Building of Informatics, Technology and Science (BITS)
Volume 6, No 1, Juni 2024 Page: 115−124
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i1.5262

Steganografi Gambar Menggunakan Metode Least Significant Bit Pada Citra Dengan Operasi XOR

Martin Adha, Febi Yanto*, Lestari Handayani, Pizaini

[1]Fakultas Sains dan Teknologi, Teknik Informatika, Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia
Email: [1]12050112287@students.uin-suska.ac.id, [2,*]febiyanto@uin-suska.ac.id, [3]lestari.handayani@uin-suska.ac.id, [4]pizaini@uin-suska.ac.id
Email Penulis Korespondensi: febiyanto@uin-suska.ac.id
Submitted: **03/06/2024**; Accepted: **23/06/2024**; Published**: 23/06/2024**

Abstrak−Salah satu cara mengamankan pesan rahasia dari pihak-pihak lain yang tidak berkepentingan adalah steganografi. Salah satu metode yang paling banyak digunakan dalam steganografi adalah Least Significant Bit. Penelitian ini menggunakan gambar sebagai cover image dan secret image. Gambar di resize ke resolusi 512x512 piksel, cover image menggunakan gambar channel RGB dan secret image juga menggunalkan gambar dengan channel RGB. Dalam penelitian ini LSB akan dikombinasikan dengan triple XOR sehingga dapat meningkatkan keamanan dari metode penyembunyian pesan tersebut. Triple XOR digunakan untuk memberikan keamanan ekstra pada gambar yang telah disisipkan gambar rahasia (Stego Image). Pada penelitian ini juga dilakukan beberapa pengujian diantaranya adalah pengujian Peak Signal to Noise Ratio (PSNR) dan Mean Square Error (MSE), untuk pengujian ketahanan juga dilakukan dengan melakukan modifikasi pada stego image seperti resize, kompres, dan menambahkan serta mengurangi kontras. Hasil dari pengujian PSNR penelitian ini sangat baik yaitu kurang lebih 49 dB dan MSE rendah. Dengan hasil PSNR dan MSE tersebut dapat dibuktikan bahwa metode LSB memeiliki tingkat imperceptible yang baik. Dalam percobaan ketahanan citra terhadap modifikasi, beberapa hasil percobaan menunjukkan ekstraksi secret image pada stego image gagal untuk diekstrak, dan dari beberapa percobaan seperti penambahan dan pengurangan kontras, rotasi gambar dan kompresi lossless, citra yang disisipkan pada stego image berhasil diekstrak.

Kata Kunci: Steganografi; Least Significant Bit; XOR; Peak Signal To Noise Ratio; Mean Square Error

Abstract−One way to secure secret messages from other unauthorized parties is steganography. One of the most widely used methods in steganography is Least Significant Bit. This research uses images as cover images and secret images. The image is resized to a resolution of 512x512 pixels, The cover image uses an RGB channel image and the secret image also uses an RGB channel image. In this research, LSB will be combined with triple XOR so that it can increase the security of this message hiding method. Triple XOR is used to provide extra security to images that have a secret image (Stego Image) inserted. In this research, several tests were also carried out, including testing the Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE), for robustness testing it was also carried out by making modifications to the stego image such as resizing, compressing, and adding and reducing contrast. The results of this research's PSNR testing are very good, namely approximately 49 dB and lower MSE. With the PSNR and MSE results, it can be proven that the LSB method has a good level of imperceptibility. In experiments on image resistance to modification, several experimental results show that secret image extraction in the stego image failed to be extracted, and from several experiments such as adding and reducing contrast, image rotation and lossless compression, the image inserted in the stego image was successfully extracted.

Keywords: Steganography; Least Significant Bit; XOR; Peak Signal to Noise Ratio; Mean Square Error

1. PENDAHULUAN

Keamanan dunia maya menghadapi tantangan yang sangat besar [1]. Seiring berkembangnya teknologi, kebutuhan akan data pun semakin meningkat. Data yang digunakan pengguna pun berbeda-beda, tidak hanya data teks saja, tetapi juga data gambar. Pada area tertentu, diperlukan keamanan data yang tinggi pada saat transmisi data [2]. Beberapa metode untuk mengatasi masalah ini adalah dengan menggunakan teknik penyembunyian data rahasia seperti steganografi. Tujuan dari steganografi adalah menyembunyikan informasi dari pihak-pihak yang tidak memiliki akses terhadap data rahasia [3] [4]. Steganografi menyembunyikan informasi kedalam suatu media sehingga data yang disembunyikan tidak dapat diketahui oleh pihak yang tidak memiliki hak akses [5] [6]. Empat fitur penting steganografi adalah Robustness, capacity, Security dan imperceptibly [7] [8] [9]. Robustness adalah tahan terhadap perubahan informasi berupa modifikasi citra, Security adalah indikator penting seberapa sensitifnya informasi disembunyikan dari penyusup, Capacity adalah jumlah informasi pribadi yang dapat disampaikan dan Imperceptibly adalah sulit membedakan antara citra original dengan citra yang telah disisipkan pesan rahasia [10].

Berbagai metode dalam kategori berbeda direkomendasikan untuk steganografi gambar. Dalam kategori yang paling umum, steganografi umumnya dibagi menjadi dua kategori yaitu domain spasial dan frekuensi. Steganografi gambar adalah teknologi penyembunyi data yang menyematkan data rahasia dalam cover image tanpa terlihat. Hal ini digunakan untuk mencegah steganalisis untuk mencapai tujuan komunikasi tersembunyi [11]. Dalam steganografi gambar dan pesan rahasia ditanamkan pada cover image kemudian dikirimkan sedemikian rupa sehingga informasinya tidak terdeteksi. Gambar yang digunakan untuk menyembunyikan informasi rahasia disebut cover image. Penyematan pesan rahasia harus memastikan tidak ada perubahan signifikan. Gambar stego adalah gambar yang diperoleh dengan menyematkan suatu pesan rahasia ke dalam cover image. Pesan rahasia mungkin berupa teks biasa, teks kriptografi, dan gambar [12].

