BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

Terdapat beberapa tinjauan pustaka penelitian-penelitian sebelumnya yang menjadi referensi penulis. Dimana tinjauan pustaka ini berkaitan dengan sistem pengamanan data dengan menggunakan steganografi. Berikut ini penjelasan mengenai penelitian-penelitian terdahulu yang dapat dilihat pada Tabel 2.1 yang dijadikan referensi untuk membantu pada penelitian ini.

Pada penelitian Sari (2012) menggunakan *Least Significant Bit* (LSB) dan *Advanced Encryption Standard* (AES), menghasilkan citra dari file PNG dengan kualitas citra baik dan dapat dilakukan *recovery* dari hasil pengolahan citra tersebut untuk membaca kembali isi pesan. Pada penelitian Faruqi dan Rozi (2015) menggunakan algoritma steganografi *Dicrete Cosine Transform* (DCT), menghasilkan nilai rata-rata PSNR sebesar 37.44 dB dan gambar tahan terhadap kompresi gambar. Penelitian yang dilakukan oleh Ardiansyah, dkk. (2017) menggunakan algoritma *Discrete Cosine Transform* (DCT), menghasilkan sebuah aplikasi yang dapat memproses file dan citra dengan baik, serta pesan yang dapat disisipkan dapat berupa huruf, angka dan simbol.

Penelitian yang dilakukan oleh Hamdani dan Samosir (2018) dengan menggunakan algoritma *Discrete Cosine Transform* (2018), menghasilkan nilai PSNR rata-rata di atas 40 dB dan tingkat kemiripan citra steganografi dengan citra asli terbilang baik. Pada penelitian yang dilakukan oleh Fatahillah (2019) menggunakan algoritma steganografi *Discrete Wavelet Transform* (DWT) dan *Discrete Cosine Transform* (DCT). Menghasilkan nilai rata-rata PSNR 38.3347 dB dengan nilai rata-rata korelasi NC dari *hidden image* sebesar 0.98455. Hal ini menandakan bahwa kualitas citra yang dihasilkan dari proses algoritma tersebut sudah berkualitas baik, sehingga algoritma ini aman untuk digunakan.

Pada penelitian yang dilakukan oleh Muhammad, dkk. (2019) dengan

menggunakan algoritma *Advanced Encryption Standart* (AES) dan *Discrete Cosine Transform* (DCT). Algoritma ini dapat mengubah isi pesan sebesar 50% jika kunci masukan yang digunakan dilakukan perubahan 1 bit terlebih dahulu, nilai PSNR yang dihasilkan juga lebih dari 30 dB dan nilai rata-rata BER kurang dari 0,03. Pada penelitian yang dilakukan Sari (2012) menggunakan algoritma LSB dimana metode ini menggunakan domain spasial. Domain spasial memang cukup mudah untuk diimplementasikan hanya saja data didalamnya mudah mengalami kerusakan dan tidak kokoh terhadap serangan yang dilakukan pada citra. Sedangkan penggunaan algoritma DCT pada penelitian-penelitian sebelumnya terlihat bahwa citra tersebut masih dalam keadaan baik, tidak mengalami perubahan yang cukup signifikan terlihat dari nilai PSNR yang dihasilkan. Sehingga penulis melakukan penelitian terkait pengaman data dengan menggunakan algoritma DCT.

Tabel 2.1 Tabel referensi

No.	Penulis	Metode	Hasil
1.	S. P. Sari, dkk. (2012)	Algoritma *Least Significant Bit* (LSB) dan *Advancced Encryption Standard* (AES)	Kualitas gambar yang di dihasilkan dari file PNG yang telah disisipkan memiliki kualitas yang baik dan dapat dilakukan *recovery* untuk mendapatkan data itu kembali.
2.	A. Adil Faruqi, dan Imam Fahrur Rozi (2015)	Algoritma *Discrete Cosine Transform* (DCT)	Menghasilkan nilai rata-rata PSNR sebesar 37.44 dB dan gambar tahan terhadap kompresi pada gambar.

