Journal Global Tecnology Computer
Vol 4, No. 2, April 2025, Hal 139-149
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i2.7325
Website https://ejurnal.seminar-id.com/index.php/jogtc

Teknik Keamanan Multimedia Menerapkan Metode Least Significant Bit Untuk Watermarking Citra Digital

Bister Purba[1,*], Yulia Agustina Dalimunthe[2], Ulfa Hasnita[3], Azanuddin[4], Purwa Hasan Putra[5]

[1] Program Studi Teknologi Rekayasa Multimedia Grafis, Jurusan Teknik Komputer dan Informatika, Politeknik Negeri Medan, Medan, Indonesia
[2] Program Studi Manajemen Informatika, Jurusan Teknik Komputer dan Informatika, Politeknik Negeri Medan, Medan, Indonesia
[3] Program Studi Elektronika, Jurusan Teknik Elektro, Politeknik Negeri Medan, Medan, Indonesia
[4] Program Studi Teknik Komputer, Jurusan Teknik Komputer dan Informatika, Politeknik Negeri Medan, Medan, Indonesia
[5] Program Studi Teknologi Rekayasa Perangkat Lunak, Jurusan Teknik Komputer dan Informatika, Politeknik Negeri Medan, Medan, Indonesia
Jl. Dr. T. Mansur No.9, Padang Bulan, Medan Baru, Kota Medan, Sumatera Utara, Indonesia
Email: [1,*]bisterpurba@polmed.ac.id, [2]yuliadalimunthe@polmed.ac.id, [3]ulfahasnita@polmed.ac.id, [4]azanuddin@polmed.ac.id, [5]pputra@polmed.ac.id
(*: coressponding author)

Abstrak−Perkembangan konten digital telah membawa peluang baru bagi kejahatan klasik di bidang teknologi informasi, yaitu pembajakan. Konten-konten yang seharusnya menjadi property legal dari produsen dan secara legal dimiliki oleh orang tertentu, bisa dengan mudah disalahgunakan oleh pihak-pihak yang tidak bertanggungjawab termasuk pada SDS Bina Satria Mulia Medan. Digital watermarking dikembangkan sebagai salah satu jawaban untuk menentukan keabsahan pencipta atau pendistribusian suatu data digital dan integritas suatu data digital. Teknik watermarking bekerja dengan menyisipkan sedikit informasi yang menunjukkan kepemilikan, tujuan atau data lain, pada media digital tanpa mempengaruhi kualitasnya. Jadi pada citra digital, mata tidak bisa membedakan apakah citra tersebut disisipi watermark atau tidak. Adapun yang menjadi tujuan penelitian ini adalah bagaimana menjaga atau melindungi sebuah citra digital dari manipulasi atau pengubahan serta pemalsuan sebuah citra digital demi kepentingan dan tujuan pihak yang tidak diinginkan dengan menerapkan watermarking. Metode yang digunakan untuk watermarking citra digital adalah metode LSB (Least Significant Bit) yaitu dengan menyisipkan sebuah kode pada citra yang akan dilindungi namun tidak merubah substansi dari citra tersebut. Kode unik inilah yang akan menjadi tanda atau mark pada sebuah citra. Dengan adanya kode tersebut dapat diketahui keaslian sebuah citra. Klaim terhadap keaslian citra dapat dibuktikan dengan adanya kode unik yang tertanam pada citra tersebut. Pada proses analisa dilakukan penyisipan watermark "BINA SATRIA" terhadap citra berukuran 140x140 piksel sehingga berdasarkan langkah-langkah yang dilakukan, maka watermark yang sebelumnya disisipkan berhasil diektraksi kembali dari citra yang telah disisipakan watermark. Berdasarkan hasil pengujian lainnya yang dilakukan terhadap empat sampel citra maka diperoleh nilai MSE sebesar 371,82665 dan nilai PSNR sebesar 181,229.

Kata Kunci: Watermarking; LSB; Citra Digital; Keamanan.

Abstract−*The development of digital content has brought new opportunities for classic crimes in the field of information technology, namely piracy. Content that should be the legal property of the producer and legally owned by a particular person, can easily be misused by irresponsible parties including SDS Bina Satria Mulia Medan. Digital watermarking was developed as one of the answers to determine the legitimacy of the creator or distribution of digital data and the integrity of digital data. Watermarking techniques work by inserting a small amount of information that indicates ownership, purpose or other data, on digital media without affecting its quality. So in a digital image, the eye cannot distinguish whether the image is inserted with a watermark or not. The purpose of this research is how to maintain or protect a digital image from manipulation or alteration and falsification of a digital image for the benefit and purpose of unwanted parties by applying watermarking. The method used for watermarking digital images is the LSB (Least Significant Bit) method, which is to insert a code in the image to be protected but does not change the substance of the image. This unique code will be a mark or mark on an image. With this code, the authenticity of an image can be known. Claims to image authenticity can be proven by the unique code embedded in the image. In the analysis process, the "BINA SATRIA" watermark is inserted into an image measuring 140x140 pixels so that based on the steps taken, the previously inserted watermark is successfully extracted from the image that has been inserted with the watermark. Based on other test results conducted on four image samples, the MSE value of 371.82665 and the PSNR value of 181.229 were obtained.*

