensitas piksel watermark asli, dan W'_i merupakan intensitas piksel hasil ekstraksi. Pembilang menghitung hubungan antara nilai piksel *watermark* asli dan *watermark* hasil ekstraksi, sedangkan penyebut menyesuaikan hasil perhitungan berdasarkan keseluruhan nilai piksel pada masing-masing *watermark*. Nilai NC sebesar 1 menunjukkan kesamaan sempurna; nilai yang semakin rendah menunjukkan pola hasil ekstraksi semakin berbeda dari *watermark* asli. Dengan demikian, kelima metrik digunakan secara komplementer. MSE, PSNR, dan SSIM menjelaskan seberapa besar perubahan visual pada citra, sedangkan BER dan NC menjelaskan keberhasilan rekonstruksi *watermark*.

HASIL PENELITIAN DAN PEMBAHASAN

Arsitektur Sistem

Arsitektur sistem terdiri atas proses penyisipan dan ekstraksi. Kedua proses menggunakan *password* yang sama untuk menghasilkan *seed*, urutan piksel *watermark*, dan lokasi kanal LSB yang sama. Arsitektur sistem kedua proses ditunjukkan pada Gambar 2.



Gambar 2. Arsitektur sistem penyisipan dan ekstraksi *watermark*

Kualitas Citra Hasil Penyisipan

Setelah arsitektur sistem ditetapkan, pengujian pertama dilakukan untuk mengetahui pengaruh penyisipan LSB terhadap kualitas citra sampul. Hasil pengukuran MSE, PSNR, dan SSIM pada 12 citra disajikan pada Tabel 3.

Journal : Jurnal Rekayasa Sistem Informasi dan Teknologi (JRS
Publisher : Yayasan Nuraini Ibrahim Mandiri
ISSN : e-ISSN 3025-888X
Volume / Issue / Year/ Page : Vol. 4 No. 1 (2026): Agustus/ Hal 53-66

Tabel 3. Hasil Pengujian Penyisipan Watermark

Citra Sampul	MSE	PSNR (dB)	SSIM
CS1	0.015036	66.3594	0.999882
CS2	0.011816	67.4061	0.999860
CS3	0.035116	62.6758	0.999688
CS4	0.124952	57.1634	0.999022
CS5	0.220537	54.6960	0.998376
CS6	0.083368	58.9208	0.999481
CS7	0.019160	65.3069	0.999840
CS8	0.012883	67.0305	0.999885
CS9	0.190138	55.3401	0.998837
CS10	0.018373	65.4890	0.999883
CS11	0.010394	67.9629	0.999878
CS12	0.020444	65.0251	0.999833
Rata-rata	0.063518	62.7813	0.999539

Berdasarkan hasil pada Tabel 3, seluruh citra ter-*watermark* memiliki kemiripan visual yang sangat tinggi. Rata-rata MSE sebesar 0,0635, PSNR 62,78 dB, dan SSIM 0,9995 menunjukkan bahwa penyisipan LSB hanya menimbulkan perubahan kecil. Meskipun seluruh hasil tergolong baik, CS4, CS5, dan CS9 memiliki PSNR relatif lebih rendah karena *watermark* berukuran 320 × 320 piksel menggunakan proporsi kapasitas yang lebih besar pada citra berdimensi lebih kecil. Sebaliknya, CS11 menghasilkan PSNR tertinggi karena proporsi kanal yang dimodifikasi lebih kecil. Hasil ini menunjukkan bahwa kualitas citra dipengaruhi oleh perbandingan antara kapasitas citra sampul dan jumlah bit *watermark* yang disisipkan.

Kemiripan *Watermark* Hasil Ekstraksi

Pengujian dilanjutkan untuk menilai kemampuan sistem dalam mengekstraksi *watermark*. Pengujian dilakukan pada kondisi tanpa manipulasi dan setelah manipulasi berupa kompresi JPEG, *cropping*, serta *resizing*. Pada kondisi manipulasi, PSNR dan SSIM membandingkan citra ter-*watermark* sebelum dan setelah manipulasi, sedangkan BER dan NC membandingkan *watermark* asli dengan hasil ekstraksi. Nilai rata-rata pada setiap kondisi disajikan pada Tabel 4.

