JNATIA Volume 3, Nomor 2, Februari 2025 p-ISSN: 2986-3929
Jurnal Nasional Teknologi Informasi dan Aplikasinya e-ISSN: 3032-1948

Penerapan Steganografi untuk Pengamanan Konten Gambar dalam Media Sosial

Gede Eka Putra Wijaya[1], I Gusti Agung Gede Arya Kadnyanan[2]

Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Udayana
Jalan Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
[1]deeka2684@gmail.com
[2]gungde@unud.ac.id

Abstract

The rapid development of technology has significantly impacted various aspects of life, especially social media. Social media platforms are not only used for interaction but also for building branding through content uploads. However, this raises concerns about unauthorized use of content that violates Intellectual Property Rights (IPR). Digital watermarking using steganography, specifically the Least Significant Bit (LSB) technique, can protect content by hiding messages without degrading visual quality. This study tests the insertion of text into digital images using two sample logos of different sizes. The test results show Mean Square Error values ranging from 1.8 to 2 and Peak Signal-to-Noise Ratio values between 94.9 and 95.3, indicating excellent visual quality and almost imperceptible differences. This technique effectively protects content from unauthorized use.

Keywords: *Steganography, Least Significant Bit (LSB), Social Media content, Digital Watermarking, Intellectual Property Rights (IPR)*

1. Pendahuluan

Perkembangan era yang cepat menyebabkan dampak yang begitu signifikan, terutama dalam domain teknologi. Media sosial merupakan bagian penting dari kehidupan sehari-hari masyarakat di era digital yang semakin maju ini. Mereka tidak hanya menjadi *platform* untuk berinteraksi dan berbagi informasi, tetapi juga sering digunakan untuk menyimpan dan membagikan konten atau karya mereka untuk membangun *branding* dengan mengunggah karya mereka. Namun, seiring dengan kemajuan teknologi, ada kekhawatiran tentang penggunaan konten tanpa seizin pemilik konten yang berkaitan dengan Hak Kekayaan Intelektual (HKI). Isu hak kekayaan intelektual telah menjadi sangat penting dalam era digital yang berkembang pesat. Hak kekayaan intelektual adalah hak yang diberikan kepada pencipta untuk melindungi karyanya yang bersifat intelektual. Perlindungan hak kekayaan intelektual menjadi sangat penting dalam kehidupan karena tantangan yang dihadapi meningkat seiring dengan penggunaan teknologi digital. Perlindungan kekayaan intelektual (hak cipta, paten, merek dagang, desain industri, dan bentuk kekayaan intelektual lainnya) juga sangat penting untuk mengembangkan inovasi dan kreativitas serta mendorong pembangunan ekonomi [1]. *Digital watermarking* salah satu cara untuk mengamankan konten di sosial media, steganografi merupakan suatu metode yang biasa digunakan untuk penyisipan pesan kedalam suatu media sebagi *covernya*. Steganografi merupakan metode menyembunyikan pesan dalam media digital sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu pesan di dalam media tersebut [2]. Dalam hal media sosial, steganografi menjadi semakin relevan karena memungkinkan pengguna melindungi konten pribadi mereka dengan menyisipkan identitas pada konten tanpa merusak visualisasi dari konten tersebut. Salah satu teknik stegano grafi yang dapat digunakana dalah *Leat Signifikan Bit* (LSB). Steganografi dengan Teknik LSB memiliki beberapa keunggulan dibandingkan dengan metode steganografi lainnya. Satu keuntungannya adalah sangat mudah untuk diterapkan dan tidak membutuhkan algoritma yang kompleks. Keuntungan lainnya dari steganografi LSB adalah kapasitas penyematan yang tinggi, yang berarti bahwa sejumlah besar data dapat disembunyikan dalam satu gambar. Selain itu, steganografi LSB tidak mempengaruhi kualitas visual gambar

p-ISSN: 2986-3929
e-ISSN: 3032-1948

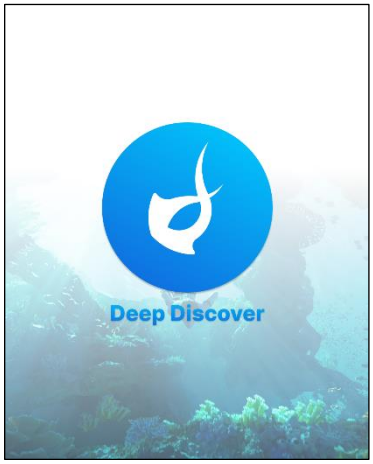
secara signifikan, sehingga pengamat sulit menemukan pesan tersembunyi [3].