LSB atau Least Significant Bit adalah bit paling kanan dalam satu byte. Bit ini disebut LSB karena tidak mempunyai pengaruh yang signifikan. Satu byte terdiri dari 4-LSB dan 4-MSB (Most Significant Bit) [13]. LSB

Building of Informatics, Technology and Science (BITS)
Volume 6, No 1, Juni 2024 Page: 115−124
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i1.5262

menyembunyikan berita dan informasi di media dengan menyisipkan pesan langsung ke dalam piksel gambar sampul. Mengubah beberapa bit di setiap piksel akan menyembunyikan pesan pada media host yang dipilih dan menggantikan posisi bit [14] [15]. Keunggulan dari metode LSB adalah relatif mudah diimplementasikan, memiliki imperceptibility yang baik dan kapasitas yang cukup besar [7].

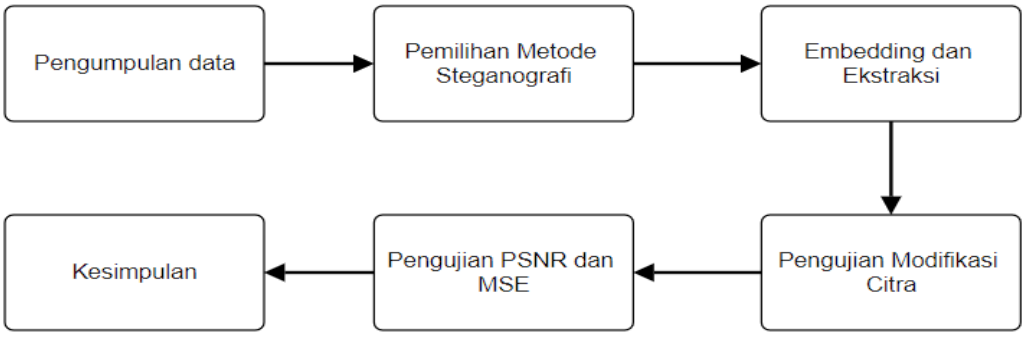
Penelitian yang dilakukan Astuti et al (2020) menunjukkan bahwa metode LSB dengan bit flipping dapat meningkatkan imperceptibility hingga sekitar 9dB dalam gambar skala abu-abu. Pada penelitian ini metode bit flipping diuji pada warna gambar dalam format RGB, kapasitas pesan yang tertanam pada gambar adalah 1 bit per piksel [16]. Penelitian lainnya yang dilakukan oleh Bhuiyan et al (2019) mengusulkan data yang sangat aman menggunakan teknik penyembunyian dalam domain spasial steganografi gambar. Skema yang diusulkan mengambil bit pesan dan melakukan XOR operasi dengan bit ke-7 dari setiap komponen RGB dan, kemudian, output yang dihasilkan tertanam dalam bit ke-8 setiap komponen RGB. Sebuah studi rinci tentang algoritma penggantian LSB yang diusulkan termasuk investigasi berbasis PSNR dan MSE telah dilakukan. Hasil percobaan menunjukkan puncak signal-to-noise yang sangat baik rasio (PSNR) (55,90 dB untuk 65.536 bit pesan dalam cover image 256x256 piksel) [17]. Pada Penelitian berikutnya yang dilakukan oleh Imanda R et al (2023) menggabungkan Kriptografi dan steganografi. Algoritma Vigenere Cipher dan Base64 adalah metode yang digunakan untuk mengenkripsi teks pesan dan steganografi Least Significant Bit (LSB) digunakan sebagai metode untuk menyisipkan pesan dienkripsi ke dalam gambar. LSB memanfaatkan bit-bit terakhir dari piksel gambar untuk menyimpan penambahan informasi tanpa mengganggu tampilan visual gambar secara signifikan [18]. Pada Penelitian yang dilakukan oleh Almayyahi A et al (2020) pengembangan metode aman untuk menyembunyikan pesan rahasia dalam sebuah gambar, berdasarkan standar Least Significant Bit (LSB). Sebelum melanjutkan ke tahap penyematan, ukuran pesan rahasia diperkecil dengan cara kompresi menggunakan algoritma Huffman yang dilanjutkan dengan dua operasi, yaitu operasi Boolean operasi Exclusive-NOR (XNOR) dan algoritma Fibonacci saat memilih piksel untuk menyematkan pesan rahasia[19]. Pada penelitian lainnya yang dilakukan oleh Al-Jarah et al (2021) menggunakan algoritma SK LSB adalah mengkodekan kunci rahasia dari gambar sampul, mengkodekan pesan rahasia menggunakan kunci rahasia, dan menyematkannya ke gambar sampul. Sekalipun penyerang mengetahui tentang steganografi, mereka tidak dapat mengetahui tentang kunci rahasianya. Algoritma SK LSB membantu mendapatkan tingkat keamanan yang lebih tinggi dan lebih baik, berguna untuk menyimpan informasi sensitif, relevan, dan penting [20].

Dari penelitian - penelitian diatas yang telah dilakukan sebelumnya terdapat kekurangan yaitu tidak ada pengujian ketahanan terhadap modifikasi citra, sehingga kondisi pesan yang disembunyikan pada citra tidak dapat diketahui jika dilakukan modifikasi pada cover image tersebut. Oleh karena itu perlu dilakukan pengujian. Penelitian kali ini akan menggunakan algoritma LSB (Least Significant Bit) dengan Triple XOR. Gambar yang digunakan pada penelitian ini menggunakan channel RGB untuk cover image dan juga stego image. Penggunaan metode LSB digunakan karena hasil dari pengujian penelitian sebelumnya sangat baik dengan hasil stego image yang mendekati gambar aslinya dibuktikan dengan skor PSNR diatas 50 dB. penelitian ini menyisipkan gambar sebagai pesan rahasia. penelitian ini akan menguji PSNR dan MSE serta menguji ketahanan terhadap modifikasi citra seperti resize, compress, dan rotating.