Tabel 4. Rata-Rata Kualitas Citra dan Kemiripan Watermark Hasil Ekstraksi

Pengujian	Level	PSNR (dB)	SSIM	BER	NC
Tanpa manipulasi	-	62,78	0,9995	0,0000	1,0000
Kompresi	50%	46,39	0,9965	0,4946	0,5979

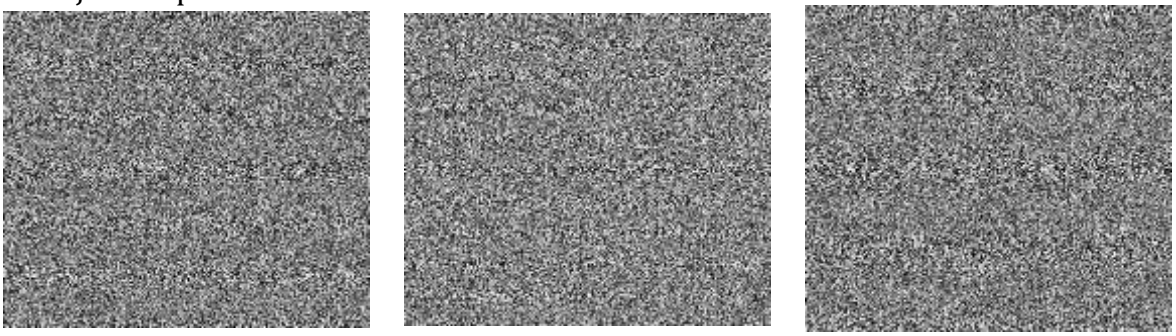
Journal : Jurnal Rekayasa Sistem Informasi dan Teknologi (JRS
Publisher : Yayasan Nuraini Ibrahim Mandiri
ISSN : e-ISSN 3025-888X
Volume / Issue / Year/ Page : Vol. 4 No. 1 (2026): Agustus/ Hal 53-66

Pengujian	Level	PSNR (dB)	SSIM	BER	NC
Kompresi	70%	42,66	0,9891	0,4999	0,5937
Cropping	5%	14,50	0,5155	0,4978	0,5913
Cropping	10%	12,79	0,4736	0,4981	0,5909
Resizing	50%	34,91	0,9527	0,4947	0,5972
Resizing	75%	29,72	0,8774	0,4990	0,5935
Rata-rata manipulasi	-	30,16	0,8008	0,4974	0,5941

Hasil pada Tabel 4 menunjukkan bahwa pada kondisi tanpa manipulasi seluruh *watermark* berhasil diekstraksi dengan BER 0 dan NC 1. Setelah enam kondisi manipulasi diterapkan, rata-rata keseluruhan menghasilkan PSNR 30,16 dB, SSIM 0,8008, BER 0,4974, dan NC 0,5941. BER yang mendekati 0,5 berarti sekitar separuh bit berbeda, sedangkan penurunan NC menunjukkan pola hasil ekstraksi tidak lagi sesuai dengan *watermark* asli. Ringkasan ini konsisten dengan tampilan *watermark* ekstraksi yang menyerupai *noise*.

Perbedaan antara kualitas visual dan keberhasilan ekstraksi terlihat jelas pada pengujian kompresi JPEG. Kompresi 50% dan 70% masih menghasilkan rata-rata PSNR masing-masing sebesar 46,39 dB dan 42,66 dB, sehingga citra tetap tampak serupa. Meskipun demikian, BER masing-masing mencapai 0,4946 dan 0,4999. Kedua hasil tersebut tidak saling bertentangan karena PSNR mengukur perubahan nilai piksel secara keseluruhan, sedangkan BER mengukur kerusakan bit *watermark*. Dengan demikian, kompresi *lossy* dapat mempertahankan tampilan citra, tetapi tetap mengubah banyak LSB dan menyebabkan autentikasi gagal.