No.	Penulis	Metode	Hasil
3.	H. Ardiansyah, dkk. (2017)	Algoritma *Discrete Cosine Transform* (DCT)	Menghasilkan sebuah aplikasi yang dapat memproses file dan citra dengan baik, serta pesan yang dapat disisipkan dapat berupa huruf, angka dan simbol.
4.	M. Hamdani dan G. N. Samosir (2018)	Algoritma *Discrete Cosine Transform* (DCT)	Menghasilkan nilai PSNR rata-rata diatas 40 dB dan tingkat kemiripan citra asli dengan citra hasil ektraksi masih dalam kondisi baik
5.	S. R. Muhamad Fatahillah, dan Ema Utami (2019)	Algoritma *Discrete Wavelet Transform* (DWT) dan *Discrete Cosine Transform* (DCT)	Menghasilkan nilai rata-rata PSNR 38.3347 dB dengan nilai rata-rata korelasi NC dari *hidden image* sebesar 0.98455 yang berarti bahwa kualitas citra yang dihasilkan berkualitas baik.
6.	R. Muhammad, dkk. (2019)	Algoritma *Data Encryption Standard* (DES) dan *Discrete Cosine Transform* (DCT)	Algoritma ini dapat mengubah isi pesan sebesar 50% jika kunci masukan diubah 1-bit, nilai PSNR yang dihasilkan lebih dari 30 dB dan nilai rata-rata BER kurang dari 0.03.

Pada penelitian ini menggunakan beberapa landasan teori, dimana konsep utama yang digunakan adalah steganografi. Steganografi digunakan untuk menyembunyikan pesan dengan menggunakan dua rumus DCT.

2.2 Steganografi

2.2.1 Pengertian Steganografi

Steganografi berasal dari bahasa Yunani (*steganos* = tersembunyi, dan *graphien* = tulisan) yang berarti "tulisan tersembunyi". Steganografi adalah suatu ilmu yang digunakan untuk penyembunyian pesan rahasia ke dalam citra digital menggunakan suatu metode sehingga pesan tersebut tidak dapat terdeteksi keberadaannya oleh indra manusia.

2.2.2 Sejarah Steganografi

Sekitar 4000 tahun yang lalu di kota Menet Khufu, Mesir steganografi sudah ada dan dikenali di kota tersebut. Diawali dengan penulisan karakter dengan bentuk gambar yang disebut dengan *hieroglyphic*. Yang diawali dengan penggunaan tulisan Mesir kuno untuk menceritakan kehidupan majikannya, dimana hal ini dijadikan landasan ide untuk dapat membuat pesan rahasia.

Oleh sebab itu, penggunaan tulisan Mesir kuno ini dianggap sebagai steganografi pertama kali di dunia. Tidak hanya bangsa Mesir saja, bangsa-bangsa lain juga telah menggunakan teknik steganografi pada masa lalu, yaitu [1]:

1. Penggunaan tinta tak tampak (*invisible ink*) yang digunakan oleh bangsa Romawi pada Perang Dunia II. Tinta ini dibuat dari campuran getah tanaman *thithymallus*, susu, sari buah, cuka dan urine. Pliny the Elder menjelaskan bahwa bila tinta tersebut digoreskan ke atas kertas maka tulisan tersebut tidak kelihatan. Untuk membacanya kembali dengan cara memanaskan kertas tersebut, sehingga tulisan tinta tak tampak berubah menjadi gelap/cokelat.
2. Pada tahun 440 BC yang dilakukan oleh sejarawan Yunani steganografi dengan menggunakan media kepala budak yang dijelaskan pada buku "*Histories of Herodatus*", ditulis oleh Herodatus (485 – 525 BC). Buku ini menceritakan kisah perang antara kerajaan Persia dan rakyat Yunani. Dimana Histaiaeus ingin mengirimkan pesan kepada Aristagoras of Miletus untuk melawan Persia. Yang dilakukan dengan cara memilih beberapa budak untuk dibotaki kepalanya, lalu pesan dituliskan dengan cara tato, hingga rambut budak dibiarkan tumbuh kembali, barulah budak

dikirim ke tempat penerima pesan. Untuk membaca isi pesan kembali kepala budak digunduli agar pesan dapat terlihat.

3. Teknik yang digunakan masyarakat Yunani kuno adalah penulisan pesan rahasia di atas kayu yang ditutupi oleh lilin (*wax*). Di dalam buku Heradatus, Demaratus memberikan peringatan mengenai serangan yang akan datang ke Yunani menggunakan tablet kayu yang dilapisi lilin dari lebah. Untuk bisa membacanya, penerima pesan harus memanaskan lilin terlebih dahulu.
4. Masyarakat Cina kunoa menggunakan kain sutra dan lilin. Yang dilakukan dengan cara menulisnya pada potongan-potongan kecil kain sutra yang digumpalkan menjadi bola kecil, kemudian dilapisi lilin. Untuk membawa pesan tersebut, dengan menelan bola kecil itu, kemudian dikeluarkan kembali dari perut pembawa pesan untuk dapat dibaca.
5. Penyembunyian pesan di dalam telur rebus. Giovanni Battista Porta menjelaskan cara penyembunyian pesan dengan menuliskannya pada kulit telur menggunakan tinta yang terbuat dari satu ons tawas dan setengah liter cuka. Tulisan tersebut tidak dapat diketahui keberadaannya dikarenakan tinta menembus kulit telur dan akan membekas pada permukaan isi telur yang sudah direbus terlebih dahulu. Untuk membaca isi pesan dibaca dengan cara mengupas kulit telur.