2. METODOLOGI PENELITIAN

2.1 Metode Penelitian

Berikut gambar dibawah ini adalah gambar dari metode yang digunakan pada penelitian ini



Gambar 1. Metode Penelitian

Pada Gambar 1 diatas merupakan metode penelitian yang mulai dengan mengumpulkan data, Pemilihan metode steganografi, embedding dan ekstraksi, Melakukan pengujian ketahanan citra, dan melakukan pengujian PSNR dan MSE. Dari tahapan tersebut akan didapatkan kesimpulan dari penelitian ini.

2.2 Tahapan Penelitian

Building of Informatics, Technology and Science (BITS)
Volume 6, No 1, Juni 2024 Page: 115−124
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i1.5262

Berikut ini adalah penjelasan langkah-langkah penelitian dari gambar 1 pada Steganografi Gambar Pada Citra Menggunakan Metode Least Signifcant Bit Pada Citra dengan Operasi XOR diantaranya

a. Pengumpulan Data

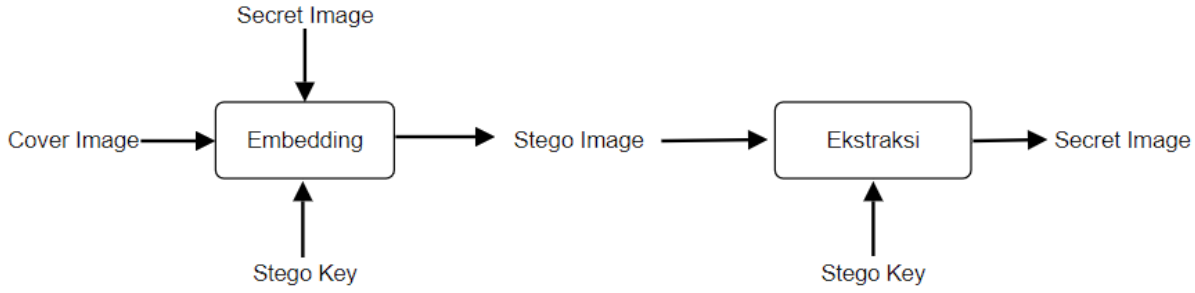
Pada tahapan penelitian ini yaitu menyiapkan data berupa gambar yaitu Baboon.bmp, airplane,bmp, dan goldhill.bmp yang akan dijadikan sebagai cover image dan pepper.bmp sebagai gambar yang akan disisipkan (secret image). Warna cover image dan yang digunakan dalam penelitian ini adalah dalam bentuk warna RGB dan warna gambar secret image yang akan disisipkan kedalam cover image juga dalam format RGB.

Bentuk ekstensi gambar yang dipakai dalam penelitian ini adalah .bmp, dikarenakan gambar yang berformat .bmp adalah gambar yang tidak menggunakan kompresi, sehingga kualitas gambar yang akan dijadikan sebagai cover image dapat terjaga, namun ukuran file dari gambar yang berformat .bmp lebih bersar dari format yang lain seperti .png ataupun .jpeg. kemudian untuk format gambar yang akan dijadikan sebagai secret image atau gambar yang akan disisipkan kedalam cover image adalah gambar berformat .bmp juga.

Gambar 2. Cover image

Gambar 3. Secret image

Pada gambar 2 dan 3 diatas merupakan gambar RGB yang akan digunakan untuk proses Embedding pada penelitian steganografi ini. Pada proses ini, citra untuk cover image akan menggunakan channel warna RGB dan citra yang akan disisipkan ke cover image juga dalam bentuk warna RGB, setelah cover image dan secret image akan di resize ke resolusi 512x512. Proses dalam penelitian ini menggunakan Jupyter Notebook. Berikut merupakan algoritma steganografi yang digunakan dalam penelitian ini.



Gambar 4. Algoritma Steganografi

Dari gambar 4 diatas merupakan algoritma dari steganografi dimulai dari menginputkan gambar yang diperlukan untuk dijadikan sebagi cover image dan gambar sebagai secret image. Kemudian setelah dilakukan input gambar akan dilakukan proses embedding, proses embedding ini adalah proses menyisipkan gambar secret image kedalam gambar cover image. Kemudian untuk langkah berikutnya dilakukan ekstraksi untuk mengambil kembali secret image yang berada didalam cover image.

b. Embedding dengan Metode LSB Operasi XOR

Embedding adalah proses menyisipkan citra pada cover image. Dalam konteks steganografi, embedding merujuk pada proses menyembunyikan informasi atau pesan rahasia di dalam data yang tampaknya biasa atau tidak

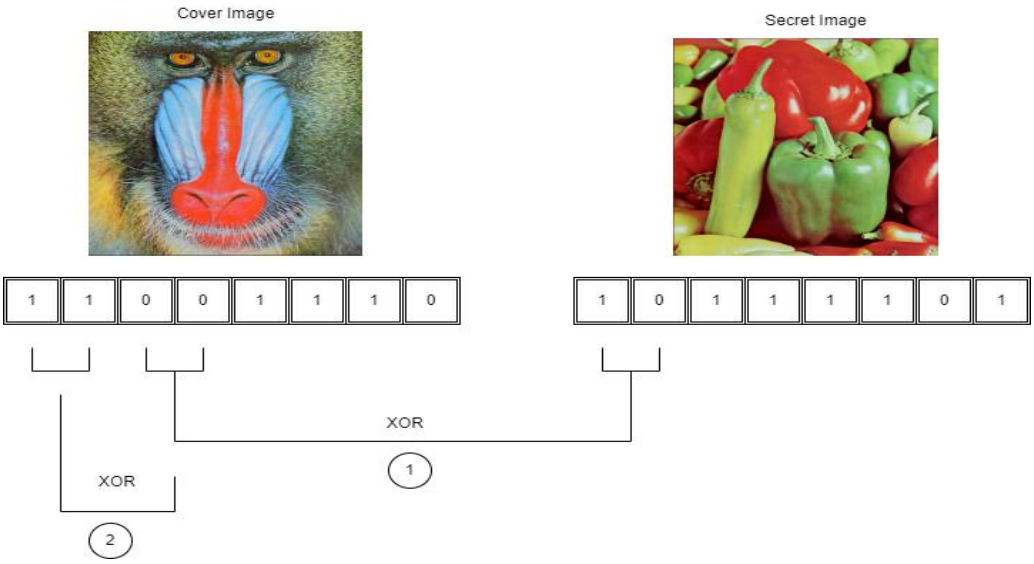
Building of Informatics, Technology and Science (BITS)
Volume 6, No 1, Juni 2024 Page: 115−124
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i1.5262

mencurigakan. Ini dapat dilakukan dalam berbagai jenis media, termasuk gambar, audio, video, dan teks. Berikut adalah langkah-langkah umum dalam proses embedding pada steganografi gambar:

1. Pemilihan Metode Embedding
   Ada beberapa metode embedding yang berbeda dalam steganografi,, dalam penelitian ini metode yang digunakan adalah Least Significant Bit (LSB)
2. Embedding Pesan
   Pesan rahasia diubah menjadi bit-bit yang kemudian disisipkan ke dalam data media cover menggunakan metode embedding yang dipilih. Dalam metode LSB, bit-bit pesan rahasia disisipkan ke dalam bit-bit yang paling tidak signifikan dari data gambar cover, sedangkan data gambar cover tetap tampak visual sama dengan sebelumnya.
3. Penyisipan dan Penyimpanan: Setelah proses embedding selesai, gambar yang telah dimodifikasi disimpan. Dalam beberapa kasus, langkah ini dapat diikuti oleh langkah kompresi untuk mengurangi ukuran file dan menyamarkan keberadaan pesan rahasia.

Pada proses ini akan dilakukan konversi piksel yang ada pada citra kedalam bentuk binary. Metode yang akan digunakan pada proses embedding adalah Least significant Bit (LSB). Dengan menggunakan LSB, bit – bit yang ada pada gambar rahasia akan disisipkan kedalam bit-bit terakhir yang ada pada cover image sehingga gambar rahasia dapat disembunyikan kedalam cover image. Citra yang telah disisipkan gambar rahasia disebut dengan stego image. Tahapan-tahapan embedding dengan metode LSB pada penelitian ini diantaranya adalah:

1. Inputkan gambar sebagai cover image dan Secret image
2. Ubah tupel bilangan bulat menjadi tupel biner (string) dalam urutan byte little-endian
3. Sembunyikan data RGB rahasia ke dalam data RGB sampul menggunakan operasi triple XOR
4. Buat gambar baru untuk menyimpan hasilnya
5. Dapatkan nilai RGB gambar sampul dan rahasia
6. Encode gambar rahasia ke dalam gambar sampul
7. Simpan gambar hasilnya



Gambar 5. Tahapan XOR

Pada Gambar 6 diatas tahapan XOR nya diantaranya adalah dimulai dari mengambil 2 bagian awal dari bit cover (penutup), kemudian Mengambil dua bit pertama dari bit secret (rahasia), lalu Mengambil dua bit terakhir dari bit cover (penutup), Mengambil dua bit kedua dari belakang dari bit cover (penutup), ketiga bit tersebut dilakukan operasi XOR dan hasil nya akan digabungkan pada bit-bit sebelumnya menjadi bit-bit baru, tahapan tersebut dilakukan pada 3 channel R,G, dan B. Pada proses embedding, citra yang disisipkan kedalam cover image langsung dilakukan proses operasi XOR sebagai pengamanan steganografi pada citra. Bit-bit yang akan di-XORkan adalah antara bit-bit yang ada pada gambar rahasia dan juga Most Signifcant Bit (MSB) dari cover image. Alur proses pada operasi XOR ini dimulai dengan melakukan operasi antara bit-bit pada cover image.

c. Pengujian Ketahanan Citra Stego

Pada proses ini akan dilakukan pengujian pada stego image yaitu citra yang telah disisipkan gambar rahasia. Pada proses ini akan dilakukan pengujian berupa kompresi, rotating, resizing dan menaikkan kontras. Pengujian ketahanan citra terhadap modifikasi yang dilakukan pada stego image menggunakan aplikasi adobe photoshop. Proses modifikasi pada citra dilakukan dengan mengompresi citra, mengubah ukuran citra, memutar citra, dan memodifikasi kontras pada citra, kemudian melakukan ekstraksi pada stego image, untuk membuktikan apakah gambar yang disisipkan pada stego image tersebut berhasil diekstrak atau tidak. Untuk pengujian kompresi dilakukan dua jenis

Building of Informatics, Technology and Science (BITS)
Volume 6, No 1, Juni 2024 Page: 115−124
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i1.5262

kompresi yaitu kompresi lossy dan kompresi lossless. Hal ini berguna agar dapat mengetahui ketahanan citra terhadap dua jenis kompresi.

d. Pengujian PSNR dan MSE

Proses pengujian ini adalah untuk mengukur perbedaan citra asli dengan stego image atau citra yang telah disisipkan gambar rahasia. PSNR (Peak Signal-to-Noise Ratio) adalah metrik yang umum digunakan untuk mengukur kualitas restorasi atau rekonstruksi dalam pengolahan sinyal dan gambar. Ini memberikan perkiraan seberapa baik kualitas suatu gambar yang telah diproses atau diubah dengan membandingkan antara sinyal asli dan sinyal yang telah diubah dengan mengabaikan kesalahan atau gangguan yang dihasilkan oleh proses tersebut. Untuk mendapatkan PSNR, diperlukan untuk melakukan pengujian MSE. Langkah-langkah umum dalam pengujian PSNR adalah sebagai berikut:

1. Persiapan Data
   Data yang diperlukan untuk pengujian PSNR adalah dua versi dari gambar yang sama: gambar asli (ground truth) dan gambar yang telah diproses atau diubah (rekonstruksi). Gambar asli ini digunakan sebagai acuan untuk membandingkan dengan gambar yang telah diubah.
2. Perhitungan PSNR
   PSNR dihitung dengan menggunakan perbandingan antara kekuatan sinyal maksimum dengan kekuatan noise yang dihasilkan oleh perubahan atau pengolahan gambar.

