STEGANOGRAFI METODE *INVERTED* LSB MENGGUNAKAN POLA ADAPTIF DAN DCT

Kukuh Yulion Setia Prakoso[1], Yulison Herry Chrisnanto [2], Fatan Kasyidi [3]

[123,] Informatika, Fakultas Sains & Informatika, Universitas Jenderal Achmad Yani

Jln. Terusan Jend. Sudirman, Kota Cimahi, Jawa Barat 40525
[1] kukuhyulionsp20@if.unjani.ac.id, [2] yhc@if.unjani.ac.id, [3] fatan.kasyidi@lecture.unjani.ac.id

Abstract

Information security is a crucial aspect in protecting data from potentially damaging threats, which includes the use of steganography techniques to hide secret messages in media such as images. Previous research focused on the Inverted LSB method with adaptive patterns, which has been shown to improve imperceptibility over conventional methods. Evaluation using MSE, PSNR and SSIM values showed relatively high image quality, although there was a decrease as the length of the inserted message increased. Test results for messages containing 1000 characters resulted in MSE values range from 0.001465 to 0.045898, for PSNR values range from 61.512825 to 76.472891 and for SSIM values range from 0.998904 to 0.999989, while for messages of 5000 characters, MSE values range from 0.040802 to 0.138763, for PSNR values range from 56.708053 to 62.023989 and for SSIM values range from 0.998151 to 0.999535. Based on the test results and comparing them with previous research, this study obtained better results in maintaining image quality as the message length increases, namely for messages containing 1000 characters, the MSE values range from 0.026306 to 0.039501, for PSNR values range from 56.1355 to 63.1976 and for SSIM values range from 0.99743 to 0.99839, while for messages of 5000 characters, the MSE values range from 0.026307 to 0.039506, for PSNR values range from 56.1333 to 63.1973 and for SSIM values range from 0.99743 to 0.99839.

Keywords : *steganography, inverted LSB, DCT, MSE, PSNR*

Abstrak

Keamanan informasi merupakan aspek krusial dalam perlindungan data dari ancaman yang berpotensi merusak, mencakup penggunaan teknik steganografi untuk menyembunyikan pesan rahasia dalam media seperti gambar. Penelitian terdahulu memfokuskan pada metode *Inverted* LSB dengan pola adaptif, yang telah terbukti meningkatkan *imperceptibility* dibandingkan metode konvensional. Evaluasi menggunakan nilai MSE, PSNR dan SSIM menunjukkan kualitas gambar yang relatif tinggi, meskipun terdapat penurunan seiring dengan peningkatan panjang pesan yang disisipkan. Hasil pengujian untuk pesan berisi 1000 karakter menghasilkan nilai MSE berkisar 0.001465 hingga 0.045898, untuk nilai PSNR berkisar 61.512825 hingga 76.472891 dan untuk nilai SSIM berkisar 0.998904 hingga 0.999989, sedangkan untuk pesan 5000 karakter, nilai MSE berkisar 0.040802 hingga 0.138763, untuk nilai PSNR berkisar 56.708053 hingga 62.023989 dan untuk nilai SSIM berkisar 0.998151 hingga 0.999535. Berdasarkan hasil pengujian dan membandingkannya dengan penelitian sebelumnya, pada penelitian ini didapatkan hasil yang lebih baik dalam mempertahankan kualitas gambar seiring meningkatnya panjang pesan, yaitu untuk pesan berisi 1000 karakter menghasilkan nilai MSE berkisar 0.026306 hingga 0.039501, untuk nilai PSNR berkisar 56.1355 hingga 63.1976 dan untuk nilai SSIM berkisar 0.99743 hingga 0.99839, sedangkan untuk pesan 5000 karakter, nilai MSE berkisar 0.026307 hingga 0.039506, untuk nilai PSNR berkisar 56.1333 hingga 63.1973 dan untuk nilai SSIM berkisar 0.99596 hingga 0.99783.

Kata kunci : *steganografi, LSB terbalik, DCT, MSE, PSNR*

1. PENDAHULUAN

Keamanan informasi adalah praktik atau serangkaian langkah yang diambil untuk melindungi data, sistem komputer, jaringan, dan informasi rahasia dari akses yang tidak sah, penggunaan yang tidak sah, perubahan, atau penghancuran yang tidak sah[1]. Keamanan informasi juga mencakup pendidikan dan kesadaran risiko serta pelatihan terkait, agar individu yang terlibat dalam pengelolaan informasi sensitif dapat mengidentifikasi dan mengatasi ancaman keamanan dengan efektif[2].

Salah satu cara pengamanan informasi atau pesan adalah melalui teknik penyembunyian pesan atau Steganografi[3] yang dimana Steganografi adalah seni menyembunyikan pesan atau informasi rahasia di dalam media yang tampak biasa, seperti gambar, teks, audio, atau video, tanpa menarik perhatian pihak yang tidak dituju[4].

Steganografi melibatkan penggunaan beragam metode untuk menyembunyikan pesan rahasia dalam berbagai jenis media. Salah satu metode pada media gambar adalah LSB (*Least significant bit*), dimana informasi tambahan disisipkan dengan mengganti bit-bit paling tidak signifikan dalam piksel gambar[5]. Saat ini, sudah terdapat pengembangan dari metode LSB yaitu salah satunya adalah metode *Inverted* LSB yang menggunakan pola adaptif[4]. Metode ini sering digunakan dalam format gambar seperti BMP atau PNG[6].

Penelitian sebelumnya telah menunjukan bahwa metode *Inverted* LSB yang menggunakan pola adaptif memberikan hasil peningkatan terhadap *imperceptibility* yang lebih baik dibandingkan dengan metode *Inverted* LSB biasa. Metode *Inverted* LSB yang menggunakan pola adaptif setelah dilakukan pengujian dan perbandingan dengan metode sebelumnya menghasilkan peningkatan nilai yaitu nilai PSNR (*Peak Signal Noise Ratio*) berkisar antara 52,49 hingga 57,45, dan SSIM (*Structural Similarity Index Measurement)* berkisar antara 0,9991 hingga 0,9999 dengan kapasitas 1 BPP (*Bit Per Pixel)*.

