

Implementasi Watermarking Digital Metode LSB (Least Significant Bit) Acak untuk Keamanan Data Visual

Rovent Van Hougend Ambarita¹⁾

¹ S-1 Teknik Elektro, Fakultas Teknik, Universitas Negeri Surabaya, Surabaya, Indonesia.

a)Corresponding author: rovent.22129@mhs.unesa.ac.id

ABSTRAK

Perkembangan teknologi yang semakin modern mempermudah dalam mengakses data dan meningkatkan risiko penyalahgunaan data, termasuk pelanggaran hak cipta. Untuk mengatasi masalah ini, diperlukan metode perlindungan yang mampu menjaga keamanan data sekaligus melindungi hak cipta pada media visual. Penelitian ini mengusulkan metode watermarking digital berbasis password dalam menyisipkan informasi pada citra digital yang aman dan tahan terhadap gangguan. Proses penyisipan (embedding) menggunakan teknik Least Significant Bit (LSB) dengan posisi acak yang ditentukan password, memastikan keamanan dan kerahasiaan watermark. Metode ini dievaluasi melalui metrik kualitas citra seperti Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), dan Structural Similarity Index Measure (SSIM). Hasil dari penelitian mampu menunjukkan metode yang diusul berhasil menyisipkan watermark tanpa mengurangi kualitas citra host secara signifikan. Hasil eksperimen menunjukkan bahwa metode ini efektif dalam menjaga kualitas citra host setelah proses penyisipan watermark, dengan PSNR rata-rata di atas 40 dB. Serta dilakukan pengekstrakan untuk mendapatkan watermark kembali.

Kata Kunci: Digital Watermarking, Least Significant Bit, Citra Digital.

Pendahuluan

Di era digital yang berkembang pesat, data visual seperti gambar dan video ataupun data lainnya menjadi salah satu bentuk informasi yang sering digunakan dalam berbagai bidang. Data bersifat privasi dan perlu adanya perlindungan. Peningkatan jumlah penggunaan data visual rentan terhadap risiko penyalahgunaan informasi, pelanggaran hak cipta, serta manipulasi data. Maka dari itu, diperlukan langkah-langkah untuk perlindungan untuk mencegah hal tersebut[1].

Salah satu metode yang efektif untuk menjaga hak cipta dan keaslian data visual adalah dengan teknik digital watermarking. Dengan teknik ini dapat dilakukan penyisipan informasi tertentu seperti, identitas pemilik atau hak cipta ke dalam media digital tanpa mengurangi kualitas aslinya[2].

Teknik digital watermarking yang dirancang dengan menyisipkan data informasi ke dalam citra digital secara tersembunyi, sehingga tidak terlihat oleh mata manusia. Tujuan dari penyisipan ini adalah agar pihak yang tidak berwenang tidak mudah mengakui hak kepemilikan terhadap sebuah citra sehingga dapat melindungi citra[4]. Teknik ini juga dapat digunakan untuk menyisipkan informasi atau pesan yang ingin disampaikan kepada pihak yang dituju[3]. Dengan berbagai keunggulannya, teknik ini dapat digunakan sebagai metode perlindungan hak cipta serta verifikasi keaslian foto digital dalam format *Portable Network Graphics* (PNG), *Bitmap Picture* (BMP), dan *Joint Photographic Experts Group* (JPEG).

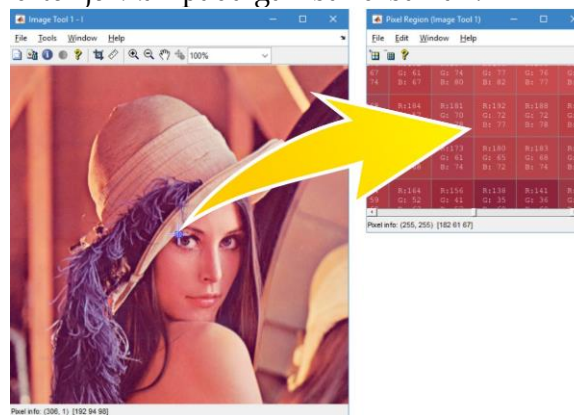
Least Significant Bit merupakan salah satu teknik dalam Steganografi dengan mengganti bit-bit terakhir dengan bit pesan yang akan disisipkan[5]. Metode Least Significant Bit (LSB) merupakan teknik watermarking yang sederhana dan banyak digunakan karena kemudahan dalam implementasinya[4]. Namun, kelemahan utama dari metode LSB konvensional adalah posisi