Kegagalan ekstraksi juga terjadi pada manipulasi spasial. *Cropping* menghilangkan sekaligus menggeser posisi piksel, sedangkan resizing membentuk nilai piksel baru melalui interpolasi. Kedua proses tersebut mengubah korespondensi lokasi LSB. Akibatnya, seluruh level *cropping* dan *resizing* menghasilkan BER yang mendekati 0,5 dan *watermark* tidak dapat dikenali. Secara keseluruhan, hasil ini membuktikan bahwa sistem sensitif terhadap manipulasi nilai piksel maupun manipulasi spasial. Namun, karena pola BER dan NC dari seluruh serangan sama-sama mendekati hasil acak, sistem belum dapat membedakan jenis dan lokasi manipulasi secara otomatis. Contoh visual hasil ekstraksi setelah manipulasi dan tanpa manipulasi masing-masing ditunjukkan pada Gambar 3 dan Gambar 4.



Gambar 3. Hasil Ekstraksi *Watermark* pada Citra dengan Manipulasi

Journal : Jurnal Rekayasa Sistem Informasi dan Teknologi (JRS
Publisher : Yayasan Nuraini Ibrahim Mandiri
ISSN : e-ISSN 3025-888X
Volume / Issue / Year/ Page : Vol. 4 No. 1 (2026): Agustus/ Hal 53-66

Gambar 4. Hasil Ekstraksi Watermark *pada Citra Tanpa Manipulasi*

Analisis Ruang Kunci dan Brute-Force

Keandalan sistem terhadap percobaan *password* dipengaruhi oleh rangkaian SHA-256, PRNG, dan Fisher-Yates Shuffle. Setiap *password* menghasilkan *seed*, susunan piksel *watermark*, dan lokasi penyisipan yang berbeda. Oleh karena itu, penggunaan *password* yang tidak sesuai menyebabkan bit diambil dari lokasi berbeda dan *watermark* tidak dapat diekstraksi dengan benar. Dalam serangan *brute-force*, penyerang harus mencoba kandidat *password* satu per satu dan menjalankan kembali seluruh proses ekstraksi. Secara teoretis, apabila setiap digit dapat berisi angka 0 sampai 9, *password* 18 digit memiliki maksimum 10^{18} kombinasi sehingga pencarian menyeluruh memerlukan usaha komputasi yang besar. Namun, ruang pencarian praktis dapat lebih kecil karena penelitian ini menggunakan NIP yang memiliki struktur tertentu dan sebagian digitnya mungkin dapat diperkirakan. SHA-256, PRNG, dan Fisher-Yates juga tidak menambah ruang *password* secara terpisah karena seluruhnya dikendalikan oleh *password* yang sama. Dengan demikian, mekanisme yang diterapkan mempersulit rekonstruksi menggunakan *password* yang salah, tetapi belum dinyatakan setara dengan sistem keamanan kriptografis 256-bit.

KESIMPULAN

Kombinasi *Password-Based Scrambling* dan *Least Significant Bit* (LSB) berhasil diterapkan untuk autentikasi citra dokumentasi. Penyisipan mempertahankan kualitas visual dengan rata-rata MSE 0,0635, PSNR 62,78 dB, dan SSIM 0,9995. Tanpa manipulasi, *watermark* dapat diekstraksi sempurna dengan BER 0 dan NC 1. Setelah kompresi, *cropping*, dan *resizing*, BER meningkat hingga sekitar 0,5 dan NC turun hingga sekitar 0,59 sehingga *watermark* tidak dapat dikenali meskipun nilai PSNR pada kompresi masih tinggi. Temuan ini menegaskan bahwa metrik kualitas visual harus dibaca bersama metrik kemiripan *watermark* hasil ekstraksi. Sistem mampu menunjukkan bahwa citra telah berubah, tetapi belum dapat mengidentifikasi jenis, lokasi, dan tingkat manipulasi secara otomatis. Selain itu, ruang kunci praktis dipengaruhi oleh struktur NIP 18 digit yang digunakan sebagai *password*. Pengembangan selanjutnya dapat menerapkan lokalisasi blok yang dimanipulasi, klasifikasi serangan, domain DCT/DWT untuk skema *semi-fragile*, fungsi derivasi kunci yang lebih kuat, serta antarmuka web atau desktop agar sistem dapat digunakan tanpa Google Colab.