Pada penelitian ini dilakukan pula metode transformasi domain dalam steganografi. DCT, salah satu jenis Transformasi domain sederhana, mengubah representasi spasial dari data menjadi domain frekuensi[7]. DCT banyak digunakan dalam kompresi gambar dan video, di mana sinyal-sinyal pixel dipecah menjadi koefisien-koefisien frekuensi yang menggambarkan kontribusi relatif dari berbagai komponen frekuensi terhadap gambar asli. Keunggulan DCT juga terletak pada kemampuannya dalam mengkompresi data dengan tingkat kerugian yang dapat dikendalikan, membuatnya menjadi bagian integral dari algoritma kompresi seperti JPEG untuk gambar[8] dan MPEG untuk video.

Sudah ada beberapa penelitian terdahulu mengenai penggunaan metode DCT sebagai metode peningkatan kapasitas penyisipan pesan diantaranya seperti pada Tabel 1

TABEL I PENELITIAN TERDAHULU

No	Nama Penulis	Judul Penelitian
1.	O.O. Evsutin, A.O. Osipov (2017)	*The algorithm of the high-capacity information embedding into the digital images DCT domain using differential evolution*
2.	Navdeep Kaur, Sukhjeet K. Ranade (2012)	*High Capacity Data Embedding System in DCT domain for Colored Images*

Pada penelitian (1) Tabel 1 dihasilkan akurasi pada salah satu gambar yaitu, PSNR 33,00 dan BPP 4,11 untuk *Adaptive algorithm* sedangkan untuk algoritma QTAR yaitu, PSNR 32,99 dan BPP 3,02[9].

Pada penelitian (2) Tabel 1 dihasilkan akurasi pada salah satu gambar yaitu, PSNR 47.2319, MSE 1.2299, dan BER 0.0212[10].

Dalam penelitian ini, difokuskan pada penggunaan metode steganografi *Inverted* LSB yang menggunakan pola adaptif sebagai metode penyisipan pada gambar sampul dan DCT sebagai metode pengolahan citra pada gambar sampul. Studi ini bertujuan untuk mengimplementasikan metode steganografi *Inverted* LSB yang menggunakan pola adaptif yang digabungkan dengan metode DCT, serta pengaruh terhadap kapasitas penyisipan pesan dan *imperceptibility* dari hasil penyembunyian pesan yang berupa teks pada gambar sampul. Untuk evaluasi hasil menggunakan PSNR (*Peak Signal Noise Ratio*), MSE (*mean squared error*) dan SSIM (*Structural Similarity Index Measurement)*.

2. TINJAUAN LITERATUR

2.1 Steganografi

Istilah "steganografi" berasal dari bahasa Yunani, di mana "steganos" berarti "tersembunyi" dan "graphein" berarti "menulis" atau "menggambar"[11]. Steganografi merupakan teknik tersembunyi yang telah lama digunakan untuk menyembunyikan pesan rahasia dalam medium komunikasi seperti gambar, teks, atau audio tanpa menarik perhatian pihak ketiga. Metode ini bertujuan untuk memastikan keamanan dan kerahasiaan informasi dengan cara menyembunyikan pesan dalam suatu media sehingga tampak sebagai data yang tidak mencurigakan. Beberapa teknik steganografi meliputi penyisipan pesan dalam gambar dengan memanfaatkan bit yang kurang signifikan, mengubah pola piksel, atau bahkan menyembunyikan pesan dalam frekuensi audio yang tidak terdengar oleh telinga manusia. Keunggulan steganografi terletak pada kemampuannya menyembunyikan pesan secara efektif tanpa memicu kecurigaan, sehingga dapat menjadi sarana yang kuat untuk komunikasi rahasia.

2.2 Gambar

Dalam konteks steganografi, gambar digunakan sebagai media untuk menyembunyikan pesan rahasia tanpa mengubah penampilan visual secara signifikan[12]. Teknik ini memanfaatkan karakteristik gambar digital yang memiliki informasi dalam bentuk piksel. Dalam proses steganografi, informasi rahasia disisipkan ke dalam piksel-piksel gambar dengan cara memanfaatkan komponen warna atau nilai numerik dari piksel tersebut[13]. Metode ini bisa mencakup penyisipan bit pesan rahasia di bit-bit yang kurang signifikan dari piksel, atau bahkan memodifikasi nilai-nilai piksel dengan pola yang tidak terlihat secara langsung oleh mata manusia. Tujuannya adalah untuk memastikan bahwa meskipun pesan rahasia ada di dalam gambar, perubahan yang dihasilkan tidak terlihat secara kasat mata dan tidak mencurigakan bagi yang tidak mengetahui adanya pesan tersembunyi.

2.3 *Least* significant *bit*

LSB (*Least significant bit*) adalah salah satu metode yang umum digunakan dalam steganografi, terutama untuk menyembunyikan pesan rahasia dalam gambar digital[14]. Ini mengacu pada penggunaan bit-bit paling tidak signifikan dari komponen warna (red, green, blue) dalam setiap piksel gambar. Dalam teknik ini, nilai-nilai biner dari piksel diubah sedikit demi sedikit dengan menyisipkan bit-bit dari pesan rahasia ke bit-bit paling tidak signifikan tersebut. Misalnya, jika nilai piksel adalah 10110001 dan bit pesan rahasia adalah 010, teknik LSB menyisipkan bit-bit pesan rahasia tersebut ke dalam piksel sehingga perubahan ini tidak secara signifikan memengaruhi tampilan visual gambar. Dalam pengambilan bit paling tidak signifikan, perubahan nilai-nilai tersebut biasanya sulit dikenali secara visual oleh manusia, menjadikannya cara yang populer untuk menyembunyikan informasi secara rahasia di dalam gambar tanpa mengganggu penampilan visualnya

2.4 *Discrete Cosine Transform*

Discrete Cosine Transform (DCT) adalah teknik pengolahan sinyal yang digunakan untuk mengubah representasi spasial dari data menjadi domain frekuensi[7]. Discrete Cosine Transform (DCT) merupakan teknik penting dalam konteks kompresi data, terutama dalam kompresi gambar dan video.