Pada 11 September 2001 ilmu steganografi mendadak naik daun, dimana *Al-Qaidah* dituding menggunakan steganografi untuk menyisipkan pesan rahasia melalui video atau gambar yang dirilis melalui internet oleh pihak FBI.

2.2.3 Proses Steganografi

Sebuah citra digital pada dasarnya didapatkan dari proses *sampling* dan kuantisasi dari citra analog. *Sampling* merupakan proses pembagian citra ke dalam elemen-elemen diskrit (piksel). Sedangkan kuantisasi merupakan proses pemberian nilai intensitas warna pada setiap piksel dengan nilai berupa bilangan bulat. Pada tahap ini dilakukan proses pembuangan informasi yang kurang penting (tidak mempengaruhi secara signifikan). Citra tersebut adalah citra biner (1 bit), citra *grayscale* (8 bit) dan citra berwarna (24 bit) [5]. Terdapat beberapa jenis gambar yang dapat dilakukan penyisipan pesan dalam proses steganografi yaitu sebagai

berikut:

a. JPG/JPEG (*Joint Photographic Experts Assemble*)

b. GIF (*Graphics Interchange Format*)

c. PNG (*Portable Network Graphics*)

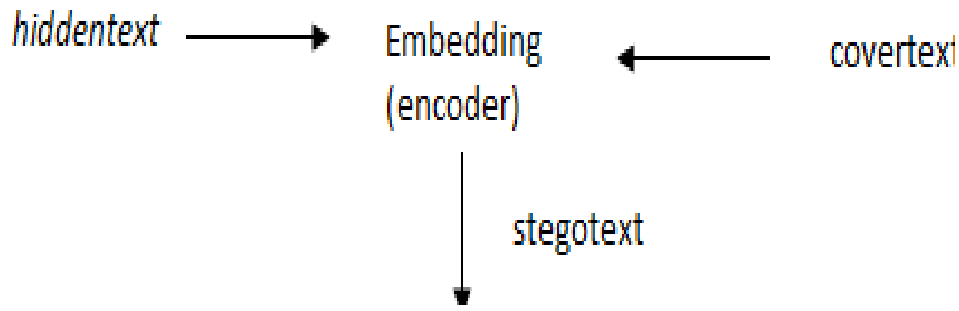
d. BMP (Bitmap)

e. TIFF (*Tagged Image Format File*)

Secara umum, steganografi terdiri atas dua proses yaitu:

a. Proses Penyembunyian Data *(Embedding)*

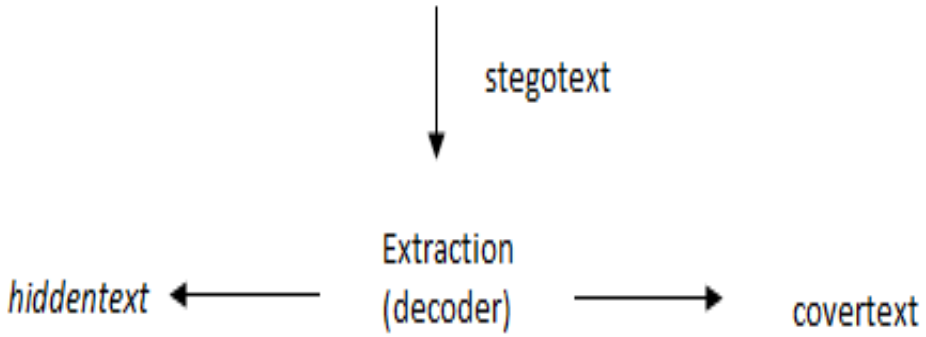
Proses penyembunyian data dilakukan dengan mengubah bit-bit data pada citra dengan bit-bit data rahasia yang akan disembunyikan. Agar data yang disembunyikan lebih aman, maka penyembunyiannya dilakukan dengan mengganti bit-bit data rahasia dengan susunan *byte* secara acak. Sehingga akan didapatkan citra yang sudah berisikan pesan di dalamnya (stegotext). Besarnya ukuran *hiddentext* yang dapat disembunyikan bergantung dari ukuran *covertext* yang digunakan. Prosesnya dapat dilihat pada Gambar 2.1 berikut ini.