Pernyataan mengenai Penggunaan Kecerdasan Buatan (AI).

AI digunakan dalam penyusunan naskah ini. Penulis menggunakan perangkat kecerdasan buatan semata-mata untuk membantu perbaikan bahasa, pemeriksaan tata bahasa, serta penyuntingan demi kejelasan dan keterbacaan. Penulis tetap bertanggung

jawab penuh atas akurasi, orisinalitas, integritas, dan konten akademis naskah tersebut. Seluruh konten yang dibantu oleh AI telah ditinjau dan diverifikasi oleh penulis sebelum naskah diserahkan.

Konflik kepentingan

Penulis menyatakan tidak terdapat konflik kepentingan dalam pelaksanaan penelitian maupun penyusunan artikel ini.

Kontribusi Penulis

Konseptualisasi, Angeli Khairunissa Aulia Rahma dan Bagus Satrio Waluyo Poetro; pengumpulan data, Angeli Khairunissa Aulia Rahma; perancangan dan implementasi sistem, Angeli Khairunissa Aulia Rahma; validasi dan analisis hasil, Angeli Khairunissa Aulia Rahma dan Bagus Satrio Waluyo Poetro; penulisan—penyusunan draf awal, Angeli Khairunissa Aulia Rahma; penulisan—peninjauan dan penyuntingan, Bagus Satrio Waluyo Poetro. Seluruh penulis telah membaca dan menyetujui versi akhir naskah ini.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Universitas Islam Sultan Agung serta Sekretariat Daerah Provinsi Jawa Tengah atas dukungan, fasilitas, dan ketersediaan data yang membantu pelaksanaan penelitian ini.

DAFTAR PUSTAKA

Aberna, P., & Agilandeeswari, L. (2024). Optimal semi-fragile watermarking based on maximum entropy random walk and Swin Transformer for tamper localization. IEEE Access, 12. https://doi.org/10.1109/ACCESS.2024.3370411

Aberna, P., & Agilandeeswari, L. (2025). PoWBWM: Proof of work consensus cryptographic blockchain-based adaptive watermarking system for tamper detection applications. Alexandria Engineering Journal, 112, 510–537. https://doi.org/10.1016/j.aej.2024.10.016

Aberna, P., & Agilandeeswari, L. (2026). A comprehensive review on fragile and semi-fragile based watermarking systems for content authentication and tamper detection applications: Open issues, challenges and future directions. Multimedia Tools and Applications, 85, 200. https://doi.org/10.1007/s11042-026-21290-x

Adi, P. W., Wibowo, A., Aryotejo, G., & Ernawan, F. (2023). Fragile watermarking for image authentication using dyadic Walsh ordering. International Journal of Advances in Intelligent Informatics, 9(3). https://doi.org/10.26555/ijain.v9i3.1017

Al Najjar, Y. (2024). Comparative analysis of image quality assessment metrics: MSE, PSNR, SSIM, and FSIM. International Journal of Science and Research, 13(3), 110–114. https://doi.org/10.21275/SR24302013533

Al-Otum, H. M., & Ellubani, A. A. A. (2022). Secure and effective color image tampering detection and self restoration using a dual watermarking approach. Optik, 262, 169280. https://doi.org/10.1016/j.ijleo.2022.169280

Alveda, A., Rakhmawati, L., Tjahyaningtijas, R. H. P. A., & Kartini, U. T. (2024). Penyisipan watermark menggunakan metode LSB untuk autentikasi citra medis. Jurnal Teknik Elektro, 13, 273–280. https://doi.org/10.26740/jte.v13n3.p273-280