Berikut persamaan perhitungan DCT yang bisa dilihat pada persamaan (1) yang disampaikan oleh[15], [16]:

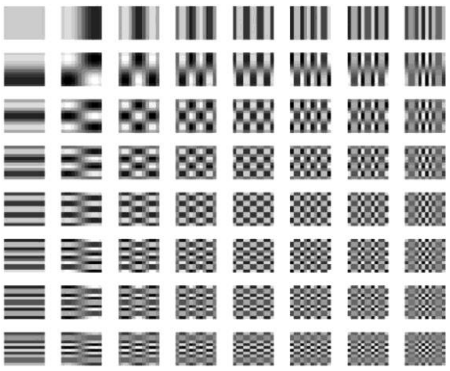
$$F(u,v) = \frac{2}{N} C(u)C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (1)$$

Kemudian untuk $u = 0, \dots, N-1$ dan $v = 0, \dots, N-1$

yang dimana $N = 8$ dan $C(k) = \begin{cases} \frac{1}{\sqrt{2}} & \text{jika } k \leq 0 \\ 1 & \text{jika } k > 0 \end{cases}$

$f(x,y)$ adalah nilai setiap piksel dalam blok 8×8 yang dipilih, dan $F(u,v)$ adalah koefisien DCT setelah transformasi. Transformasi blok 8×8 juga merupakan blok 8×8 yang terdiri dari $F(u,v)$.

DCT memungkinkan representasi sinyal gambar atau video dalam bentuk koefisien-koefisien frekuensi yang memungkinkan eliminasi informasi yang tidak signifikan dengan mengurangi redundansi data. Ketika menggunakan DCT untuk kompresi, sinyal gambar atau video dipecah menjadi blok-blok kecil, kemudian setiap blok diubah ke dalam domain frekuensi dengan DCT[17].



Gambar 1. Dasar DCT Lengkap Ukuran N = 8

Koefisien DCT yang dihasilkan kemudian diurutkan berdasarkan tingkat kontribusi frekuensi mereka terhadap sinyal asli. Dengan melakukan kuantisasi pada koefisien yang kurang signifikan, informasi yang dianggap kurang penting dapat dihilangkan dengan tingkat kerugian yang dapat dikendalikan, memungkinkan kompresi yang signifikan tanpa kehilangan kualitas gambar atau video yang terlalu banyak. Teknik ini menjadi dasar dari berbagai standar kompresi seperti JPEG untuk gambar dan MPEG untuk video.

2.5 *Inverted* LSB yang menggunakan pola adaptif

Metode steganografi *Inverted* LSB yang memanfaatkan pola adaptif merupakan teknik penyisipan pesan rahasia dalam media digital dengan menggunakan *least significant bit* (LSB) yang diubah berdasarkan pola adaptif. Dalam hal ini, pola adaptif mengacu pada keputusan yang dibuat berdasarkan analisis terhadap piksel sekitarnya untuk menentukan apakah perubahan pada bit LSB diperlukan atau tidak[4].

2.6 Imperceptibility

Imperceptibility adalah salah satu prinsip penting dalam steganografi yang mengacu pada kemampuan pesan tersembunyi untuk tidak terdeteksi oleh pengamat yang tidak sah[18]. Dalam steganografi bertujuan untuk menyembunyikan informasi secara tidak terlihat dalam media penampung, seperti gambar atau teks, sehingga tidak menarik kecurigaan. Metode yang efektif dalam mencapai *imperceptibility* melibatkan penyisipan pesan tersembunyi dengan modifikasi minimal pada data penampung, sehingga tidak mengganggu kualitas atau karakteristik asli dari media tersebut, tetapi tetap memungkinkan pengambilan kembali pesan dengan akurasi yang tinggi.

2.7 Fidelity

Fidelity dalam steganografi mengacu pada kemampuan sistem untuk mempertahankan kualitas asli atau integritas data penampung, seperti gambar atau teks, setelah pesan

tersembunyi disisipkan[18]. Artinya, teknik steganografi yang memiliki tingkat *fidelity* yang tinggi akan memastikan bahwa proses penyisipan pesan tersembunyi tidak merusak atau mengurangi kualitas visual atau struktural dari media yang digunakan. Dengan kata lain, pesan tersembunyi harus disisipkan sedemikian rupa sehingga tidak terlihat bagi mata manusia, tetapi juga tidak mengganggu penggunaan normal atau interpretasi media tersebut.

2.8 *Recovery*

Recovery dalam steganografi merujuk pada kemampuan untuk mengambil kembali pesan tersembunyi yang telah disisipkan ke dalam media penampung tanpa kehilangan informasi atau mengurangi kualitasnya[18]. Proses *recovery* ini harus dilakukan dengan presisi tinggi sehingga pesan tersembunyi dapat dipulihkan dengan akurasi maksimum. Dalam praktiknya, teknik-teknik *recovery* dalam steganografi sering melibatkan ekstraksi dan dekripsi pesan tersembunyi menggunakan algoritma khusus, yang memungkinkan untuk memisahkan pesan tersembunyi dari media penampung tanpa menyebabkan kerusakan pada informasi yang disembunyikan atau pada media itu sendiri.

2.9 *Mean Squared Error*

Mean Squared Error (MSE) dalam konteks steganografi merujuk pada metode untuk mengukur seberapa baik informasi yang tersembunyi dalam gambar sampul dengan menggunakan teknik steganografi. MSE digunakan untuk membandingkan perbedaan antara piksel-piksel pada gambar asli dengan gambar yang telah dimodifikasi untuk menyembunyikan informasi rahasia. Semakin kecil nilai MSE, semakin sedikit perbedaan antara gambar asli dan gambar yang dimodifikasi, menunjukkan bahwa informasi yang disembunyikan telah berhasil diintegrasikan dengan baik ke dalam media penutup tanpa mengganggu kualitas visualnya secara signifikan. Berikut persamaan perhitungan MSE yang bisa dilihat pada persamaan (2) yang disampaikan oleh[8]:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{i,j} - x'_{i,j})^2 \quad (2)$$

Yang dimana $x_{i,j}$ dan $x'_{i,j}$ masing-masing adalah citra stego dan citra asli yang akan dibandingkan dan ukuran gambar mereka adalah (M x N). di mana M dan N adalah jumlah baris dan kolom.