Keywords*: Watermarking; LSB; Digital Image; Security.*

1. PENDAHULUAN

Keamanan multimedia adalah suatu bentuk perlindungan berbasis konten. Dalam konteks pembuatan, pemrosesan, transmisi dan penyimpanan informasi, konten mengacu pada representasi tingkat tinggi atau semantik data. Tentu saja hal ini menyiratkan bahwa konten dapat terdiri dari berbagai bentuk media seperti citra, audio, video, teks dan grafik dalam berbagai format digital[1]. Penggunaan data digital selain kemudahan dalam penyebaran dengan menggunakan jaringan internet, juga dikarenakan kemudahan dan kemurahan dalam penggandaan (peng-copy-an) serta penyimpanannya untuk digunakan dikemudian hari. Kemudahan tersebut dapat digunakan secara negatif tanpa memperhatikan aspek hak cipta *(Intellectual Property Right)*[2]. Perlindungan hak cipta terhadap data digital memang sudah menjadi perhatian orang-orang sejak dulu. Banyak cara yang sudah ditempuh untuk memberikan atau melindungi data digital seperti *encryption, copy protection, visible marking, header marking* dan sebagainya, tetapi semua cara tersebut memiliki kelemahannya masing-masing[3].

Seiring berjalannya waktu mulai muncul penggunaan untuk mengatasi masalah hak cipta pada data digital tersebut yang lebih dikenal dengan istilah watermarking. Digital watermarking dikembangkan sebagai salah satu jawaban untuk

Journal Global Tecnology Computer
Vol 4, No. 2, April 2025, Hal 139-149
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i2.7325
Website https://ejurnal.seminar-id.com/index.php/jogtc

menentukan keabsahan pencipta atau pendistribusi suatu data digital dan integritas suatu data digital. Penelitian sebelumnya menyimpulkan bahwa teknik watermarking bekerja dengan menyisipkan sedikit informasi yang menunjukkan kepemilikan, tujuan atau data lain pada media digital tanpa mempengaruhi kualitasnya. Jadi pada citra digital, mata tidak bisa membedakan apakah citra tersebut disisipi watermark atau tidak[4].

Seperti halnya pada SDS Bina Satria Mulia Medan, banyak kasus-kasus yang mendasari sehingga membutuhkan watermarking pada citra digital khususnya seperti dokumen-dokumen penting yang discan menjadi sebuah gambar. Masalah kepemilikan, pemalsuan atas kepemilikan produk digital sering terjadi. Foto digital, misalnya, tidak memiliki suatu label atau informasi pengidentifikasi yang melekat pada foto tersebut. Apabila ada klaim dari pihak lain yang juga mengaku sebagai pemiliksah atas foto digital tersebut, pemilik foto yang asli tidak dapat memberikan bantahan karena memang tidak memiliki bukti otentik yang menandakan kepemilikan.

Menurut penelitian yang sebelumnya dilakukan oleh Putra Wibowo, dkk menyimpulkan bahwa selain masalah pelanggaran hak cipta, penggandaan yang tidak berizin atas citra digital dapat merugikan pemiliknya sebab pemilik citra digital tidak memperoleh royalti apapun terhadap penggandaan ilegal tersebut. Hal ini juga berdampak pada masalah keaslian[5]. Penelitian lain yang dilakukan oleh Apriyani juga menyimpulkan bahwa produk digital digital sangat mudah diubah. Perubahan tersebut dapat berupa rekayasa terhadap produk yang asli, baik perubahan yang dapat dipersepsi maupun tidak[6]. Perubahan yang timbul dapat menyebabkan informasi penting yang terdapat di dalam citra digital hilang. Hal ini sulit dipecahkan karena tidak terdapat jejak yang dapat menunjukkan bahwa seseorang bertanggung jawab atas penyebaran, penggandaan dan pengubahan citra digital ataupun otentikasi mengenai hak seseorang atas produk digital tersebut.

Selanjutnya pada penelitian yang oleh Ardhi Fadlika Satria, dkk menyimpulkan bahwa Pemilik citra dapat melakukan otentikasi (temper proofing) untuk membuktikan keaslian citra tersebut saat proses ekstraksi dilakukan, citra manipulasi berhasil di deteksi karena mengalami kerusakan. Hasil pengujian menunjukkan teknik digital watermarking dengan metode Least Significant Bit ini mampu melindungi dan membuktikan keaslian citra tersebut[7]. Penelitian lain yang dilakukan Lani Asep Sutisna menyimpulkan bahwa Aplikasi digital watermark ini bisa digunakan untuk melihat apakah file gambar masih keadaan asli belum termodifikasi atau sudah dimodifikasi oleh pihak yang tidak bertanggung jawab[8] .

Teguh Budi Harjo, dkk juga melakukan penelitian dan menyimpulkan bahwa dengan metode LSB (Least Significant Bit), image yang disisipkan pesan atau dokumen tidak terlalu banyak terlihat perbedaan dari citra warna terkecuali disisipkan pesan atau dokumen dengan ukuran besar[9]. Hertika Yuni Asti Sinaga dan Lamhot Sitorus juga menyimpulkan bahwa Algoritma Least Significant Bit dan End Of File untuk meningkatkan keamanan sebuah gambar yang bersifat rahasia tersebut tetap aman dari orang-orang yang bermaksud memanipulasi gambar tersebut[10].