Gambar 2.1 Proses Penyembunyian Data

b. Proses Pengungkapan Data *(Extraction)*

Proses pengungkapan data (*extraction*) dilakukan dengan membangkitkan bilangan acak untuk mengetahui posisi *byte* yang menyimpan bit data. Nilai bilangan acak yang diperoleh harus sama dengan nilai yang digunakan pada waktu penyembunyian data. Sehingga akan didapatkan bit data rahasia yang ada pada *stegotext*. Prosesnya dapat dilihat pada Gambar 2.2 berikut.



Gambar 2.2 Proses Pengungkapan Data

Dari kedua proses di atas dapat dijelaskan terminologi yang umum digunakan dalam steganografi antara lain:

- *Hiddentext* (*embedded message*) : pesan rahasia yang akan diamankan dengan menyembunyikannya ke dalam *covertext*.
- *Covertext* (*cover-object*) : gambar digital yang akan digunakan sebagai media penampung pesan rahasia.
- *Stego image (stego-object)* : gambar yang sudah berisikan pesan rahasia didalamnya (*hiddentext*).

Kualitas citra yang dihasilkan dapat berubah dikarenakan penyembunyian data rahasia ke dalam citra digital tersebut. Oleh karena itu, ada beberapa kriteria yang perlu diperhatikan dalam menyembunyikan data rahasia ke dalam citra digital tersebut adalah sebagai berikut [1]:

1. *Imperceptibility*

   Imperceptibility adalah kriteria dimana pesan rahasia tidak dapat dipersepsi keberadaannya baik secara visual maupun audio oleh pihak lain yang tidak berhak.

2. *Fidelity*

   Fidelity adalah kriteria dimana kualitas citra penampung masih terlihat baik kualitasnya. Yang diukur dengan melakukan perhitungan dari MSE (*Mean Square Error*) dan PSNR (*Peak Signal to Noise Ratio*), hasilnya dapat kita melihat apakah kualitas citra masih dalam keadaan baik atau tidak [4].

3. *Recovery*

   Recovery adalah kriteria dimana data rahasia yang telah disembunyikan ke dalam citra dapat diekstraksi kembali untuk dipahami dan dibaca isinya.

4. *Capacity*

   Capacity adalah kriteria dimana ukuran pesan yang dapat disembunyikan pada citra sebisa mungkin berukuran besar.

Terdapat tiga aspek dalam steganografi yang dapat menentukan tingkat keberhasilan dari proses yang telah dilakukan (Ermadi, dkk, 2004) yaitu sebagai berikut:

1. *Capacity*

   Aspek mengenai kapasitas pesan yang dapat disembunyikan di dalam citra *cover* sebisa mungkin berukuran besar.

2. *Security*

   Aspek keamanan sistem steganografi perlu diperhatikan dan benar-benar harus aman dari pihak tiga.

3. *Robustness*

   Aspek mengenai tingkat ketahanan citra hasil steganografi terhadap manipulasi citra seperti *resize* dan rotasi [4].

2.2.4 Teknik Dasar Steganografi

Steganografi memiliki enam buah teknik dasar yang biasa digunakan yaitu sebagai berikut [1]:

1. Teknik substitusi

   Teknik substitusi adalah dengan memasukkan bit pesan rahasia ke dalam citra digital. Adapun metode steganografi yang menggunakan teknik substitusi adalah modifikasi LSB.

2. Teknik transformasi domain

   Teknik transformasi domain menyisipkan pesan rahasia di dalam *transform space* dari sinyal.

3. Teknik s*pread spectrum*

   Tedapat dua metode yang berbeda, yaitu pertama dengan mentransmisikan pesan rahasia menjadi beberapa bagian kecil dan pada setiap bagiannya

disebar di seluruh spektrum frekuensi yang tersedia. Kedua dengan membagi spektrum *badwidth* yang sengaja disebarkan ke banyak frekuensi *broadcast*.

4. Teknik statistik

   Teknik ini dengan melakukan perubahan beberapa properti statistik dari citra untuk bisa disisipkan pesan rahasia ke dalamnya dan pada proses ekstraksi pesan menggunakan metode uji hipotesis.

5. Teknik distorsi

   Teknik ini melakukan penyimpanan pesan rahasia dengan distorsi sinyal dan melakukan perubahan pada citra yang digunakan.