2.10 *Peak Signal Noise Ratio*

Peak Signal-to-Noise Ratio (PSNR) dalam steganografi adalah metrik yang digunakan untuk mengevaluasi kualitas citra yang telah dimodifikasi dengan teknik steganografi. Berikut persamaan perhitungan PSNR yang bisa dilihat pada persamaan (3) yang disampaikan oleh[10]:

$$PSNR = 10 \log_{10} \frac{255^2}{\frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{i,j} - x'_{i,j})^2} \quad (3)$$

Yang dimana $x_{i,j}$ dan $x'_{i,j}$ menunjukkan piksel dari gambar asli dan gambar yang direproduksi, dan gambar berukuran $M \times N$.

PSNR mengukur perbandingan antara kekuatan sinyal maksimum yang diinginkan dengan kekuatan noise yang terdapat dalam citra. Dalam steganografi, PSNR memberikan informasi tentang seberapa baik citra yang telah dimodifikasi untuk menyembunyikan informasi rahasia dengan citra asli. Semakin tinggi nilai PSNR, semakin sedikit noise yang dihasilkan, menunjukkan bahwa informasi yang disembunyikan telah berhasil terintegrasi ke dalam citra penutup dengan sedikit atau tanpa mengorbankan kualitas visual secara signifikan.

2.11 *Structural Similarity Index*

Structural Similarity Index (SSIM) dalam steganografi adalah metrik yang digunakan untuk mengevaluasi seberapa baik citra yang dimodifikasi dengan teknik steganografi mempertahankan struktur dan informasi visual dari citra asli. SSIM mengukur kesamaan struktural, kontras, dan kecerahan antara citra asli dan citra yang telah dimodifikasi, serta sensitif terhadap perubahan kecil dalam citra. Dalam steganografi, SSIM membantu dalam menentukan sejauh mana informasi rahasia dapat

disembunyikan tanpa merusak kualitas visual citra penutup secara signifikan. Semakin tinggi nilai SSIM, semakin baik citra penutup mempertahankan informasi dan struktur citra asli, menandakan keberhasilan teknik steganografi dalam menyembunyikan informasi dengan efektif.

Pada citra berwarna RGB, SSIM dapat didefinisikan dengan Persamaan SSIM berikut:

$$SSIM(i,i') = l(i,i')c(i,i')s(i,i') \quad (4)$$

$$l(i,i') = \frac{2\mu_i\mu_{i'}+C1}{\mu_i^2+\mu_{i'}^2+C1} \quad (5)$$

$$c(i,i') = \frac{2\sigma_i\sigma_{i'}+C2}{\sigma_i^2+\sigma_{i'}^2+C2} \quad (6)$$

$$s(i,i') = \frac{\sigma_{ii'}+C3}{\sigma_i\sigma_{i'}+C3} \quad (7)$$

$$\mu_i = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{o} i_{xyz}}{MNO} \quad (8)$$

$$\sigma_i^2 = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{o}(i_{xyz}-\mu_i)^2}{MNO} \quad (9)$$

$$\sigma_{ii'} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{o}(i_{xyz}-\mu_i)(i'_{xyz}-\mu_{i'})}{MNO} \quad (10)$$

$$\mu_{i'} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{o} i'_{xyz}}{MNO} \quad (11)$$

$$\sigma_{i'}^2 = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{o}(i'_{xyz}-\mu_{i'})^2}{MNO} \quad (12)$$

$$\sigma_{i'i} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{o}(i'_{xyz}-\mu_{i'})(i_{xyz}-\mu_i)}{MNO} \quad (13)$$

Faktor pertama dalam persamaan (4) adalah $l(i,i')$ yang merupakan fungsi untuk membandingkan pencahayaan antara gambar i dan gambar i'. Nilai maksimum dari $l(i,i')$ adalah 1, yang terjadi ketika luminansi (μ) dari kedua gambar tersebut sama $(\mu = \mu')$. Faktor kedua adalah $c(i,i')$, yang membandingkan kontras antara gambar i dan gambar i'. Nilai maksimum $c(i,i')$ adalah 1, yang terjadi ketika kontras kedua gambar, dihitung berdasarkan standar deviasi (σ), adalah sama $(\sigma = \sigma')$. Faktor ketiga adalah $s(i,i')$, fungsi yang membandingkan struktur antara gambar i dan gambar i' berdasarkan koefisien korelasi, dengan catatan bahwa $\sigma_{ii'}$ adalah kovariansi antara gambar i dan gambar i'. Nilai maksimum $s(i,i')$ adalah 1, yang tercapai jika $\sigma_{ii'} = \sigma_i\sigma_{i'}$. Jadi, jika ketiga faktor memiliki nilai 1, maka nilai maksimum SSIM adalah 1. Banyak penelitian menyebutkan bahwa rentang nilai SSIM adalah antara 0 sampai 1, tetapi sebenarnya nilai minimum SSIM bisa mencapai -1. Hal ini dikarenakan nilai negatif sangat jarang terjadi dan tidak relevan. Konstanta C1, C2, dan C3 digunakan untuk menghindari penyebut nol, sehingga disarankan untuk menggunakan nilai \($C1 = (0.01 \times 255)^2$, $C2 = (0.03 \times 255)^2$, dan $C3 = C2/2$ sebagai nilai tetapannya[19].