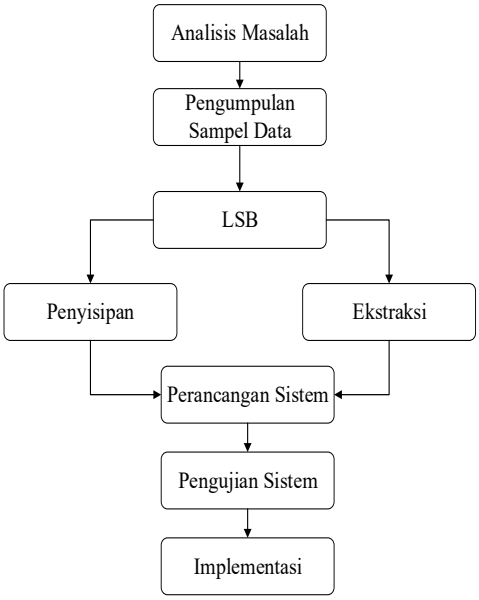
Untuk menghindari permasalahan tersebut di atas, maka pengusul pengusul mencoba meneliti tentang seberapa besar kekuatan pengamanan gambar digital menggunakan teknologi watermarking dengan menerapkan metode Metode *Least Significant Bit (LSB)* untuk melindungi citra digital. Metode LSB bekerja dengan menambahkan bit watermark pada bit terakhir Piksel, sehingga perubahan warna yang diakibatkan sangat kecil. Metode LSB menggunakan citra digital sebagai covertext. Pada susunan bit di dalam sebuah byte (1 byte= 8 bit), ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti *(least significant bit atau LSB)*[11]. Dengan adanya teknik watermarking metode LSB ini dapat dengan mudah untuk melindungi karya cipta dari pemalsuan. Secara kasat mata perubahan warna tidak akan terlihat oleh mata sehingga terlindung dari tindakan penyalahgunaan citra digital.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Metode penelitian yang digunakan adalah *Least Significant Bit (LSB)* dengan subjek pada penelitian ini adalah untuk tujuan keamanan dan perlindungan hak cipta citra digital menyembunyikan watermark pada gambar digital untuk melindungi hak cipta atau memberikan autentikasi pada materi visual. Subjek tersebut dapat berupa string yang digunakan adalah menggunakan dokumentasi citra sebagai watermark untuk melindungi citra digital dari penggunaan yang tidak sah. Thapan penelitian adalah langkah-langkah sistematis yang dilakukan oleh peneliti dalam rangka menyelesaikan suatu permasalahan khususnya watermarking citra digital. Adapun yang menjadi tahapan penelitian yang dilakukan dapat dilihat pada gambar 1 berikut:

Journal Global Tecnology Computer
Vol 4, No. 2, April 2025, Hal 139-149
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i2.7325
Website https://ejurnal.seminar-id.com/index.php/jogtc



Gambar 1. Tahapan Penelitian

a. Analisis Masalah
Langkah awal ini bertujuan untuk mengidentifikasi dan merumuskan permasalahan yang akan diselesaikan. Peneliti menggali kebutuhan dan tantangan yang ada dalam bidang keamanan data, lalu menentukan bahwa solusi yang tepat adalah dengan menggunakan teknik watermarking.
b. Pengumpulan Sampel Data
Setelah masalah dianalisis, langkah selanjutnya adalah mengumpulkan data yang relevan. Data ini berupa Citra digital yang akan digunakan sebagai media penyisipan serta data atau pesan rahasia yang akan disisipkan ke dalam citra.
c. LSB (Least Significant Bit)
Ini adalah tahap pemilihan dan penerapan metode steganografi. LSB merupakan teknik menyisipkan bit data pada bit paling tidak signifikan dari Piksel citra digital, karena perubahan kecil pada bit ini tidak akan terlalu memengaruhi tampilan visual gambar.
d. Penyisipan
Proses di mana data rahasia disisipkan ke dalam citra digital menggunakan teknik LSB. Setiap bit dari pesan disisipkan ke bit paling tidak signifikan dari Piksel gambar, sehingga gambar hasil penyisipan tampak hampir identik dengan gambar asli.
e. Ekstraksi
Setelah data disisipkan, proses ekstraksi dilakukan untuk menguji apakah data rahasia dapat diambil kembali dari gambar. Tahap ini penting untuk memastikan keberhasilan teknik watermarking yang digunakan.
f. Perancangan Sistem
Di tahap ini, sistem perangkat lunak dirancang berdasarkan hasil dari penyisipan dan ekstraksi. Sistem ini mencakup antarmuka pengguna, algoritma LSB, dan alur proses secara keseluruhan.
g. Pengujian Sistem
Sistem yang telah dirancang diuji dengan menggunakan data uji untuk memastikan bahwa fungsinya berjalan dengan baik. Pengujian ini mencakup keakuratan ekstraksi data, kualitas gambar setelah penyisipan dan ketahanan terhadap modifikasi
h. Implementasi
Tahap akhir berupa penerapan sistem ke dalam penggunaan nyata, baik untuk studi kasus tertentu maupun untuk distribusi lebih luas. Implementasi juga mencakup dokumentasi dan potensi pengembangan lebih lanjut.

2.2 Aplikasi

Aplikasi merupakan penerapan suatu konsep program komputer yang terintegrasi dengan kebutuhan user, untuk melaksanakan pekerjaan tertentu. Aplikasi software yang dirancang untuk suatu tuga khusus dapat dibedakan menjadi dua jenis, yaitu:

a. Aplikasi software spesialis, program dengan dokumentasi tergabung yang dirancang untuk menjalankan tugas tertentu.
b. Aplikasi software paket, suatu program dengan dokumentasi tergabung yang dirancang untuk jenis masalah tertentu

Aplikasi dapat beroperasi dengan mengandalkan sistem operasi, dimana operating system (OS) bertindak sebagai perantara antara perangkat keras (hardware) dengan program aplikasi. Pemutar media, lembar kerja, dan pengolah kata merupakan beberapa contoh perangkat lunak yang terkadang digabung menjadi satu. Perangkat lunak atau software yang digabung menjadi satu ini disebu sebagai application suite. Aplikasi merupakan penerapan, menyimpan sesuatu hal, data,