Dengan pengujian tersebut akan diperoleh hasil perbandingan kualitas pada gambar asli dengan stego image dan ketahanan citra terhadap serangan modifkasi pada citra yang telah disisipkan gambar rahasia. Berikut adalah rumus PSNR dan MSE.

$$MSE = \frac{1}{M}\sum_{y=0}^{M}[I(y) - I'(y)]^2 \quad (1)$$

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

Rumus 1 diatas merupakan rumus MSE dan rumus 2 adalah rumus PSNR, untuk mendapatkan hasil dari PSNR diperlukan hasil dari mean square error dari dua gambar yang telah dibandingkan sehingga didapatkan hasil untuk dimasukkan kedalam rumus PSNR.

e. Ekstraksi

Proses Ekstraksi merupakan proses memperoleh gambar rahasia dari stego image. Proses ekstraksi dalam steganografi adalah langkah-langkah untuk mengambil pesan rahasia yang disembunyikan dari media yang telah dimodifikasi (biasanya gambar, audio, atau teks) tanpa mengubah atau merusak data media tersebut. Berikut adalah langkah-langkah umum dalam proses ekstraksi pada steganografi:

1. Penerimaan Media Tersembunyi
   Penerima menerima media yang berisi pesan tersembunyi, yang bisa saja merupakan gambar, audio, atau teks.
2. Penentuan Metode Ekstraksi
   Penerima perlu mengetahui metode steganografi yang digunakan dalam menyembunyikan pesan rahasia dalam media tersebut. Pengetahuan tentang metode ini sangat penting untuk melakukan ekstraksi dengan benar.
3. Ekstraksi Pesan Rahasia
   Jika media tersebut mengandung pesan tersembunyi, langkah selanjutnya adalah mengekstraksi pesan rahasia dari media tersebut. Proses ekstraksi ini tergantung pada metode steganografi yang digunakan. Misalnya, jika metode steganografi LSB (Least Significant Bit) digunakan, penerima perlu mengekstraksi bit-bit yang paling tidak signifikan dari data media untuk mendapatkan pesan rahasia.

Pada penelitian ini dilakukan operasi XOR kembali untuk mendapatkan gambar rahasia yang telah disisipkan pada cover image. Operasi XOR dilakukan dengan secara berbalik dari proses XOR yang terdapat pada embedding.

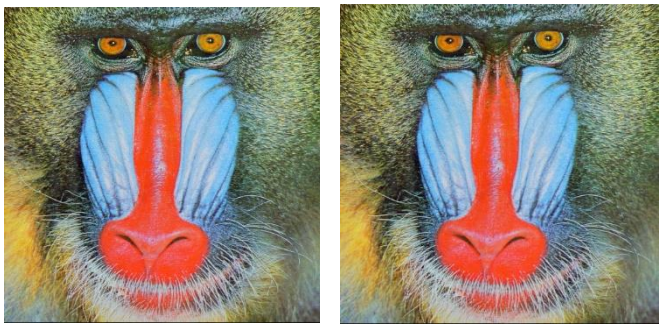
3. HASIL DAN PEMBAHASAN

Berikut ini merupakan hasil dan pembahasan dari penelitian steganografi gambar menggunakan metode LSB dengan operasi XOR diantaranya berupa hasil embedding, ekstraksi dan pengujian terhadap Stego image menggunakan PSNR dan MSE serta pengujian dengan modifikasi citra seperti kompresi, rotasi, resizing dan menaikkan kontras.

3.1 Hasil Embedding dan Ekstraksi

Berikut ini adalah hasil dari proses embedding dan ekstraksi pada citra menggunakan metode LSB dengan operasi XOR

Building of Informatics, Technology and Science (BITS)
Volume 6, No 1, Juni 2024 Page: 115−124
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i1.5262



a b

Gambar 6. Gambar a Citra Asli , gambar b Stego Image

Pada Gambar 6, gambar a merupakan gambar asli yang belum disisipkan gambar rahasia, dan gambar b merupakan gambar yang telah disisipkan gambar rahasia (Stego image), Proses embedding telah berhasil dilakukan dan menghasilkan gambar b pada gambar 8 diatas. Hasil dari proses embedding tidak merusak kualitas cover image dan sangat identik dengan gambar aslinya. Untuk mengetahui kualitas perbandingan gambar 6 diatas akan dilakukan pada pengujian PSNR. Kemudian setelah disisipkan gambar akan diekstraksi kembali untuk mendapatkan gambar yang disisipkan sebelumnya. Proses tersebut berhasil dilakukan dan menghasilkan gambar 7 dibawah ini. dari

Gambar 7. Hasil Eksraksi

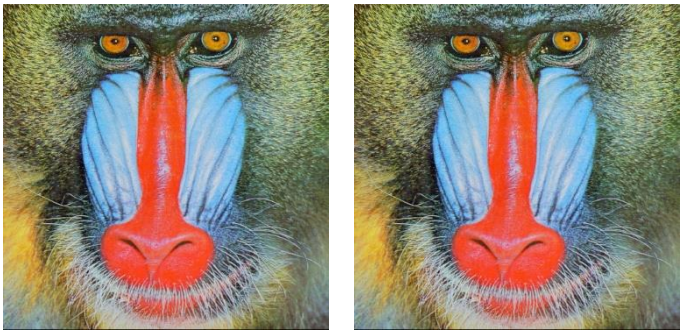
Pada gambar 7 diatas merupakan gambar hasil eksraksi dari gambar 6 diatas. Gambar secret yang telah disisipkan dapat kembali diambil, namun terdapat sedikit perbedaan kontras dan warna dari gambar yang disisipkan sebelumnya.