3. METODOLOGI PENELITIAN

Gambar 2. Alur Metodologi Penelitian

3.1. Tahap Penginputan Pesan Rahasia dan Gambar Sampul

Pada tahap pertama, program ini membaca gambar sampul dan pesan rahasia yang akan disembunyikan. Gambar sampul dipilih dengan ekstensi '.jpg' berukuran 512x512 piksel. Setelah

gambar dipilih, gambar tersebut dibaca ke dalam program dan kemudian ditampilkan untuk memverifikasi bahwa gambar yang benar telah dipilih. Selanjutnya, memilih jenis pesan rahasia berupa teks, melalui input prompt. Program membuka file teks dengan ekstensi '.txt', dan mengubahnya menjadi bentuk numerik. Proses ini memastikan bahwa teks dapat digunakan sebagai pesan rahasia yang akan disembunyikan dalam gambar sampul.

3.2. Tahap Pemrosesan Gambar Menggunakan Metode DCT

Pada tahap pemrosesan gambar sampul, program dimulai dengan mengubah ukuran gambar sampul yang telah dibaca menjadi 512x512 piksel dan mengkonversinya ke tipe data double untuk mempersiapkan transformasi selanjutnya. Setelah itu, program menerapkan Discrete Cosine Transform (DCT) pada gambar sampul seperti yang sudah dijelaskan pada tinjauan literatur sub-bab 2.4 yaitu pada persamaan (1). DCT adalah transformasi yang mengubah data gambar dari domain spasial ke domain frekuensi, memungkinkan kompresi dan pengolahan yang lebih efisien. Dalam implementasi ini, gambar sampul dipecah menjadi blok-blok berukuran 8x8 piksel, dan setiap blok diterapkan DCT dua dimensi.

Hasil transformasi DCT ini kemudian dikuantisasi menggunakan matriks kuantisasi yang telah ditentukan, Q. Selama Kuantisasi, setiap koefisien dalam matriks DCT 8×8 dibagi dengan nilai kuantisasi yang sesuai. Koefisien yang dikuantisasi didefinisikan dalam persamaan (14), dan kebalikan dari proses tersebut dapat dicapai dengan persamaan (15) yang disampaikan oleh[15]:

$$F(u,v)_{Quantization} = round\left(\frac{F(u,v)}{Q(u,v)}\right) \quad (14)$$

$$F(u,v)_{deQ} = F(u,v)_{Quantization} \times Q(u,v) \quad (15)$$

Kuantisasi bertujuan untuk mengurangi jumlah data yang diperlukan dengan membagi setiap elemen blok DCT dengan elemen yang sesuai dari matriks Q dan kemudian membulatkan hasilnya. Proses ini membuat data menjadi kurang sensitif terhadap perubahan kecil, sehingga lebih tahan terhadap kompresi dan gangguan. Tujuan lainnya dari kuantisasi adalah untuk mengurangi sebagian besar koefisien DCT frekuensi tinggi yang kurang penting menjadi nol. Semakin banyak angka nol yang dihasilkan, semakin baik kompresi gambarnya. Matriks Q biasanya memiliki nilai yang lebih kecil di sudut kiri atas dan nilai yang lebih besar di sudut kanan bawah. Komite JPEG telah merekomendasikan matriks Q tertentu yang memberikan kinerja mendekati optimal, dengan matriks Q untuk komponen luminansi dan krominansi yang telah ditentukan seperti pada matriks (16) dan (17) yang disampaikan oleh[15].

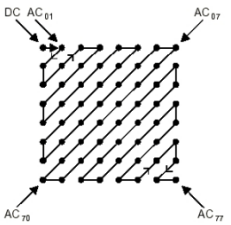
$$Q_Y = \begin{pmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 69 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 80 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 103 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{pmatrix} \quad (16)$$

$$Q_c = \begin{pmatrix} 17 & 18 & 24 & 47 & 99 & 99 & 99 & 99 \\ 18 & 21 & 26 & 66 & 99 & 99 & 99 & 99 \\ 24 & 26 & 56 & 99 & 99 & 99 & 99 & 99 \\ 47 & 66 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \end{pmatrix} \quad (17)$$

Hasil kuantisasi disimpan kembali ke dalam matriks yang diberi nama "dct_img" yang memiliki ukuran yang sama dengan gambar asli.

Selanjutnya, program mengaplikasikan teknik Run-Length Coding (RLC) untuk mengompres hasil kuantisasi dari DCT. Teknik ini mengonversi blok 8x8 hasil kuantisasi menjadi urutan zigzag.

0	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63



Gambar 3. Zigzag Scan

Setelah itu, urutan zigzag ini diproses dengan Run-Length Encoding (runlengthEncoding), yang mengompresi data dengan mencatat jumlah elemen berurutan yang sama. Hasil kompresi ini disimpan dalam vector yang diberi nama rlc_vector.

Dengan pemrosesan ini, gambar sampul telah disiapkan untuk penyisipan pesan rahasia dengan ukuran yang lebih efisien dan format yang lebih tahan terhadap gangguan. Transformasi DCT dan kuantisasi mengurangi jumlah data yang harus ditangani, sementara RLC lebih lanjut mengompres data, mempersiapkan tahap penyisipan berikutnya yang melibatkan Discrete Wavelet Transform (DWT). Proses ini memastikan bahwa data pesan rahasia dapat disisipkan dengan cara yang efisien dan aman, dengan mempertahankan kualitas visual gambar sampul.

3.3. Tahap Penyisipan Gambar

Pada tahap penyisipan dengan Discrete Wavelet Transform (DWT), program memulai dengan mengaplikasikan DWT pada gambar sampul yang telah diproses menggunakan DCT dan kuantisasi. DWT adalah teknik transformasi yang mengubah data dari domain spasial ke domain frekuensi, mirip dengan DCT, tetapi dengan menggunakan gelombang (wavelets) sebagai basis. Teknik ini efektif dalam menangkap informasi frekuensi lokal dari gambar, yang membuatnya sangat berguna untuk steganografi. Dalam implementasi ini, program menggunakan wavelet Haar, yang merupakan wavelet paling sederhana dan sering digunakan untuk pengolahan gambar.