Aminuddin, A., & Ernawan, F. (2022a). AuSR1: Authentication and self-recovery using a new image inpainting technique with LSB shifting in fragile image watermarking. Journal of King Saud University - Computer and Information Sciences, 34(8), 5822–5840. https://doi.org/10.1016/j.jksuci.2022.02.009

Aminuddin, A., & Ernawan, F. (2022b). AuSR2: Image watermarking technique for authentication and self-recovery with image texture preservation. Computers & Electrical Engineering, 102, 108207. https://doi.org/10.1016/j.compeleceng.2022.108207

Durstenfeld, R. (1964). Algorithm 235: Random permutation. Communications of the ACM, 7(7), 420. https://doi.org/10.1145/364520.364540

Ernawan, F., Adi, P. W., Liew, S. C., Sarwoko, E. A., & Winarno, E. (2022). Fast image watermarking based on signum of cosine matrix. Indonesian Journal of Electrical Engineering and Computer Science, 25(3), 1383–1391. https://doi.org/10.11591/ijeecs.v25.i3.pp1383-1391

Faheem, Z. B., Hanif, D., Arslan, F., Ali, M., Hussain, A., Ali, J., & Baz, A. (2023). An edge inspired image watermarking approach using compass edge detector and LSB in cybersecurity. Computers & Electrical Engineering, 111, 108979. https://doi.org/10.1016/j.compeleceng.2023.108979

Fauzi, I., & Khairani, M. (2025). Analisis perbandingan kapasitas penyisipan data dan kualitas citra dalam teknik steganografi LSB dan MSB. Jurnal Ilmu Komputer dan Sistem Informasi, 4, 344–355. https://doi.org/10.70340/jirsi.v4i3.236

Firmansyah, M. A., & Tahir, M. (2026). Integrasi algoritma SHA-256 dan AES untuk pengamanan kredensial dan data sensitif. Jurnal Komputer Teknologi Informasi Sistem Informasi, 5(1), 462–468. https://doi.org/10.62712/juktisi.v5i1.1032

Jana, M., Jana, B., & Joardar, S. (2022). Local feature based self-embedding fragile watermarking scheme for tampered detection and recovery utilizing AMBTC with fuzzy logic. Journal of King Saud University - Computer and Information Sciences, 34. https://doi.org/10.1016/j.jksuci.2021.12.011

Kosuru, S. N. V. J. D., Swain, G., Kumar, N., & Pradhan, A. (2022). Image tamper detection and correction using Merkle tree and remainder value differencing. Optik, 261, 169212. https://doi.org/10.1016/j.ijleo.2022.169212

Makhrib, Z. F., & Karim, A. A. (2022). A hybrid digital image watermarking by using DWT and LSB method. Iraqi Journal of Computers, Communications, Control and Systems Engineering, 22(4), 115–126. https://doi.org/10.33103/uot.ijccce.22.4.9

Ma, K., Teng, L., Wang, X., & Meng, J. (2021). Color image encryption scheme based on the combination of the Fisher-Yates scrambling algorithm and chaos theory. Multimedia Tools and Applications, 80, 24737–24757. https://doi.org/10.1007/s11042-021-10847-7

Maulid, E., Pradana, A. N., & Kurniawan, R. (2026). Perbandingan metode watermarking Singular Value Decomposition dan Discrete Wavelet Transform untuk perlindungan hak cipta. Jurnal Sentinel, 6(1), 648–654. https://doi.org/10.56622/sentineljournal.v6i1.64

Neena Raj, N. R., & Shreelekshmi, R. (2022). Fragile watermarking scheme for tamper localization in images using logistic map and singular value decomposition. Journal of Visual Communication and Image Representation, 85, 103500. https://doi.org/10.1016/j.jvcir.2022.103500

Ouyang, J., Huang, J., & Wen, X. (2023). A semi-fragile reversible watermarking method based on QDFT and tamper ranking. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-023-16963-w

Permana, F. R., Setiyanto, R. F., & Fauzi, A. R. (2023). Image steganography dengan menggunakan metode LSB pada Python. Jurnal Pendidikan Teknologi Informasi, 2(1), 1–7.