2. Metode Penelitian

2.1. Pengumpulan Data

Pada penelitian ini data yang digunakan oleh sistem yang dikembangkan adalah data citra atau gambar yang akan pengguna unggah ke media sosial. Data uji yang digunakan merupakan 2 sampel karya digital berupa logo.

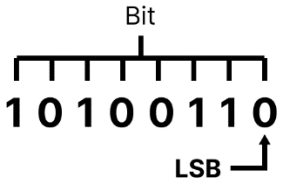
Tabel 1. Data gambar yang diuji

Karya 1	Karya 2
	
1080 x 1080 piksel	1080 x 1350 piksel

Pada tablel 1 terdapat dua gambar yang digunakan untuk penelitian ini, karya 1 merupakan gambar dengan ukuran 1080 x 1080 piksel, dan karya 2 merupakan gambar dengan ukuran 1080 x1350 piksel.

2.2. Least Significant Bit (LSB)

Metode ini memanipulasi bit terakhir yang tidak memiliki nilai berarti atau terkecil pada citra gambar.



Gambar 1. Least Significant Bit (LSB)

Metode steganografi LSB memungkinkan penyembunyian informasi rahasia dalam gambar digital tanpa mengubah penampilannya secara signifikan. Misalkan kita menggunakan gambar berukuran 1080 x 1080 piksel sebagai contoh. Dalam gambar ini, setiap piksel memiliki tiga komponen warna RGB (*red, green, blue*), direpresentasikan masing-masing oleh 8 bit, sehingga total 24 bits per piksel. Dengan demikian, kita dapat menyimpan 3-bit pesan dalam setiap piksel dengan mengubah bit dari setiap komponen warna. Dengan total 1.166.400 piksel dalam gambar, kita dapat menyembunyikan total 3.499.200-bit atau sekitar 437.400-byte data yang disisipkan. Pesan rahasia, dalam bentuk urutan bit, akan disisipkan ke dalam bit terkecil (LSB) dari setiap

p-ISSN: 2986-3929
e-ISSN: 3032-1948

nilai piksel dalam gambar. Pesan ini akan tersembunyi di dalam gambar tanpa mengganggu penampilan visualnya secara signifikan. Proses ekstraksi pesan melibatkan pengekstrakan LSB dari setiap nilai piksel dalam gambar, dan urutan bit yang ditemukan akan dikonversi kembali menjadi pesan yang dapat dibaca. Dengan demikian, metode ini memungkinkan penyembunyian pesan yang cukup besar dalam gambar berukuran 1080x1080 piksel tanpa mengurangi kualitas visualnya secara nyata [4].