Journal Global Tecnology Computer
Vol 4, No. 2, April 2025, Hal 139-149
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i2.7325
Website https://ejurnal.seminar-id.com/index.php/jogtc

permasalahan, pekerjaan kedalam suatu sarana atau media yang dapat digunakan untuk menerapkan atau mengimplementasikan hal atau permasalahan yang ada sehingga berubah menjadi suatu bentuk yang baru tanpa menghilangkan nilainilai dasar dari hal data, permasalahan, dan pekerjaan itu sendiri[12]

2.3 Citra Digital

Citra digital merupakan citra yang dinyatakan dalam kumpulan data digital dan dapat diproses oleh komputer. Akuisisi citra digital dengan menggunakan berbagai peranti digital sebagai contoh, gambar awan diperoleh melalui kamera digital, citra artikel koran diperoleh melalui alat pemindai (scanner). Citra di dalam komputer disusun atas jumlah sejumlah Piksels, sebuah Piksels dapat dibayangkan sebagai sebuah titik yang dinyatakan dengan bentuk (y, x) dengan y menyatakan baris dan x menyatakan kolom.

Umumnya, koordinat pojok kiri atas dinyatakan dengan (0,0) dan dengan demikian, jika suatu citra berukuran M baris dan N kolom atau biasa dinyatakan sebagai MxN, koordinat Piksels terbawah dan terkanan berada di koordinat (M-1, N-1).Citra digital juga dapat diartikan sebagai suatu representasi (gambaran) atau kemiripan imitasi dari suatu objek. Citra sebagai keluaran suatu sistem perekam data yang bersifat optik berupa foto, bersifat analog yang berupa sinyal-sinyal video seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada suatu media penyimpanan[13].

2.4 Watermark

Watermarking dapat dipandang sebagai suatu proses penyisipan sebuah data rahasia (watermark) terhadap sebuah gambar atau dokumen, yang berkembang hingga media digital atau disebut dengan Digital Watermarking. yang dapat dijalankan pada berbagai media digital, seperti citra digital, suara dan video. Secara umum, watermarking adalah proses penyisipan citra digital dengan pesan atau watermark. Watermark yang disisipkan dalam citra digital haruslah imperceptible atau tidak terdeteksi oleh sistem penglihatan manusia (Human Visual System) atau sistem pendengaran manusia (Human Auditory System)[14][15].

Digital watermarking adalah teknik untuk menyisipkan informasi tertentu ke dalam sebuah data dengan suatu cara tertentu sehingga watermark itu sulit dirusak dan dihapus. Secara garis besar, watermark terbagi menjadi dua tipe, yaitu visible watermark dan invisible watermark. Visible watermark merupakan salah satu jenis yang dapat terlihat oleh indera manusia. Visible watermark bersifat sangat robust karena keberadaan watermark dapat dikenali dengan mudah dan biasanya sangat sulit untuk dihapus. Watermark yang disisipkan dapat bersifat solid ataupun semi transparan, dan untuk memindahkannya membutuhkan cropping yang signifikan[16].

Pada watermarking diketahui bahwa citra hasil manipulasi sedikit sekali yang berubah. Hal ini menjadi salah satu kelebihan watermarking dibandingkan dengan kriptografi dan steganografi. Watermarking dikenal sebagai teknik yang mudah untuk diaplikasikan dalam tujuan copyright protection maupun fingerprinting. Menurut ketidaknampakan oleh mata manusia, watermarking dibagi menjadi dua yaitu visible dan invisible watermaking. Visible watermarking biasanya digunakan oleh fotografer untuk menandai hasil karyanya yang diunggah ke dunia maya, sedangkan invisible watermarking biasa digunakan untuk mengamankan data tanpa terlihat oleh mata manusia. Kriteria baik atau buruk pada invisible watermarking dapat diketahui dengan melihat nilai evaluasinya, salah satunya dapat menggunakan Peak Signal to Noise Ratio (PSNR) dalam satuan dB (Desible)[17].

2.5 Least Significant Bit (LSB)

Metode LSB ini merupakan teknik watermarking sederhana dengan menyisipkan kode-kode tertentu pada citra yang akan dilindungi. Biasanya citra dengan 24-bit atau 8-bit digunakan untuk menyimpan citra digital. Representasi warna dari Piksel-Piksel bias diperoleh dari warna-warna primer yaitu Red, Green, Blue. Penggunaan citra 24-bit memungkinkan setiap Piksel direpresentasikan dengan nilai warna sebanyak 16.777.216 warna. Dua bit terakhir bias digunakan untuk menyimpan kode rahasia sebagai penanda keaslian karya cipta[18].

Ada dua jenis teknik yang dapat digunakan pada metode LSB, yaitu secara sekuensial (berurutan) dan secara random (acak)[19]:

a. Sekuensial (Berurutan)
   1. Teknik Penyembunyian Pesan (*Embedding*)
      Penyembunyian pesan secara sekuensial (berurutan) berarti pesan rahasia disisipkan secara berurutan dari data titik pertama yang ditemukan pada file gambar. Penyisipan dilakukan dari indeks (0,0), dari kiri ke kanan, baris per baris, sepanjang bit-bit pesan yang disembunyikan.
   2. Teknik Pengungkapan Pesan (Ektraksi)
      Ekstraksi pesan dilakukan dengan cara mengekstrak bit-bit LSB sebagaimana urutan proses penyisipan. Dimulai dari indeks (0,0), dari kiri ke kanan, baris per baris, sehingga diperoleh bit-bit LSB. Berdasarkan bit-bit tersebut, kemudian disusun ulang hingga diperoleh nilai bit pesan yang disisipkan.
b. Acak (*Random*)
   1. Teknik Penyembunyian Pesan (*Embedding*)
      Acak berarti penyisipan pesan rahasia dilakukan secara acak pada gambar. Untuk melakukan penyisipan secara acak, bit-bit data rahasia tidak disipkan dengan mengganti *byte-byte* yang berurutan, namun dipilih susunan byte secara acak.