Purba, B., Dalimunthe, Y. A., Hasnita, U., & Putra, P. H. (2025). Teknik keamanan multimedia menerapkan metode Least Significant Bit untuk watermarking citra digital. Journal Global Tecnology Computer, 4(2), 139–149. https://doi.org/10.47065/jogtc.v4i2.7325

Putra, I. P. K., & Supriana, I. W. (2024). Analisis perbandingan kualitas citra hasil steganografi DCT dan LSB berdasarkan parameter RMSE dan PSNR. Jurnal Nasional Teknologi Informasi dan Aplikasinya, 2, 609–616. https://doi.org/10.24843/JNATIA.2024.v02.i03.p20

Rezaei, M., & Taheri, H. (2022). Digital image self-recovery using CNN networks. Optik, 264, 169345. https://doi.org/10.1016/j.ijleo.2022.169345

Senol, A., Elbasi, E., Topcu, A. E., & Mostafa, N. (2023). A semi-fragile, inner-outer block-based watermarking method using scrambling and frequency domain algorithms. Electronics, 12(4), 1065. https://doi.org/10.3390/electronics12041065

Setiawati, I., Hermanto, M. T., & Ujianto, E. I. H. (2023). Implementation of digital watermarking on images using the Least Significant Bit method. International Journal of Engineering, Technology and Natural Sciences, 5(1), 10–18. https://doi.org/10.46923/ijets.v5i1.191

Sharma, S., Zou, J. J., & Fang, G. (2022). A novel multipurpose watermarking scheme capable of protecting and authenticating images with tamper detection and localisation abilities. IEEE Access, 10, 85677–85700. https://doi.org/10.1109/ACCESS.2022.3198963

Sharma, S., Zou, J. J., Fang, G., Shukla, P., & Cai, W. (2024). A review of image watermarking for identity protection and verification. Multimedia Tools and Applications, 83, 31829–31891. https://doi.org/10.1007/s11042-023-16843-3

Simangunsong, V., Hutasoit, Y. R., & Siallagan, D. (2025). Analisis terhadap keamanan password menggunakan hash SHA-256. Jurnal Quancom, 3(1). https://doi.org/10.62375/jqc.v3i1.431

Singh, B., & Kasana, G. (2024). A review of digital watermarking techniques: Current trends, challenges and opportunities. Web Intelligence, 22. https://doi.org/10.3233/WEB-230280

Tran, D. N., Zepernick, H.-J., & Chu, T. M. C. (2022). LSB data hiding in digital media: A survey. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 9(30). https://doi.org/10.4108/eai.5-4-2022.173783

Vaidya, S. P., Kandala, R. N. V. P. S., Mouli, P. V. S. S. R. C., Zaini, H. G., Jaffar, A., Paramasivam, P., & Ghoneim, S. S. M. (2025). A robust fragile watermarking approach for image tampering detection and restoration utilizing hybrid transforms. Scientific Reports, 15, 17645. https://doi.org/10.1038/s41598-025-01297-4

Wan, W., Wang, J., Zhang, Y., Li, J., Yu, H., & Sun, J. (2022). A comprehensive survey on robust image watermarking. Neurocomputing, 488, 226–247. https://doi.org/10.1016/j.neucom.2022.02.083

Yacoub, M. H., Fetteha, M. A., Sharobim, B. K., & Zayed, H. H. (2023). Semi-fragile watermark for the authentication and recovery of tampered images. Proceedings of the 5th Novel Intelligent and Leading Emerging Sciences Conference, 194–199. https://doi.org/10.1109/NILES59815.2023.10296710

Yuan, Z., Zhang, X., Wang, Z., & Yin, Z. (2024). Semi-fragile neural network watermarking for content authentication and tampering localization. Expert Systems with Applications, 238, 121315. https://doi.org/10.1016/j.eswa.2023.121315