DWT menguraikan gambar sampul menjadi empat sub-band: Approximasi (Ap), Horizontal Detail (De1), Vertikal Detail (De2), dan Diagonal Detail (De3). Sub-band Approximasi (Ap) berisi informasi frekuensi rendah dan mempertahankan sebagian besar energi gambar, sedangkan sub-band detail (De1, De2, De3) berisi informasi frekuensi tinggi yang menangkap detail-detail gambar. Setelah menguraikan gambar, program mengkuantisasi koefisien hasil DWT dengan membulatkannya.

Koefisien Approximasi (Ap_co1) kemudian dipecah menjadi blok-blok kecil untuk proses penyisipan. Proses pemecahan dilakukan dengan membagi koefisien tersebut menjadi sejumlah bagian kecil yang lebih mudah untuk disisipkan pesan rahasia. Ukuran blok yang digunakan adalah 16x16 piksel, dan koefisien ini diubah menjadi blok-blok matriks kecil, yaitu memecah matriks besar menjadi beberapa matriks kecil sesuai dengan ukuran yang diinginkan. Pemecahan ini menghasilkan matriks sel (`output`) yang berisi blok-blok koefisien yang siap untuk disisipi pesan.

Pesan rahasia yang telah diubah menjadi vektor satu dimensi pada tahap sebelumnya kemudian diembed ke dalam blok-blok koefisien DWT ini. Penyisipan dilakukan dengan mengubah nilai bit terkecil (*Least significant bit*, LSB) dari setiap elemen dalam blok koefisien sesuai dengan nilai bit dari pesan rahasia. Proses ini dikenal sebagai LSB modification, yang merupakan teknik steganografi dasar namun efektif. Program menghitung LSB dari setiap elemen koefisien dan melakukan operasi XOR dengan nilai bit pesan rahasia untuk menentukan perubahan yang diperlukan. Nilai koefisien kemudian diubah sesuai dengan hasil operasi ini.

Setelah penyisipan selesai, blok-blok koefisien yang telah disisipi pesan disusun kembali menjadi matriks besar. Matriks ini kemudian diolah lebih lanjut dengan *inverse* DWT (IDWT) untuk merekonstruksi gambar stego. IDWT menggabungkan kembali sub-band Approximasi dan Detail menjadi satu gambar utuh, menghasilkan gambar stego yang tampak serupa dengan gambar sampul asli tetapi telah menyisipkan pesan rahasia. Gambar stego ini kemudian ditampilkan untuk verifikasi visual dan disimpan untuk proses selanjutnya.

Penyisipan dengan DWT memastikan bahwa pesan rahasia disisipkan dalam komponen frekuensi rendah dan tinggi dari gambar, membuat pesan lebih tersembunyi dan lebih

tahan terhadap berbagai jenis serangan atau kompresi. Teknik ini mengambil keuntungan dari sifat lokal dari wavelet, memungkinkan penyisipan yang lebih efisien dan aman. Proses ini menjaga kualitas visual gambar stego sambil memastikan bahwa pesan rahasia dapat disisipkan dan diekstraksi dengan andal.

3.4. Tahap Rekonstruksi Gambar Stego

Pada tahap rekonstruksi gambar stego, program menggunakan Discrete Wavelet Transform (DWT) untuk mengekstrak pesan rahasia dan merekonstruksi gambar sampul. Gambar stego diuraikan menjadi empat sub-band: Approximasi (Ap_steg1), Horizontal Detail (De_steg1), Vertikal Detail (De_steg2), dan Diagonal Detail (De_steg3). Sub-band Approximasi kemudian dipecah menjadi blok-blok kecil untuk mengekstrak pesan rahasia dengan membaca nilai bit terkecil (LSB) dari elemen koefisiennya, yang dikonversi kembali menjadi pesan asli.

Setelah pesan rahasia diekstraksi, program menyusun kembali blok-blok koefisien Approximasi dan sub-band Detail untuk merekonstruksi gambar sampul. Proses ini melibatkan penerapan *inverse* DWT (IDWT) untuk menghasilkan gambar sampul yang mirip dengan gambar asli sebelum penyisipan. Gambar hasil rekonstruksi ditampilkan dan disimpan sebagai "Recon_image.jpg".

Program menghitung nilai *Mean Squared Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR) antara gambar asli dan hasil rekonstruksi untuk mengukur kualitas rekonstruksi. Nilai PSNR yang lebih tinggi menunjukkan kualitas rekonstruksi yang lebih baik. Selain itu, ukuran file dari gambar hasil rekonstruksi dihitung untuk memastikan efisiensi penyimpanan.

Dengan keseluruhan proses ini, program memastikan bahwa pesan rahasia dapat disisipkan dan diekstraksi dengan aman, menjaga kualitas visual dan ukuran gambar sampul, menjadikan teknik steganografi ini praktis dan efektif untuk keamanan data.

3.5. Tahap Ekstraksi Pesan Dari Gambar Stego

Pada tahap ekstraksi pesan dari gambar stego, tujuan utamanya adalah mengembalikan pesan rahasia tanpa merusak integritas gambar stego. Proses dimulai dengan menerapkan Discrete Wavelet Transform (DWT) pada gambar stego, memisahkannya menjadi empat sub-band: Approximasi (Ap_steg1), Horizontal Detail (De_steg1), Vertikal Detail (De_steg2), dan Diagonal Detail (De_steg3). Fokus utama adalah pada sub-band Approximasi, di mana sebagian besar pesan rahasia disisipkan.

Sub-band Approximasi dipecah menjadi blok-blok kecil berukuran 16x16 piksel, yang ditempatkan dalam matriks sel (`stegOut`) untuk memudahkan akses dan manipulasi. Ekstraksi pesan dilakukan dengan membaca nilai bit terkecil (LSB) dari setiap elemen dalam blok-blok koefisien Approximasi. LSB ini diubah kembali menjadi vektor bit, yang kemudian dikonversi menjadi karakter teks atau nilai numerik sesuai dengan jenis pesan rahasia.

Bit-bit yang diekstraksi diubah menjadi karakter ASCII dengan mengelompokkan setiap 8 bit menjadi satu byte. Proses ini berlanjut hingga seluruh pesan rahasia berhasil diekstraksi dan disimpan ke dalam file teks bernama "Output.txt".