Journal Global Tecnology Computer
Vol 4, No. 2, April 2025, Hal 139-149
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i2.7325
Website https://ejurnal.seminar-id.com/index.php/jogtc

b. Teknik Pengungkapan Pesan (Ektraksi)
Data yang disembunyikan di dalam citra dapat dibaca kembali dengan cara pengungkapan (*reveal* atau *extraction*). Posisi byte yang menyimpan bit data dapat diketahui dari bilangan acak yang dibangkitkan oleh PRNG. Dengan demikian, bit-bit data rahasia yang bertaburan di dalam citra dapat dikumpulkan kembali.
Proses penyisipan pesan dengan metode LSB dapat dituliskan dalam algoritma sebagai berikut:

a. Inputkan pesan yang akan disisipkan.
b. Ubah pesan menjadi kode-kode biner. Untuk mempermudah dapat terlebih dulu diubah menjadi desimal, kemudian biner.
c. Inputkan citra grayscale yang akan disisipi pesan.
d. Dapatkan nilai derajat keabuan masing-masing Piksel.
e. Ubah derajat keabuan tersebut menjadi kode-kode biner.
f. Ganti bit terakhir kode biner citra dengan bit pesan.
g. Ubah kode biner menjadi derajat keabuan citra baru (citra yang sudah disisipi pesan).
h. Petakan menjadi citra baru.

Sedangkan ekstraksi pesan yang sudah disisipkan dengan metode LSB dapat dilakukan dengan algoritma berikut[20]:

a. Input image yang sudah mengandung pesan.
b. Dapatkan nilai derajat keabuan citra tersebut.
c. Ubah nilai derajat keabuan menjadi kode-kode biner.
d. Ambil nilai kode binet bit terakhir. Terjemahkan menjadi karakter

3. HASIL DAN PEMBAHASAN

3.1 Pembahasan

Metode *Least Significant Bit (LSB)* untuk menyisipkan pesan sebagai watermark pada citra dilakukan dengan menyediakan terlebih dahulu sebuah citra yang akan digunakan untuk proses watermark. Lalu citra tersebut dicropping dan diambil dengan resolusi sebesar 5x6 Piksel atau sebesar 30 Piksel piksel. Berikut ini merupakan citra sampel yang digunakan untuk proses analisa yang dapat dilihat pada gambar 2 di bawah ini.

Gambar 2. Citra Sampel Yang akan Diwatermark

Selanjutnya adalah melakukan penyisipan watermark “BINASATRIA” dengan metode LSB sebagai berikut:
Tahap pertama yaitu mengubah teks watermark ke dalam bilangan biner yang dapat dilihat seperti pada tabel 1 berikut:

Tabel 1. Konversi teks ke dalam bilangan biner

Teks	B	I	N	A	S	A	T	R	I	A
Biner	01000010	01001001	01001110	01000001	01010011	01000001	01010100	01010010	01001001	01000001

Jumlah bit =80bit
Jumlah Piksel = Jumlah Bit Data / 3
= 80/3
= 26,7
= 27 Piksel

Citra yang dijadikan sebagai cover (penampung data) harus memiliki jumlah Piksel minimal 27 Piksel (boleh lebih). Proses penyembunyian, dimulai secara berturut-turut dari Piksel 1 sampai Piksel selanjutnya. Proses penyisipan nilai biner terhadap masing-masing kanal RGB citra sampel sebesar 27 piksel yang dapat dilihat pada tabel 2 berikut ini:

Tabel 2. Proses penyembunyian nilai biner watermark “BINASATRIA” yang pada setiap piksel citra

PIKSEL	WARNA	DESIMAL	BINER
0	R	40	00101000
	G	26	00011010

Journal Global Tecnology Computer
Vol 4, No. 2, April 2025, Hal 139-149
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i2.7325
Website https://ejurnal.seminar-id.com/index.php/jogtc

PIKSEL	WARNA	DESIMAL	BINER
	B	51	00110011
PIKSEL	WARNA	DESIMAL	BINER
	R	63	00111111
1	G	36	00100100
	B	79	01001111
PIKSEL	WARNA	DESIMAL	BINER
	R	110	01101110
2	G	90	01011010
	B	132	10000100
PIKSEL	WARNA	DESIMAL	BINER
	R	48	01100000
3	G	27	00110110
	B	63	00111111
PIKSEL	WARNA	DESIMAL	BINER
	R	46	00101110
4	G	29	00011101
	B	59	00111011
PIKSEL	WARNA	DESIMAL	BINER
	R	47	00101111
5	G	18	00010010
	B	69	01000101
PIKSEL	WARNA	DESIMAL	BINER
	R	85	01010101
6	G	60	00111100
	B	114	01110010
PIKSEL	WARNA	DESIMAL	BINER
	R	130	10000010
7	G	109	01101101
	B	161	10100001
PIKSEL	WARNA	DESIMAL	BINER
	R	74	01001010
8	G	43	00101011
	B	93	01011101
PIKSEL	WARNA	DESIMAL	BINER
	R	59	00111011
9	G	34	00100010
	B	78	01001110
PIKSEL	WARNA	DESIMAL	BINER
	R	70	01000110
10	G	52	00110100
	B	77	01001101
PIKSEL	WARNA	DESIMAL	BINER
	R	111	01101111
11	G	84	01010100
	B	101	01100101
PIKSEL	WARNA	DESIMAL	BINER
	R	126	01111110
12	G	99	01100011
	B	117	01110101
PIKSEL	WARNA	DESIMAL	BINER
	R	95	01011111
13	G	70	01000110
	B	109	01101101
PIKSEL	WARNA	DESIMAL	BINER
	R	94	01011110
14	G	69	01000101
	B	104	01101000
PIKSEL	WARNA	DESIMAL	BINER
	R	47	00101111
15	G	48	00110000
	B	47	00101111