2.3. Analisis Kebutuhan

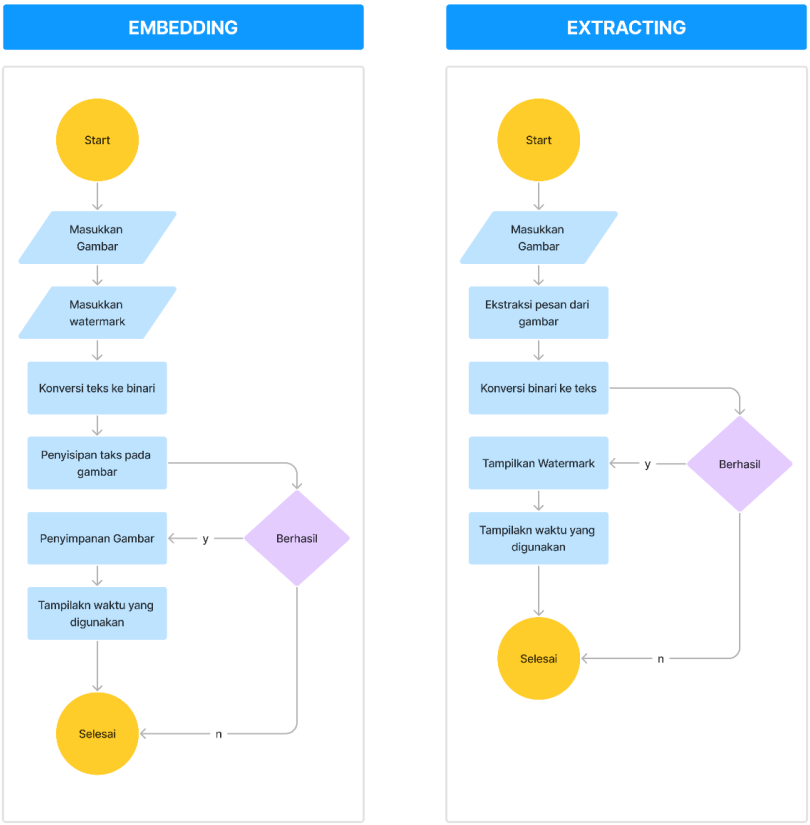
2.3.1. Kebutuhan *Input*

a. Media yang digunakan untuk *cover image* adalah gambar yang dengan format **.png.*
b. Pesan yang dimasukan adalah teks.

2.3.2. Kebutuhan *Output*

a. File gambar yang telah disisipkan teks degan format **.png.*
b. Pesan yang sebelumnya telah di sisipkan atau plain teks yang telah di ekstrak setelah proses dekripsi gambar stegano.

2.4. Perancangan Sistem



Gambar 2. Flowchart sistem.

Pada gambar 2 dijelaskan mengenai alur atau *flowchart* dari sistem yaitu proses *embedding* dan proses pengekstrakan.

p-ISSN: 2986-3929
e-ISSN: 3032-1948

2.5. Pengujian Sistem

Pengujian sistem dilakukan dengan mengukur kemiripan dua buah citra, citra pertama adalah citra sebelum dilakukan penyisipan dan citra kedua adalah citra setelah dilakukan penyisipan.Parameter yang digunakan adalah *Mean Square Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR). Parameter ini merupakan parameter yang sering digunakan sebagai indikator untuk mengukur kemiripan dua buah gambar. Semakin mirip kedua citra maka nilai MSE nya semakin mendekati nilai nol, untuk PSNR gambar dikatakan memiliki tingkat kemiripan yang rendah jika nilai PSNR di bawah 30 dB. Berikut merupakan persamaan yang digunakan untuk menghitung kedua paramater tersebut [5].

2.5.1. *Mean Square Error* (MSE)

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

2.5.2. *Peak Signal-to-Noise Ratio* (PSNR)

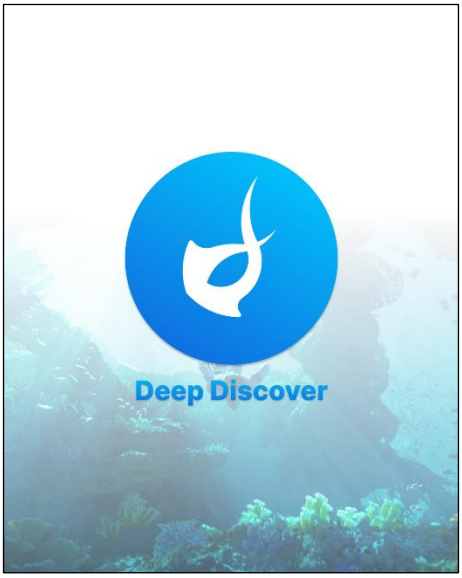
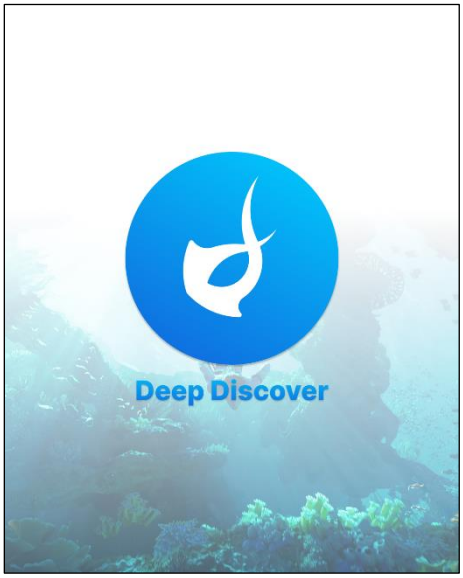
$$10 \, log_{10} \, \frac{255^2}{MSE} \quad (2)$$

3. Hasil dan Diskusi

3.1. Pengujian Citra

Setelah dilakukan proses *embedding* atau penyisipan teks kedalam gambar, akan dilakukan pembandingan antara gambar sebelum penyisipan dan setelah penyisipan.