penyisipan yang tetap dan mudah ditebak, sehingga rentan terhadap serangan. Untuk mengatasi hal ini, penelitian ini mengusulkan teknik LSB acak yang dikendalikan oleh password, di mana lokasi penyisipan watermark ditentukan melalui algoritma berbasis password. Pendekatan ini diharapkan dapat meningkatkan keamanan dan kerahasiaan watermark tanpa mengurangi kualitas citra host.

Kajian Pustaka

Citra Digital

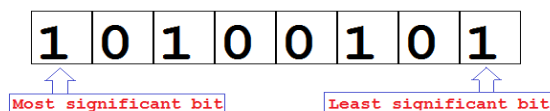
Citra digital adalah representasi visual dari suatu gambar atau objek dalam format digital yang dapat diproses, disimpan, atau ditampilkan oleh perangkat komputer[8]. Citra ini terdiri dari piksel (picture elements), yang merupakan unit terkecil dari gambar. Setiap piksel memiliki nilai yang merepresentasikan warna atau intensitas cahaya pada titik tertentu dalam citra. Untuk representasi citra beserta piksel penyusun ditunjukkan pada gambar dibawah.



Gambar 1. (Sumber : Pemrograman MATLAB. (2017, July 26). Pengolahan citra digital)

Least Significant Bit (LSB)

Least significant bit merupakan sebuah bagian dalam barisan data biner yang memiliki nilai paling tidak signifikan[6]. Letak dari lsb sendiri adalah paling kanan dari barisan bit, sedangkan letak paling kiri dari barisan bit disebut MSB (Most Significant Bit).



Gambar 2. (Sumber : Pemrograman MATLAB, 2023).

Metode LSB (Least Significant Bit) dalam steganografi untuk menyisipkan pesan rahasia ke dalam citra dengan mengganti bit terakhir setiap piksel dengan bit pesan. Proses ini dimulai dengan membagi citra menjadi blok piksel, mengubah pesan menjadi kode biner, lalu menggantikan bit terakhir piksel dengan bit pesan. Hasilnya adalah citra stego yang mengandung pesan rahasia, yang dapat diekstraksi oleh penerima dengan membaca bit terakhir piksel dan mengembalikannya ke bentuk pesan asli.

Peak Signal to Noise Ratio (PSNR)

PSNR dan MSE adalah dua parameter yang digunakan untuk membandingkan kualitas sebuah citra. Perhitungan PSNR dilakukan untuk membandingkan kesamaan antara citra host dan citra terwatermark. Untuk melakukan perhitungan PSNR perlu dilakukan perhitungan terhadap MSE terlebih dahulu[1]. MSE dapat dihitung dengan rumus :

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} [f(i,j) - g(i,j)]^2$$

Nilai PSNR yang tinggi menunjukkan Tingkat kemiripan dari dua buah citra. Nilai PSNR dapat dihitung dengan rumus :

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

MSE tidak memiliki satuan sedangkan PSNR satuannya adalah desibel.

Metode

Penelitian ini menggunakan pendekatan eksperimental untuk menguji efektivitas metode watermarking digital berbasis LSB acak dalam menjaga kualitas citra host. Pada tahap ini citra host dan citra watermark dipersiapkan. Algoritma penyisipan watermark menggunakan Teknik LSB (Least Significant Bit) yang dimana watermark disisipkan dalam bit-bit paling rendah dari piksel citra host.

Teknik berbasis password menambahkan lapisan keamanan pada proses penyisipan watermark. Password digunakan untuk mengontrol dan memastikan bahwa proses penyisipan dan ekstraksi watermark hanya dapat dilakukan oleh pihak yang memiliki password yang tepat. Ini meningkatkan ketahanan watermark terhadap usaha penghapusan atau manipulasi..