Journal Global Tecnology Computer
Vol 4, No. 2, April 2025, Hal 139-149
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i2.7325
Website https://ejurnal.seminar-id.com/index.php/jogtc

PIKSEL	WARNA	DESIMAL	BINER
PIKSEL	WARNA	DESIMAL	BINER
	R	80	01010000
16	G	47	00101111
	B	30	00011110
PIKSEL	WARNA	DESIMAL	BINER
	R	117	01110101
17	G	77	01001101
	B	53	00110101
PIKSEL	WARNA	DESIMAL	BINER
	R	84	01010100
18	G	70	01000110
	B	62	00111110
PIKSEL	WARNA	DESIMAL	BINER
	R	88	01011000
19	G	56	00111000
	B	45	00101101
PIKSEL	WARNA	DESIMAL	BINER
	R	69	01000101
20	G	80	01010000
	B	66	01000010
PIKSEL	WARNA	DESIMAL	BINER
	R	130	10000010
21	G	128	10000000
	B	126	01111110
PIKSEL	WARNA	DESIMAL	BINER
	R	127	01111111
22	G	117	01110101
	B	115	01110011
PIKSEL	WARNA	DESIMAL	BINER
	R	158	10011110
23	G	155	10011011
	B	154	10011010
PIKSEL	WARNA	DESIMAL	BINER
	R	109	01101101
24	G	99	01100011
	B	94	01011110
PIKSEL	WARNA	DESIMAL	BINER
	R	128	10000000
25	G	142	10001110
	B	113	01110001
PIKSEL	WARNA	DESIMAL	BINER
	R	146	10010010
26	G	171	10101011
	B	155	10011011
PIKSEL	WARNA	DESIMAL	BINER
	R	224	11100000
27	G	231	11100111
	B	238	11101110

Setelah citra cover dikonversi menjadi biner, maka nilai-nilai bit ke-8 (LSB) dari setiap elemen warna piksel diganti dengan nilai bit-bit dari teks yang akan disembunyikan. Proses pergantian nilai biner bit ke-8 yang disembunyikan terhadap citra sampel seperti yang terlihat pada tabel 3 berikut ini:

Tabel 3. Nilai bit ke-8 diganti dengan bit teks yang disembunyikan

PIXEL	WARNA	DESIMAL	BINER	Biner Cipher Text	BINER	DESIMAL	WARNA	PIXEL
	R	40	00101000	0	00101000	40	R	
0	G	26	00011010	1	00011011	27	G	0
	B	51	00110011	0	00110010	50	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	63	00111111	0	00111110	62	R	
1	G	36	00100100	0	00100100	37	G	1
	B	79	01001111	0	01001110	78	B	

Journal Global Tecnology Computer
Vol 4, No. 2, April 2025, Hal 139-149
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i2.7325
Website https://ejurnal.seminar-id.com/index.php/jogtc

PIXEL	WARNA	DESIMAL	BINER	Biner Cipher Text	BINER	DESIMAL	WARNA	PIXEL
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	110	01101110	1	01101111	111	R	
2	G	90	01011010	0	01011010	90	G	2
	B	132	10000100	0	10000100	132	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	48	01100000	1	01100001	97	R	3
3	G	54	00110110	0	00110110	54	G	
	B	63	00111111	0	00111110	62	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	46	00101110	1	00101110	46	R	4
4	G	29	00011101	0	00011101	29	G	
	B	59	00111011	0	00111010	58	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	47	00101111	1	00101111	47	R	5
5	G	18	00010010	0	00010010	18	G	
	B	69	01000101	1	01000101	69	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	85	01010101	0	01010100	84	R	6
6	G	60	00111100	0	00111100	60	G	
	B	114	01110010	1	01110011	115	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	130	10000010	1	10000011	131	R	7
7	G	109	01101101	1	01101101	109	G	
	B	161	10100001	0	10100000	160	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	74	01001010	0	01001010	74	R	8
8	G	43	00101011	1	00101011	43	G	
	B	93	01011101	0	01011100	91	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	59	00111011	0	00111010	58	R	9
9	G	34	00100010	0	00100010	34	G	
	B	78	01001110	0	01001110	78	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	70	01000110	0	01000110	70	R	10
10	G	52	00110100	1	00110101	53	G	
	B	77	01001101	0	01001100	76	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	111	01101111	1	01101111	111	R	11
11	G	84	01010100	0	01010101	85	G	
	B	101	01100101	1	01100101	101	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	126	01111110	0	01111110	126	R	12
12	G	99	01100011	0	01100010	98	G	
	B	117	01110101	1	01110100	116	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	95	01011111	1	01011111	95	R	13
13	G	70	01000110	0	01000110	70	G	
	B	109	01101101	1	01101101	109	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	94	01011110	0	01011110	94	R	14
14	G	69	01000101	0	01000100	68	G	
	B	104	01101000	0	01101000	104	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	47	00101111	0	00101110	46	R	15
15	G	48	00110000	0	00110000	48	G	
	B	47	00101111	1	00101111	47	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	80	01010000	0	01010000	80	R	16
16	G	47	00101111	1	00101111	46	G	
	B	30	00011110	0	00011110	30	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	117	01110101	1	01110101	117	R	17
17	G	77	01001101	0	01001100	76	G	
	B	53	00110101	1	00110101	53	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
18	R	84	01010100	0	01010100	84	R	18
	G	70	01000110	0	01000110	70	G	