3.2 Pengujian Modifikasi Citra

Berikut ini adalah hasil dari pengujian modifikasi citra. pada pengujian ini menggunakan gambar BaboonRGB.bmp. dalam pengujian modifikasi ini akan mengukur persentase kerusakan pada secret image saat dilakukan modifikasi. Pengujian dilakukan dengan cara citra yang telah dimodifikasi dan akan dilakukan ekstraksi. Untuk pengujian rotasi, resize, dan penambahan kontras pengujian tersebut ditambahkan gambar yang merupakan hasil dari pengujian kompres seperti lossy dan lossless.

3.2.1 Kompresi

Berikut ini adalah hasil dari pengujian dari kompresi, pengujian dilakukan dengan melakukan kompresi lossy dan lossless dengan tingkat kompresi 80%. Berikut ini adalah gambar yang akan digunakan dalam pengujian kompresi



a b

Gambar 8. Gambar a kompresi lossy , gambar b kompresi lossless

Building of Informatics, Technology and Science (BITS)
Volume 6, No 1, Juni 2024 Page: 115−124
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i1.5262

Gambar 8 diatas merupakan gambar yang telah dilakukan kompresi secaara lossy dan kompresi secara lossless. Gambar diatas akan juga dilakukan pengujian seperti pengujian rotasi, Resize dan Modifikasi kontras. Sehingga dengan pengujian tersebut akan diketahui hasill apakah gambar yang dapat dikompresi dapat bertahan atau tidak.

Tabel 1. Hasil Pengujian Kompresi

Nama	Kerusakan	
	Lossy	Lossless
BaboonRGB.bmp	100%	0%

Dari tabel 1 diatas, dapat diketahui bahwa kompresi lossy pada saat proses ekstraksi secret image berhasil diekstrak, namun pesan yang disisipkan menjadi rusak. Hasil pengujian dengan kompresi secret image berhasil diektstrak dan kualitas secret image masih baik. Gambar 9 dibawah ini merupkan hasil dari ekstraksi lossy dan lossless.

a b

Gambar 9. a gambar ekstraksi lossless , b gambar ekstraksi lossy

3.2.2 Rotasi

Berikut ini adalah hasil dari rotasi citra yang telah disisipkan. Rotasi citra dilakukan dalam beberapa derajat diantaranya adalah sebagai berikut.

a b c

Gambar 10. a 90°ke kiri, b 90°ke kanan, c rotate 180°

Gambar 10 diatas merupakan gambar yang digunakan untuk melakukan pengujian rotate. Gambar a adalah gambar yang sudah dirotate kekiri sebesar 90°, gambar b adalah gambar yang sudah di rotate ke kanan sebesar 90°, dan gambar c adalah gambar yang sudah di rotate sebesar 180°. Pengujian rotasi juga ditambahkan dengan melakukan percobaan diataranya adalah melakukan flip secara horizontal dan vertikal.

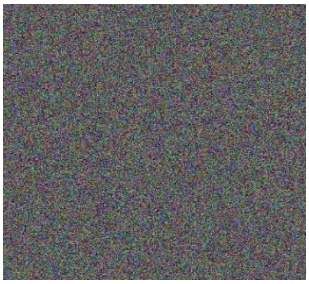
Tabel 3. Hasil Pengujian Rotasi

Rotasi	Kerusakan		
	Original	Lossy	Lossless
90°ke kiri	100%	100%	100%
90°ke kanan	100%	100%	100%
180°	100%	100%	100%
Flip horizontal	100%	100%	100%
Flip vertikal	100%	100%	100%

Dari tabel 3 diatas merupakan hasil pengujian didapatkan bahwa secret image dapat diekstrak namun dapat merusak kualitas gambar yang telah disisipkan pada cover image. untuk pengujian lossy gagal, dikarenakan kompresi

Building of Informatics, Technology and Science (BITS)
Volume 6, No 1, Juni 2024 Page: 115−124
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i1.5262

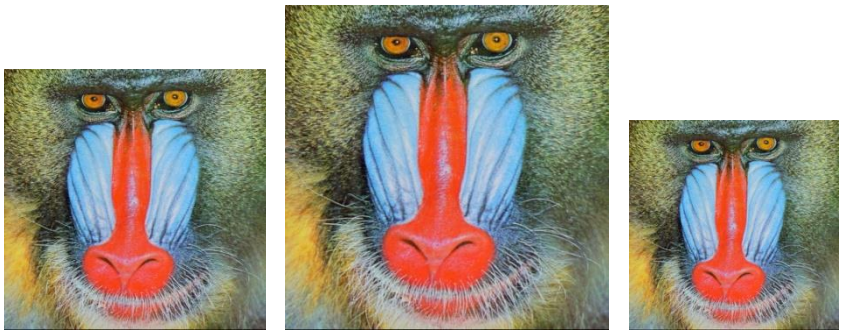
lossy merusak kualitas secret image. Berikut ini terdapat gambar ekstraksi dari hasil pengujian diatas. Semua pengujian menghasilkan seperti gambar 11 dibawah ini.



Gambar 11. Gambar ekstrasi pengujian rotasi

3.2.3 Resize

Adapun hasil dari pengujian mengubah resolusi gambar yang telah disisipkan gambar rahasia, diantaranya adalah memperkecil dan memperbesar gambar. Gambar dibawah merupakan gambar yang digunakan untuk pengujian Resize



a b c

Gambar 12. a 512x512 , b 1024x1024, c 256x256

Gambar 12 diatas merupakan gambar yang digunakan untuk pengujian resize. Gambar a merupakan gambar stego asli yang resolusinya berukuran 256x256 , gambar b adalah gambar yang diperbesar ke resolusi 512x512, dan gambar c adalah gambar yang diperkecil ke resolusi 128x128.