Program memastikan integritas dan akurasi pesan yang diekstraksi dengan memverifikasi bit-bit yang dihasilkan. Jika ada kesalahan atau ketidaksesuaian, program memberikan peringatan atau mencoba metode koreksi kesalahan. Proses ekstraksi ini menggunakan teknik DWT dan manipulasi bit yang teliti untuk menjaga kualitas gambar stego dan memastikan pesan rahasia dapat diambil kembali dengan akurat dan utuh.

4. HASIL DAN PEMBAHASAN

1. Hasil uji pesan berisi 1000 karakter

TABEL II PENGUJIAN 1000 KARAKTER

Gambar	MSE	PSNR	SSIM
MR-1	0.026306	63.1976	0.99822

MR-2	0.030918	60.3914	0.99832
MR-3	0.03315	59.1807	0.99839
MR-4	0.029415	61.2571	0.9981
MR-5	0.039501	56.1355	0.99775
MR-6	0.039429	56.1674	0.99748
MR-7	0.026829	62.8559	0.99787
MR-8	0.037872	56.8671	0.99757
MR-9	0.031906	59.845	0.99739
MR-10	0.03941	56.1758	0.99743

2. Hasil uji pesan berisi 5000 karakter

TABEL III PENGUJIAN 5000 KARAKTER

Gambar	MSE	PSNR	SSIM
MR-1	0.026307	63.1973	0.99635
MR-2	0.030919	60.3911	0.99596
MR-3	0.03315	59.1805	0.99652
MR-4	0.029416	61.2568	0.99783
MR-5	0.039506	56.1333	0.99742
MR-6	0.039431	56.1666	0.99719
MR-7	0.026829	62.8556	0.99658
MR-8	0.037873	56.8668	0.99626
MR-9	0.031907	59.8447	0.99612
MR-10	0.03941	56.1756	0.99613

Berdasarkan hasil uji pesan yang berisi 1000 karakter dan 5000 karakter yang ditampilkan dalam Tabel 1 dan Tabel 2, terdapat beberapa parameter yang diukur yaitu *Mean Squared Error* (MSE), *Peak Signal-to-Noise Ratio* (PSNR), dan *Structural Similarity Index* (SSIM). Pada Tabel 1, untuk pesan berisi 1000 karakter, MSE terendah adalah 0.026306 pada gambar MR-1 dan tertinggi adalah 0.03941 pada gambar MR-10. PSNR tertinggi dicapai oleh gambar MR-1 dengan nilai 63.1976, sedangkan nilai terendah pada gambar MR-10 dengan 56.1758. SSIM tertinggi adalah 0.99839 pada gambar MR-3 dan terendah adalah 0.99743 pada gambar MR-10.

Pada Tabel 2, yang menguji pesan berisi 5000 karakter, MSE terendah juga ditemukan pada gambar MR-1 dengan nilai 0.026307 dan tertinggi pada gambar MR-10 dengan 0.03941. PSNR tertinggi kembali dicapai oleh gambar MR-1 dengan nilai 63.1973 dan terendah pada gambar MR-10 dengan 56.1756. SSIM tertinggi adalah 0.99787 pada gambar MR-8 dan terendah adalah 0.99566 pada gambar MR-2.

Secara keseluruhan, nilai MSE dan PSNR menunjukkan bahwa kualitas gambar setelah penyisipan pesan berkurang seiring dengan bertambahnya panjang pesan yang disisipkan. Meskipun demikian, nilai SSIM yang masih relatif tinggi menunjukkan bahwa kualitas struktur gambar tetap terjaga dengan baik meskipun ada penurunan kecil pada beberapa gambar. Perbandingan antara pesan berisi 1000 karakter dan 5000 karakter menunjukkan konsistensi dalam penurunan nilai PSNR dan SSIM, yang mengindikasikan bahwa peningkatan panjang pesan yang disisipkan cenderung menurunkan kualitas gambar secara keseluruhan.

5. Kesimpulan dan Saran

Kesimpulan dari penelitian ini menunjukkan bahwa metode penyisipan pesan rahasia ke dalam gambar menggunakan Discrete Cosine Transform (DCT) efektif dalam meningkatkan kapasitas penyisipan pesan dan juga mampu mempertahankan kualitas visual gambar. Berdasarkan hasil pengujian dengan pesan yang berisi 1000 dan 5000 karakter, terdapat beberapa parameter yang diukur yaitu *Mean Squared Error* (MSE), *Peak Signal-to-Noise Ratio* (PSNR), dan *Structural Similarity Index* (SSIM).

Untuk pesan berisi 1000 karakter, nilai MSE terendah adalah 0.026306 pada gambar MR-1 dan tertinggi adalah 0.03941 pada gambar MR-10. Nilai PSNR tertinggi dicapai oleh gambar MR-1 dengan nilai 63.1976, sedangkan nilai terendah pada gambar MR-10 dengan 56.1758. SSIM tertinggi adalah 0.99839 pada gambar MR-3 dan terendah adalah 0.99743 pada gambar MR-10. Sementara itu, untuk pesan berisi 5000 karakter, nilai MSE terendah adalah 0.026307 pada gambar MR-1 dan tertinggi pada gambar MR-10 dengan 0.03941. PSNR tertinggi kembali dicapai oleh gambar MR-1 dengan nilai 63.1973 dan terendah pada gambar MR-10 dengan 56.1756. SSIM tertinggi adalah 0.99787 pada gambar MR-8 dan terendah adalah 0.99566 pada gambar MR-2.

Secara keseluruhan, peningkatan panjang pesan yang disisipkan cenderung menurunkan kualitas gambar, yang tercermin dari peningkatan nilai MSE dan penurunan nilai PSNR serta SSIM. Meskipun demikian, nilai SSIM yang masih relatif tinggi menunjukkan bahwa struktur gambar tetap terjaga dengan baik meskipun ada sedikit penurunan kualitas pada beberapa gambar. Peningkatan nilai MSE dan penurunan nilai PSNR dan SSIM secara konsisten menunjukkan bahwa panjang pesan yang lebih besar mempengaruhi kualitas gambar secara keseluruhan, namun metode ini tetap efektif meskipun mengalami peningkatan nilai MSE dan penurunan pada nilai PSNR dan SSIM namun hasil menunjukan perubahan nilai yang tidak terlalu signifikan, dengan demikian maka penelitian ini berhasil meningkatkan kapasitas penyisipan pesan namun tetap mempertahankan *imperceptibility* dengan baik.