Hasil dan Pembahasan

Alat dan Bahan

a) Alat

Alat yang digunakan adalah processor Intel(R) Celeron(R) N4020 CPU 1.10GHz 1.10 GHz dan matlab online.

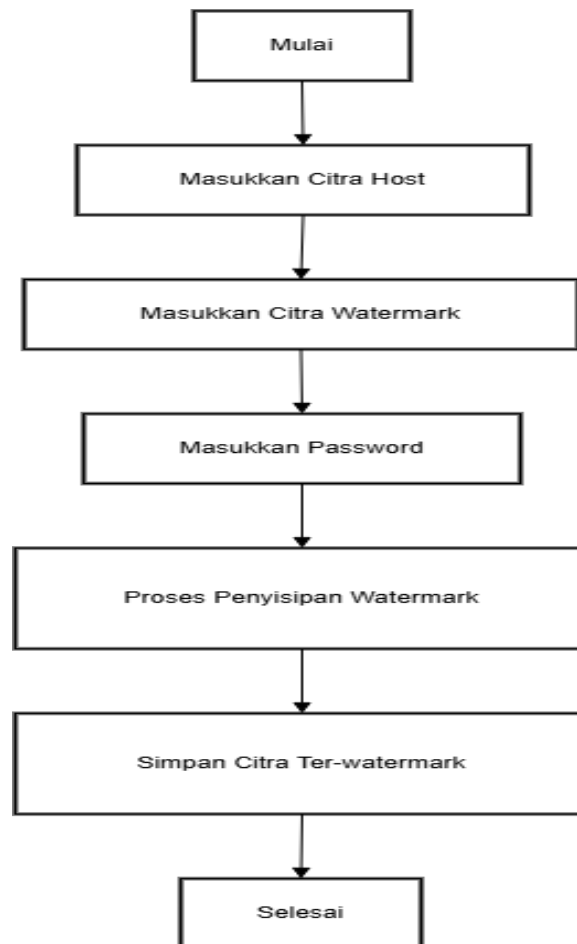
b.) Bahan

Bahan yang digunakan adalah 3 citra digital berwarna dengan citra host berukuran 427x640 dengan format *.jpg, 2 citra host berukuran 360x360 dengan format *.png, dan citra watermark dengan ukuran 200x200 dengan format *.png.

Prosedur Penelitian

1. Penyisipan Watermark

Tahapan penyisipan watermark menggunakan metode least significant bit ditunjukkan pada Gambar 3.