Tabel 2. Pembandingan gambar sebelum dan setelah penyisipan

No	Sebelum	Sesudah
1		

p-ISSN: 2986-3929
e-ISSN: 3032-1948

No	Sebelum	Sesudah
2		

Terlihat dari tabel 2, tidak terdapat perbedaan yang signifikan antara kedua gambar jika dilihat secara langsung antara gambar yang belum disisipkan pesan dan gambar yang sudah disisipkan pesan.

3.2. Pengujian Akurasi

Berikut ini merupakan hasil pengukuran gambar sebelum dan setelah penyisipan menggunakan parameter MSE dan PSNR.

Tabel 3. Hasil pengukuran MSE dan PSNR

No	Gambar	MSE	PSNR
1	Karya 1	1,8	95,3
2	Karya 2	2,0	94,9

Dari tabel diatas dapat dilihat hasil dari pengukuran menggunakan parameter MSE dan PSNR, pada gambar karya 1 mendapatkan nilai MSE sebesar 1,8 dan PSNR sebesar 95,3 kemudian untuk gambar karya 2 mendapatkan nilai MSE sebesar 2,0 dan PSNR sebesar 94,9.

4. Kesimpulan

Berdasarkan penelitian yang telah dilakukan bahwa penyisipan watermarking berupa teks pada gambar konten media sosial berhasil dilakukan menggunakan metode *Least Significant Bit (*LSB) dan mampu memberi perlindungan yang cukup efektif dengan menyembunyikan informasi tanpa merusak estetika dari gambar asli. Dengan adanya informasi yang tersembunyi ini memastikan konten gambar dapat terlindungi dari penggunaan konten yang tidak tepat, karena dapat diidentifikasi secara akurat dan dibedakan berdasarkan informasi watermark yang telah disisipkan. Dalam penelitian ini citra yang digunakan adalah gambar yang akan di posting kemedia sosial, dalam pengujian menggunakan dua sampel gambar. Pengujian yang digunakan untuk mengukur akurasi dari hasil penyisipan adalah menggunakan parameter *Mean Square Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR). Berdasarkan hasil pengujian dari kedua sample gambar, gambar karya 1 mendapatkan nilai MSE sebesar 1,8 dan PSNR sebesar 95,3. Kemudian untuk gambar karya 2 mendapatkan nilai MSE 2,0 dan PSNR sebesar 94,9. Dari hasil tersebut menunjukan rata-rata perbedaan kuadrat per piksel antara gambar asli dan gambar yang dimodifikasi adalah 1,8 hingga 2 dan PSNR sebesar 94,9 hingga 95,3 menunjukkan kualitas yang sangat baik, juga menunjukkan perbedaan antara gambar asli dan gambar yang dimodifikasi hampir tidak terlihat walaupun setelah dilakukan penyisipan.

Daftar Pustaka

[1] M. E. Darnia, C. D. Monica, M. Munawardi, and R. Aprillia, “Perlindungan Hak Kekayaan Intelektual di Era Digital,” *JERUMI J. Educ. Relig. Humanit. Multidiciplinary*, vol. 1, no. 2, pp. 411–419, 2023, doi: 10.57235/jerumi.v1i2.1378.

[2] M. Syahril and H. Jaya, “Aplikasi Steganografi Pengamanan Data Nasabah di Standard Chartered Bank Menggunakan Metode Least Significant Bit dan RC4,” *Sensasi*, pp. 505–509, 2019, [Online].
Available: http://prosiding.seminar-id.com/index.php/sensasi/issue/archivePage%7C505

[3] M. Miftahul Amri, M. Waeno, and M. Zain Musa, “LSB Steganography to Embed Creator’s Watermark in Batik Digital Arts,” *Eng. Sci. Lett.*, vol. 2, no. 01, pp. 27–32, 2023, doi: 10.56741/esl.v2i01.301.

[4] A. Khuzaifi, F. Fauziah, and I. Fitri, “Teknik Steganography untuk Menyisipkan Pesan pada Sebuah Citra Menggunakan Metode Least Significant Bit (LSB),” *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, vol. 6, no. 3, pp. 417–423, 2022, doi: 10.35870/jtik.v6i3.461.

[5] A. Pamungkas, “Cara Menghitung Nilai MSE, RMSE, dan PSNR pada Citra Digital,” pemrogramanmatlab.com. [Online].
Available: https://pemrogramanmatlab.com/2017/06/04/cara-menghitung-nilai-mse-rmse-dan-psnr-pada-citra-digital/