Saran untuk penelitian selanjutnya diharapkan untuk menggunakan metode yang lebih efektif dari metode yang digunakan pada penelitian ini.

Daftar Pustaka:

[1] Y. W, R. Anto, D. Teguh Yuwono, and Y. Yuliadi, "Deteksi Serangan Vulnerability Pada Open Jurnal System Menggunakan Metode Black-Box," *J. Inform. dan Rekayasa Elektron.*, vol. 4, no. 1, pp. 68–77, 2021, doi: 10.36595/jire.v4i1.365.

[2] P. Prajapati, P. Kumar MTech Scholar, and V. Kumar Sharma Asst, "Information Security Based on Steganography & Cryptography Techniques: A Review," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 10, p. 2277, 2014, [Online]. Available: https://www.researchgate.net/publication/268388237

[3] Abdul Halim Hasugian, Yusuf Ramadhan Nasution, and N. A. Simanjuntak, "Kombinasi Algoritma Beaufort Cipher Dan Lsb2Bit Untuk Keamanan File Teks," *J. Inform. dan Rekayasa Elektron.*, vol. 6, no. 1, pp. 28–36, 2023, doi: 10.36595/jire.v6i1.730.

[4] S. Rustad, D. R. I. M. Setiadi, A. Syukur, and P. N. Andono, "*Inverted* LSB image steganography using adaptive pattern to improve imperceptibility," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 6, pp. 3559–3568, 2022, doi: 10.1016/j.jksuci.2020.12.017.

[5] A. K. Singh, "Steganography in Digital Images Using LSB Technique," *J. Xidian Univ.*, vol. 14, no. 5, 2020, doi: 10.37896/jxu14.5/506.

[6] A. Yahya, *Steganography techniques for digital images*. 2018. doi: 10.1007/978-3-319-78597-4.

[7] A. Ansor, "Penerapan Steganografi Video Dengan Metode Discrete Cosine Transform," *MEANS (Media Inf. Anal. dan Sist.*, vol. 1, no. 2, pp. 25–32, 2016.

[8] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 3, pp. 1168–1175, 2019, doi: 10.12928/TELKOMNIKA.V17I3.12230.

[9] O. O. Evsutin and A. O. Osipov, "The algorithm of the high-capacity information embedding into the digital images DCT domain using differential evolution," *CEUR Workshop Proc.*, vol. 1901, pp. 55–64, 2017, doi: 10.18287/1613-0073-2017-1901-55-64.

[10] N. Kaur and S. K. Ranade, "High Capacity Data Embedding System in DCT domain for Colored Images," vol. 3, no. 3, 2012.

[11] K. Rabah, "Steganography-The Art of Hiding Data," *Information Technology Journal*, vol. 3, no. 3. pp. 245–269, 2004. doi: 10.3923/itj.2004.245.269.

[12] S. Atawneh, A. Almomani, and P. Sumari, "Steganography in digital images: Common approaches and tools," *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)*, vol. 30, no. 4, pp. 344–358, 2013, doi: 10.4103/0256-

4602.116724.

[13] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[14] S. A. Jebur, A. K. Nawar, L. E. Kadhim, and M. M. Jahefer, "Hiding Information in Digital Images Using LSB Steganography Technique," *Int. J. Interact. Mob. Technol.*, vol. 17, no. 7, pp. 167–178, 2023, doi: 10.3991/ijim.v17i07.38737.

[15] M. A. Joshi, M. S. Raval, Y. H. Dandawate, K. R. Joshi, and S. P. Metkar, "Introduction to Image Compression," *Image and Video Compression*, pp. 18–21, 2014, doi: 10.1201/b17738-4.

[16] D. Bansal and R. Chhikara, "An Improved DCT based Steganography Technique," *Int. J. Comput. Appl.*, vol. 102, no. 14, pp. 46–49, 2014, doi: 10.5120/17887-8861.

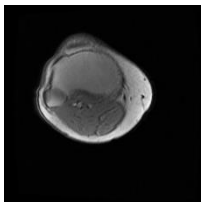
[17] C. Florea, M. Gordan, B. Orza, and A. Vlaicu, "Compressed Domain Computationally Efficient Processing Scheme for JPEG Image Filtering," *Adv. Eng. Forum*, vol. 8–9, pp. 480–489, 2013, doi: 10.4028/www.scientific.net/aef.8-9.480.

[18] S. Anwar, "Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES," *J. Format*, vol. 6, no. 1, pp. 65–74, 2017.

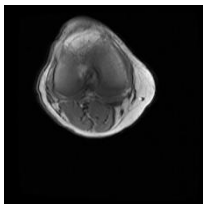
[19] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography," *Multimed. Tools Appl.*, vol. 80, no. 6, pp. 8423–8444, 2021, doi: 10.1007/s11042-020-10035-z.

LAMPIRAN

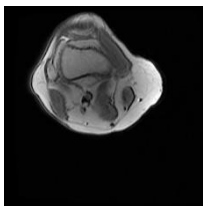
3. MR-1



4. MR-2

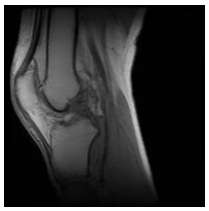


5. MR-3



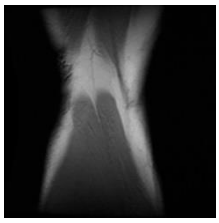
6. MR-4

7. MR-5



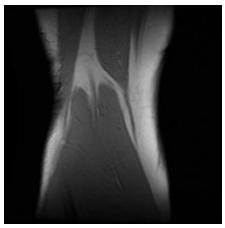
8. MR-6

9. MR-7



10. MR-8

11. MR-9



12. MR-10