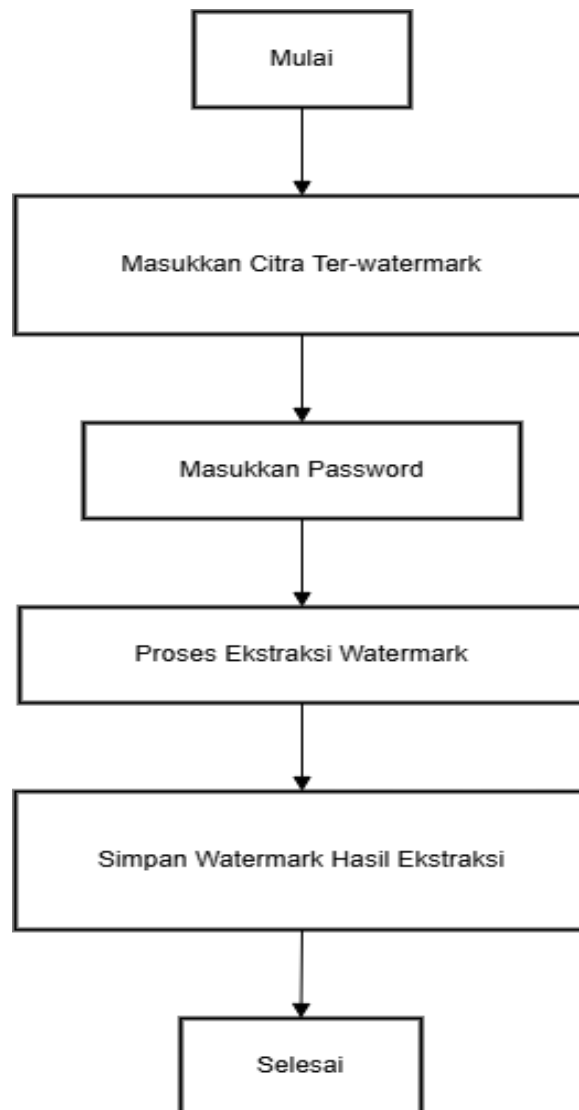


Gambar 3. Flowchart Penyisipan

Pada proses penyisipan watermark dilakukan peng-inputan citra host dan citra watermark yang akan di proses. Kemudian dengan memasukkan password maka system akan mengacak bit-bit watermark ke dalam citra host sehingga posisi penyisipan tidak dapat di tebak dengan mudah dan data posisi penyisipan akan tersimpan tersendiri.

2. Ekstraksi watermark

Proses ekstraksi watermark dari citra terwatermark ditunjukkan pada Gambar 4.



Gambar 4. Flowchart Ekstraksi

Seperti pada flowchart diatas, proses pengestraksi citra watermark kembali dilakukan dengan memasukkan data dan password yang digunakan ketika awal penyisipan sehingga watermark dapat di peroleh kembali.

Hasil dan Pembahasan

Setelah merancang sistem watermarking adalah mensimulasikan sistem tersebut menggunakan MATLAB. Dalam penelitian ini, metode watermarking yang diterapkan adalah *Least Significant Bit (LSB)*, di mana citra watermark disisipkan ke dalam citra host dengan mengganti bit paling tidak signifikan (bit terakhir) dari setiap piksel citra host. Teknik ini memungkinkan watermark disembunyikan di dalam citra tanpa menyebabkan perubahan yang mencolok pada tampilan visual citra host, karena perubahan yang terjadi sangat kecil dan hampir tidak terlihat oleh mata manusia.

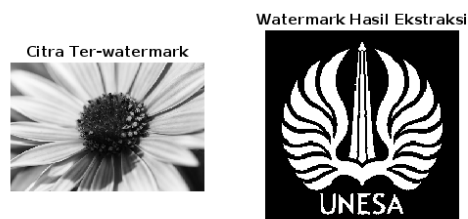
Hasil uji

Tabel 1. Hasil pengujian

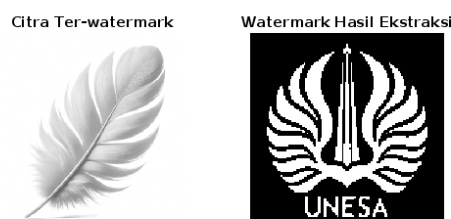
Citra terwatermark	MSE	PSNR	SSIM
	0.0629	60.14 dB	0.9995
	0.0782	59.20 dB	0.9991
	0.0677	59.82 dB	0.9996

Dari hasil perhitungan pada tabel 1 hasil pengujian menunjukkan bahwa kualitas citra setelah watermarking tetap sangat tinggi. Untuk citra pertama menunjukkan nilai *PSNR* 60.14 dB, *MSE* 0.0629, dan *SSIM* 0.9995 yang berarti perubahan sangat kecil dan hampir tidak terlihat. Pada citra kedua menunjukkan nilai *PSNR* 59.20 dB, *MSE* 0.0782, dan *SSIM* 0.9991, yang juga menunjukkan perbedaan minimal antara citra asli dan citra ter-watermark. Dan citra yang ketiga juga menunjukkan nilai *PSNR* 59.82 dB, *MSE* 0.0677, dan *SSIM* 0.9996 yang berarti struktur citra tetap terjaga dengan baik. Secara keseluruhan, nilai *PSNR* di atas 40 dB dan *SSIM* mendekati 1 menandakan bahwa watermarking tidak merusak citra dan kualitasnya tetap optimal.