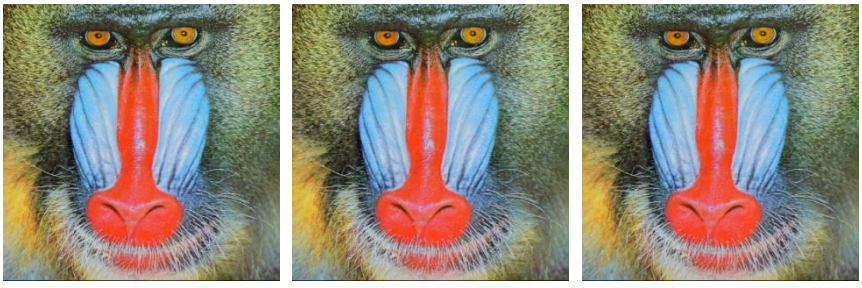
Tabel 4. Hasil Pengujian Resize

Resize	Kerusakan		
	Original	Lossy	Lossless
256x256	100%	100%	100%
1024x1024	Gagal diekstrak	Gagal diekstrak	Gagal diekstrak

Dari tabel 4 diatas, hasil pengujian dengan merubah resolusi stego image menyebabkan secret image gagal di ekstraksi dikarenakan piksel pada gambar dimodifikasi dengan cara diperbesar dan diperkecil. Hal tersebut juga berlaku pada gambar yang dikompresi secara lossy dan loseless

3.2.4 Memodifikasi Kontras

Adapun hasil dari pengujian penambahan dan pengurangan kontras dari gambar yang telah disisipkan gambar rahasia.



a b c

Gambar 13. a menambahkan kontras sebanyak 4 , b menambahkan kontras sebanyak 1, c mengurangi kontras sebanyak 4

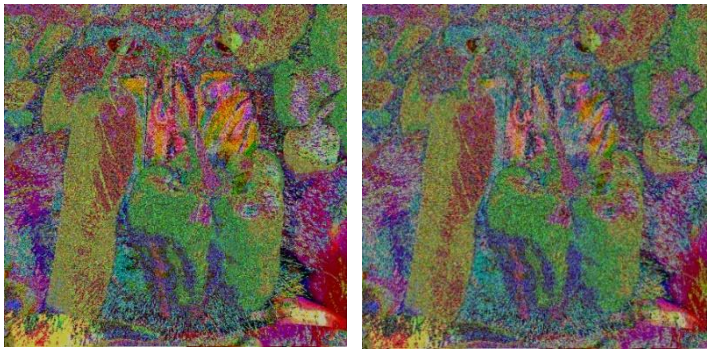
Building of Informatics, Technology and Science (BITS)
Volume 6, No 1, Juni 2024 Page: 115−124
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i1.5262

Gambar 13 diatas merupakan gambar yang digunakan dalam pengujian memodifikasi kontras. Gambar a adalah gambar yang telah ditambahkan kontras sebanyak +4, gambar b adalah gambar yang ditambahkan kontras sebanyak +1, dan gambar c adalah gambar yang dikurangi kontrasnya sebesar -4.

Tabel 5. Hasil Pengujian Modifikasi kontras

Kontras	Kerusakan		
	Original	Lossy	Lossless
-4	100%	100%	100%
-3	100%	100%	100%
-2	0%	100%	0%
-1	0%	100%	0%
+1	0%	100%	0%
+2	0%	100%	0%
+3	100%	100%	100%
+4	100%	100%	100%

Dari tabel 5 didapatkan hasil pengujian dalam memodfikasi kontras pada stego image, kontras yang ditambah maupun yang dikurangi lebih dari 2 akan merusak secret image yang ada pada stego image. sehingga hasil dari pengujian tersebut, jika modifikasi kontras dilakukan lebih dari 2 maka kualitas secret image tersebut menjadi rusak. Pada gambar 14 dibawah ini merupakan hasil dari ekstraksi jika dilakukan penambahan kontras sebanyak lebih dari 2 dan melakukan pengurangan kontras sebanyak lebih dari 2.



a b

Gambar 14. a menambahkan kontras sebanyak 3 , b menambahkan kontras sebanyak 4

3.3 Pengujian PSNR dan MSE

Adapun hasil dari pengujian PSNR dan MSE dari beberapa gambar yang disisipkan gambar rahasia dengan menggunakan metode LSB dengan triple XOR.

Tabel 6. Hasil Pengujian PSNR dan MSE

Nama	PSNR	MSE
BaboonRGB.bmp	49.17685604469248	0.5117950439453125
airplane.bmp	48.636757605991335	0.5771942138671875
goldhill.bmp	47.128502285988624	0.7255096435546875

Dari tabel 6 diatas merupakan hasil pengujian PSNR dan MSE didapatkan hasil yang cukup baik yaitu dengan PSNR skor 49 dB dan MSE rendah. hasil tersebut membuktikan bahwa metode LSB sangat baik dalam aspek imperceptible.

4. KESIMPULAN

Adapun kesimpulan dari penelitian ini adalah penggunaan metode LSB memiliki beberapa kelebihan dan kekurangan. Untuk kelebihan dari metode LSB ini adalah perbandingan gambar asli (original image) dengan citra yang telah disisipkan gambar rahasia (stego image) adalah sulit untuk membedakannya dengan citra yang asli dan tingkat imperceptible nya sangat baik dapat dibuktikan dengan hasil pengujian PSNR dengan skor 49 dB. Skor tersebut merupakan skor yang bagus. Dari hasil pengujian pengujian modifikasi citra pada original stego image maupun yang sudah dikompresi secara lossy dan lossless dihasilkan kekurangan pada metode ini. Untuk kekurangan metode ini adalah saar dilakukan modifikasi di citra stego, maka akan terjadi kerusakan pada gambar citra yang disisipkan karena metode LSB adalah metode steganografi di ranah spatial. Metode LSB memodifikasi bit-bit yang terdapat didalam gambar saat menyisipkan gambar rahasia, sehingga penggunaan metode LSB dapat bermasalah jika citra stego

Building of Informatics, Technology and Science (BITS)
Volume 6, No 1, Juni 2024 Page: 115−124
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i1.5262

dimodifikasi seperti dikompresi, dirotate, diresize dan memodifikasi kontras. Adapun kekurangan lain di metode LSB adalah jika kapasitas media yang disisipkan terlalu besar maka terdapat perubahan yang terjadi pada cover image dan hal tersebut dapat menyebabkan pengurangan kualitas cover image. Penambahan triple XOR pada LSB dapat meningkatkan keamanan citra stego, sehingga dibutuhkan kombinasi XOR untuk mengekstrak gambar yang disisipkan ke dalam citra stego. Untuk penelitian yang akan datang diperlukan metode yang lebih baik agar dapat mengamankan secret image dari modifikasi citra.