Journal Global Tecnology Computer
Vol 4, No. 2, April 2025, Hal 139-149
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i2.7325
Website https://ejurnal.seminar-id.com/index.php/jogtc

PIXEL	WARNA	DESIMAL	BINER	Biner Cipher Text	BINER	DESIMAL	WARNA	PIXEL
	B	62	00111110	0	00111110	62	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	88	01011000	1	01011001	89	R	19
19	G	56	00111000	0	00111000	56	G	
	B	45	00101101	1	00101101	45	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	69	01000101	0	01000100	68	R	20
20	G	80	01010000	0	01010000	80	G	
	B	66	01000010	1	01000011	67	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	130	10000010	0	10000010	130	R	21
21	G	128	10000000	0	10000000	128	G	
	B	126	01111110	1	01111111	127	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	127	01111111	0	01111110	126	R	22
22	G	117	01110101	0	01110100	116	G	
	B	115	01110011	1	01110011	115	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	158	10011110	0	10011110	158	R	23
23	G	155	10011011	0	10011010	154	G	
	B	154	10011010	1	10011011	155	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	109	01101101	0	01101100	108	R	24
24	G	99	01100011	1	01100011	99	G	
	B	94	01011110	0	01011110	94	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	128	10000000	0	10000000	128	R	25
25	G	142	10001110	0	10001110	142	G	
	B	113	01110001	0	01110000	112	B	
PIXEL	WARNA	DESIMAL	BINER		BINER	DESIMAL	WARNA	PIXEL
	R	146	10010010	0	10010010	146	R	26
26	G	171	10101011	1	10101011	171	G	
	B	155	10011011	-	10011011	155	B	

Setelah proses watermark dilakukan, maka citra akan disimpan menjadi citra baru. Proses ekstraksi watermark yang telah disisipkan ke dalam citra dilakukan dengan langkah-langkah berikut:

a. Konversi citra hasil watermark menjadi biner
b. Ambil nilai-nilai bit ke-8 dari setiap elemen warna pixel
c. Kelompokkan menjadi 8 bit per kelompok
d. Konversi biner-biner setiap kelompok menjadi karakter

Sehingga berdasarkan langkah-langkah di atas diperoleh proses ekstraksi dengan mengubah nilai biner menjadi karakter seperti yang terlihat pada tabel 4 berikut:

Tabel 4. Ekstraksi nilai biner ke string

Biner	01000010	01001001	01001110	01000001	01010011	01000001	01010100	01010010	01001001	01000001
Teks	B	I	N	A	S	A	T	R	I	A

Berdasarkan langkah-langkah yang dilakukan, maka watermark yang sebelumnya disisipkan yaitu "**BINASATRIA**" terhadap citra berukuran 140x140 piksel berhasil diektraksi kembali dari citra yang telah disisipakan watermark. Pengujian juga dilakukan terhadap empat sampel citra lainnya yang memiliki resolusi berbeda serta dengan menyisipkan watermark yang berbeda pula untuk setiap sampel yang dapat dilihat pada table 5 berikut:

Tabel 5. Proses pengujian terhadap empat sampel citra lainnya

No	Citra Asli dan Resolusi	Watermark	Citra Hasil Watermark	MSE	PSNR
1	 140x140	SATRIA		0.00058	130.214
2	 4096x3072	BINA		5.5631	199.716

Journal Global Tecnology Computer
Vol 4, No. 2, April 2025, Hal 139-149
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i2.7325
Website https://ejurnal.seminar-id.com/index.php/jogtc

No	Citra Asli dan Resolusi	Watermark	Citra Hasil Watermark	MSE	PSNR
3	 6000x3376	MULIA		5.10137	200.445
4	 6000x3376	BINASATRIAMULIA		9.21538	194.539
				ΣMSE=1487,30658	ΣPSNR= 724,914
				$\overline{MSE}$=371,82665	$\overline{PSNR}$=181,229

4. KESIMPULAN

Metode LSB salah satu metode yang baik dan cepat digunakan untuk mengamankan citra digital dengan teknik watermark. Watermak yang mampu disipkan adalah berupa string yang mampu kembali diekstrak. Proses penyisipan watermark misalnya dalam bentuk logo atau teks digital, disisipkan ke dalam bit paling rendah dari setiap piksel. Karena perubahan ini terjadi pada bit paling tidak signifikan, perubahan pada citra tidak terlihat oleh mata manusia. Untuk pembentukan citra berwatermark, setelah watermark disisipkan, citra digital baru yang telah diwatermark dihasilkan dan citra ini tampak sama dengan citra asli secara visual, namun memiliki watermark tersembunyi di dalamnya. Untuk proses ekstraksi watermark, pengambilan watermark dilakukan untuk memverifikasi keaslian gambar. Algoritma LSB memungkinkan pengambilan kembali watermark dengan mudah dari citra yang telah diwatermark, selama citra tidak mengalami perubahan signifikan. Berdasarkan hasil pengujian yang dilakukan pada empat sampel citra maka diperoleh nilai MSE sebesar 371,82665 dan nilai PSNR sebesar 181,229.