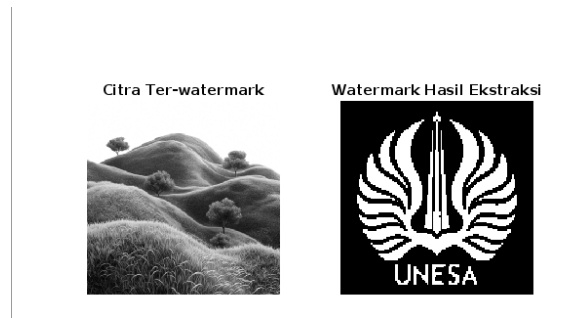
Hasil Ekstraksi



Gambar 5. Hasil ekstraksi citra pertama



Gambar 6. Hasil ekstraksi citra kedua



Gambar 7. Hasil ekstraksi citra ketiga

Setelah watermark disisipkan dan dilakukan perhitungan untuk mengukur kualitas serta perubahan pada citra yang ter-watermark, langkah selanjutnya adalah melakukan ekstraksi untuk memperoleh kembali watermark yang disisipkan. Untuk hasil ekstraksi ditampilkan pada gambar diatas dan dapat dinyatakan bahwa hasil ekstraksi berhasil.

Kesimpulan

Berdasarkan hasil dari percobaan yang dilakukan pada penyisipan dan proses ekstraksi watermark menggunakan metode Least Significant Bit (LSB), dapat disimpulkan bahwa proses watermarking ini berhasil dalam mempertahankan kualitas citra host dengan sangat baik. Hasil perhitungan PSNR, MSE, dan SSIM menunjukkan bahwa perubahan yang terjadi pada citra asli sangat kecil, bahkan hampir tidak terdeteksi oleh mata manusia. Nilai PSNR yang sangat tinggi (lebih dari 59 dB) menunjukkan kualitas citra yang hampir tidak terpengaruh oleh penyisipan watermark, sementara nilai MSE yang rendah mengindikasikan bahwa perbedaan antara citra asli dan citra ter-watermark sangat minim. Nilai SSIM yang sangat mendekati 1 menandakan bahwa struktur dan informasi utama citra tetap terjaga dengan sangat baik meskipun watermark telah disisipkan.

Selain itu, proses ekstraksi watermark juga berhasil dengan baik, yang berarti bahwa watermark yang disisipkan dapat diekstrak kembali dengan menggunakan password yang sesuai. Ini menunjukkan bahwa sistem watermarking ini dapat digunakan untuk perlindungan hak cipta dan integritas citra secara efektif.

Daftar Pustaka

- [1] Kurniawan, N., Siradjuddin, I. A., & Muntasa, A. (2015). "Keamanan citra dengan watermarking menggunakan pengembangan algoritma least significant bit," *J. Informatika*, vol. 13, no. 1, pp. 9–14, 2015, doi: 10.9744/informatika.13.1.9-14.
- [2] A. Suheryadi, "Penerapan digital watermark sebagai validasi keabsahan gambar digital dengan skema blind watermark," *J. Teknol. Terapan*, vol. 3, no. 2, Sep. 2017, ISSN: 2477-3506.
- [3] Al Jum'ah, M. N., & Sarimuddin. (2024). "Implementasi steganografi metode least significant bit (LSB) untuk menyembunyikan file pesan dalam gambar," *J. Informatika dan Rekayasa Perangkat Lunak*, vol. 6, no. 1, pp. 102–108, 2024, doi: 10.xxxx/jirpl.2024.xxxx.
- [4] B. W. A. Putro and Febriani, *Aplikasi watermarking dengan metode least significant bit menggunakan MATLAB*, 2017.
- [5] Alveda, A., Rakhmawati, L., & Tjahyaningtijas, R. H. P. A. (n.d.). "Penyisipan watermark menggunakan metode LSB (Least Significant Bit) untuk autentikasi citra medis," *S1 Teknik Elektro, Fakultas Teknik, Universitas Negeri Surabaya*.
- [6] Sutisna, L. A. (n.d.). "Implementasi digital watermarking menggunakan metode LSB (Least Significant Bit) untuk menyisipkan teks dan gambar ke dalam karya digital," *Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur*. 2016.
- [7] Niswati, Z. (n.d.). "Steganografi berbasis Least Significant Bit (LSB) untuk menyisipkan gambar ke dalam citra gambar," *Faktor Exacta*, vol. 5, no. 2, pp. 181–191, n.d.
- [8] A. Pamungkas, "Pengolahan citra digital," *Pemrograman MATLAB*, Jul. 26, 2017.