REFERENCES

[1] A. Yang, Y. Bai, T. Xue, Y. Li, and J. Li, "A novel image steganography algorithm based on hybrid machine leaning and its application in cyberspace security," Future Generation Computer Systems, vol. 145, pp. 293–302, 2023, doi: https://doi.org/10.1016/j.future.2023.03.035.

[2] T. Indriyani, S. Nurmuslimah, A. Taufiqurrahman, R. K. Hapsari, C. N. Prabiantissa, and A. Rachmad, "Steganography on Color Images Using Least Significant Bit (LSB) Method," 2023, pp. 39–48. doi: 10.2991/978-94-6463-174-6_5.

[3] M. Hassaballah, Digital Media Steganography: Principles, Algorithms, Advances. 2020. doi: 10.1016/C2018-0-04865-3.

[4] D. Ratnasari and A. S. Aji, "Text to Color Image Steganography Using LSB Technique and XOR Operations," vol. 3, no. 2, pp. 59–63, 2019, [Online]. Available: http://pubs.ascee.org/index.php/ijabis|E:info@ascee.org

[5] R. Rizal, A. Rahmatulloh, N. Widiyasono, R. R, and D. R. Nursamsi, "Steganography: Combination of Least Significant Bit (LSB) and Bit-Plane Complexity Segmentation (BPCS) Methods for Hiding Massage on Image and Audio," Int J Comput Appl, vol. 185, no. 21, pp. 1–7, Jul. 2023, doi: 10.5120/ijca2023922929.

[6] D. Megías, W. Mazurczyk, and M. Kuribayashi, "Data hiding and its applications: Digital watermarking and steganography," Applied Sciences (Switzerland), vol. 11, no. 22, Nov. 2021, doi: 10.3390/app112210928.

[7] A. Setyono and D. R. Ignatius Moses Setiadi, "Securing and hiding secret message in image using xor transposition encryption and lsb method," in Journal of Physics: Conference Series, Institute of Physics Publishing, Apr. 2019. doi: 10.1088/1742-6596/1196/1/012039.

[8] R. M. Neamah, J. A. Abed, and E. A. Abbood, "Hide text depending on the three channels of pixels in color images using the modified LSB algorithm," International Journal of Electrical and Computer Engineering, vol. 10, no. 1, pp. 809–815, 2020, doi: 10.11591/ijece.v10i1.pp809-815.

[9] A. Ahmed and A. Ahmed, "A Secure Image Steganography using LSB and Double XOR Operations," 2020. [Online]. Available: https://www.researchgate.net/publication/342663405

[10] S. Utama and R. Din, "Performance Review of Feature-Based Method in Implementation Text Steganography Approach," Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 28, no. 2, pp. 325–333, Oct. 2022, doi: 10.37934/araset.28.2.325333.

[11] S. K. Salim, M. M. Msallam, and H. I. Olewi, "Hide text in an image using Blowfish algorithm and development of least significant bit technique," Indonesian Journal of Electrical Engineering and Computer Science, vol. 29, no. 1, pp. 339–347, Jan. 2023, doi: 10.11591/ijeecs.v29.i1.pp339-347.

[12] V. Sabeti and M. Amerehei, "Secure and Imperceptible Image Steganography in Discrete Wavelet Transform Using the XOR Logical Function and Genetic Algorithm," vol. 14, no. 2, pp. 167–179, 2022, doi: 10.22042/ISECURE.2022.

[13] N. Hidayasari and F. Yanto, "Analysis of Least Significant Bit Method Using Sequential Encoding-Decoding in Steganography Digital Image," vol. 3, pp. 201–205, 2020.

[14] G. Swain, Advanced Digital Image Steganography Using LSB, PVD, and EMD: Emerging Research and Opportunities. 2019. doi: 10.4018/978-1-5225-7516-0.

[15] L. B. Handoko and C. Umam, "Data Security Using Color Image Based on Beaufort Cipher, Column Transposition and Least Significant Bit (LSB)id 2 *Corresponding author," 2023.

[16] E. Z. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and M. K. Sarker, "LSB-based Bit Flipping Methods for Color Image Steganography," in Journal of Physics: Conference Series, Institute of Physics Publishing, May 2020. doi: 10.1088/1742-6596/1501/1/012019.

[17] T. Bhuiyan, A. H. Sarower, M. Rashed Karim, and M. Maruf Hassan, "An image steganography algorithm using LSB replacement through XOR substitution," in 2019 International Conference on Information and Communications Technology, ICOIACT 2019, Institute of Electrical and Electronics Engineers Inc., Jul. 2019, pp. 44–49. doi: 10.1109/ICOIACT46704.2019.8938486.

[18] R. Imanda, H. Nasution, A. Fauzi, and H. Khair, "Journal of Artificial Intelligence and Engineering Applications Hybrid Cryptosystem Algorithm Vigenere Cipher and Base64 for Text Message Security Utilizing Least Significant Bit (LSB) Steganography as Insert into Image," 2023. [Online]. Available: https://ioinformatic.org/

[19] A. A. Almayyahi, R. Sulaiman, F. Qamar, A. E. Hamzah, K. Malaysia, and U. Bangi, "High-Security Image Steganography Technique using XNOR Operation and Fibonacci Algorithm," 2020. [Online]. Available: www.ijacsa.thesai.org

[20] A. I. H. Al-Jarah and J. L. O. Arjona, "Secret Key Steganography: improve security level of LSB algorithm," in 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2021, pp. 215–220. doi: 10.1109/UEMCON53757.2021.9666569.