UCAPAN TERIMAKASIH

Tim penulis menyampaikan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan dan bantuan dalam pelaksanaan penelitian ini terutama SD Bina Satria Mulia Medan. Tim penulis juga berterima kasih kepada rekan-rekan dan partisipan yang telah membantu dalam tahap pengujian sistem ini. Tim penulis menghargai dukungan keluarga dan teman-teman yang selalu memberikan semangat dan doa. Semua bantuan, baik secara langsung maupun tidak langsung, telah menjadi bagian penting dalam kelancaran dan keberhasilan penelitian ini

REFERENCES

[1] P. Lumbanraja, "Watermarking Pada Citra Digital Menggunakan Kombinasi Pixel Value Indicator Dan Metode Most Significant Bit," *Jurnal METHODIKA*, vol. 5, no. 1, 2019.
[2] K. Kurniawan, I. A. Siradjuddin, and A. Muntasa, "Keamanan Citra Dengan Watermarking Menggunakan Pengembangan Algoritma Least Significant Bit," *Jurnal Informatika*, vol. 13, no. 1, Feb. 2016, doi: 10.9744/informatika.13.1.9-14.
[3] Widiyono, Ari Putra Wibowo, And Arief Soma Darmawan, "Teknik Watermarking Menggunakan Metode Least Significant Bit Pada Citra Untuk Perlindungan Hak Cipta," vol. 6, no. 1, 2021.
[4] A. W. Laksono, S. Suhada, and A. Zakaria, "Implementasi Metode Least Significant Bit (Lsb) Dalam Teknik Steganografi Pada Citra Digital Menggunakan Matlab," vol. 4, no. 1, 2024.
[5] A. Putra Wibowo, A. Soma Darmawan, and S. Widya Pratama, *Watermarking Technique Using Least Significant Bit Method On Batik Motif Image*.
[6] E. R. Apriyani, "Teknik Steganografi Pesan Teks Menggunakan Metode Least Significant Bit dan Algoritma Linear Congruential Generator (Text Message Steganography Using Least Significant Bit Method and Linear Congruential Generator Algorithm)," 2016.
[7] A. Fadlika Satria, R. Ibnu Adam, and Carudin, "Analisis Digital Watermarking untuk Otentikasi pada Citra Manipulasi Menggunakan Metode Least Significant Bit," *Edumatic: Jurnal Pendidikan Informatika*, vol. 5, no. 2, pp. 204–213, 2021, doi: 10.29408/edumatic.v5i2.3901.
[8] L. A. Sutisna, "Implementasi Digital Watermarking Menggunakan Metode LSB (Least Significant Bit) untuk Menyisipkan Teks dan Gambar ke Dalam Karya Digital", doi: 10.13140/RG.2.2.18938.21446.
[9] T. B. Harjo, M. Kapriati, and D. A. Susanto, "Aplikasi Steganografi Menggunakan LSB (Least Significant Bit) dan Enkripsi Triple Des Menggunakan Bahasa Pemrograman C#," *JURNAL SISFOTEK GLOBAL*, vol. 6, no. 1, Mar. 2016.
[10] H. Yuni, A. Sinaga, and L. Sitorus, "Pengamanan File Citra Digital Dengan Menggunakan Metode Least Significant Bit Dan End Of File," 2017.
[11] J. Rosmiyati and T. Matius Surya Mulyana, "Watermark Gabungan Steganografi dan Visible Watermarking," 2018. [Online]. Available: https://journal.ubm.ac.id/index.php/alu
[12] Yenni Iskandar, *Buku Ajar Pengantar Aplikasi Komputer*, 1st ed., vol. 1. Yogyakarta: Deepublish, 2018.

Vol 4, No. 2, April 2025, Hal 139-149
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i2.7325
Website https://ejurnal.seminar-id.com/index.php/jogtc

[13] Andono Pulung Nurtantio, Sutojo T, and Muljono, *Pengolahan Citra Digital*, 1st ed., vol. 1. Yogyakarta: ANDI OFFSET, 2017.
[14] P. Lumbanraja, "Watermarking Pada Citra Digital Menggunakan Kombinasi Pixel Value Indicator Dan Metode Most Significant Bit," *Jurnal METHODIKA*, vol. 5, no. 1, 2019.
[15] A. Suheryadi, "Penerapan Digital Watermark Sebagai Validasi Keabsahan Gambar Digital Dengan Skema Blind Watermark," *Jurnal Teknologi Terapan* |, vol. 3, no. 2, 2017.
[16] S. Wahyuningsih, T. V. D. Pandex, and V. Stefanny, "Implementasi Visible Watermarking Dan Steganografi Least Significant Bit Pada File Citra Digital," 2016.
[17] Susanto Ajib, Sari Christy Atika, Setiadi De Rosal Ign. Moses, and Rachmawanto Eko Hari, "UJI PERFORMA WATERMARKING 256x256 CITRA KEABUAN DENGAN LEAST SIGNIFICANT BIT," *SNATIF*, vol. 4, 2017.
[18] F. Masykur, "Implementasi Watermarking Metode LSB Pada Citra Guna Perlindungan Karya Cipta," Online, 2016.
[19] L. Ali Fitriani, "Analisa Keamanan Data Teks Dengan Menerapkan Kriptografi RSA dan Steganografi LSB," *Journal of Computer System and Informatics (JoSYC)*, vol. 1, no. 2, 2020.
[20] S. Rasita Febriani and D. Cita Irawati, "Implementasi Digital Watermarking Pada Citra Menggunakan Metode Least Significant Bit," 2016.