6. Teknik c*over generation*

   Teknik ini cukup unik dimana teknik penyembunyian pesan rahasia tidak menggunakan citra *cover* sembarang yang akan digunakan, tetapi dengan mencari citra *cover* yang sesuai untuk pesan rahasia tersebut.

2.2.5 Transformasi Discrete Cosine Transformation (DCT)

Persamaan DCT satu dimensi dengan citra berukuran 1xN didefinisikan pada persamaan berikut [10]:

$$DCT(i) = \frac{2}{N} C(i) \sum_{x=0}^{N-1} f(x) cos \frac{(2x+1)i\pi}{2N}, \qquad 0 \leq i \leq N\text{-}1 \quad \text{.....(2.1)}$$

Keterangan:

DCT(i): hasil transformasi DCT pada indeks ke i

f(x) : nilai piksel pada indeks ke x

N : banyaknya mat

Himpunan hasil C(i) dengan nilai sebagai berikut [10]:

$$C(i) = \begin{cases} \frac{1}{\sqrt{2}}, & i = 0 \\ 1, & 1 \leq i \leq N-1 \end{cases}$$

Sedangkan rumus untuk mengubah nilai hasil transformasi DCT yang telah didapatkan ke nilai awal yang disebut dengan *invers* DCT (IDCT). Yang didefinisikan dengan persamaan sebagai berikut [10]:

$f(x) = \frac{2}{N}\sum_{i=0}^{N-1} C(i)DCT(i)\ cos\frac{(2x+1)i\pi}{2N}$, $\quad 0 \leq i \leq N\text{-}1$ .....(2.2)

Akan diilustrasikan DCT 1 dimensi dengan matriks [10 15 24 14 35 16 27 48]. Yang dihitung menggunakan persamaan (2.1) dengan nilai yang diketahui [10]:

i = 1, 2, 3, 4;

x = 0, 1, 2, 3;

N = 8;

f(x) = 10, 15, 24, 14, 35, 16, 27, 48;

C(i) = 1 jika i > 0,

C(i) = $\frac{1}{\sqrt{2}}$ jika i = 0.

Setelah melakukan perhitungan maka hasil transformasinya adalah seperti pada table 2.2 [10]. Dari data DCT yang didapatkan bila dikembalikan seperti semula menggunakan fungsi *invers* DCT (IDCT) dengan persamaan 2.2 maka akan didapatkan hasil yang sama dengan aslinya yaitu [1 2 3 4 5 6 7 8].

Tabel 2.2 Perhitungan DCT 1 dimensi

Nilai i	DCT (i)
1	66.8216
2	-23.4499
3	4.5401
4	-12.7170
5	8.8388
6	-12.6212
7	0.7982
8	13.2508

Rumus transformasi DCT dua dimensi dinyatakan dengan persamaan berikut ini [10]:

$$DCT(i,j) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}C(i)C(j)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)cos\frac{(2x+1)i\pi}{2M}cos\frac{(2y+1)j\pi}{2N} \quad ....(2.3)$$

Keterangan :

DCT(i,j) : hasil transformasi DCT 2 dimensi indeks ke (i, j)

M, N : banyaknya kolom dan baris

C(i) dan C(j) : himpunan hasil

f(x,y) : nilai *pixel* pada indeks ke (x,y)

Dengan nilai C(i) dan C(j) adalah sebagai berikut [10]:

$$C(i,j) = \begin{cases} \frac{1}{\sqrt{2}}, & i,j = 0 \\ 1, & i,j > 0 \end{cases}$$

Sedangkan persamaan untuk invers DCT (IDCT) sebagai berikut [10]:

$$f(x,y) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}C(i)C(j)DCT(i,j)cos\frac{(2x+1)i\pi}{2M}cos\frac{(2y+1)j\pi}{2N} \quad ....(2.4)$$

Berikut ini ilustrasi untuk DCT dua dimensi dengan matriks berukuran 3x3 sebagai berikut [10]:

$$\begin{bmatrix} 10 & 15 & 9 \\ 11 & 8 & 27 \\ 34 & 12 & 6 \end{bmatrix}$$

Untuk menghitungnya DCT 2 dimensi menggunakan persamaan 2.3 dan invers DCT menggunakan persamaan 2.4 dengan [10]:

i = 1, 2, 3; j = 1, 2, 3; x = 0, 1, 2; y = 0, 1, 2

f(x,y) = 10, 15, 9, 11, 8, 27, 34, 12, 6,

N = 3; M = 3

C(i), C(j) = $\frac{1}{\sqrt{2}}$, jika i,j = 0; C(i), C(j) = 1, jika i,j > 0

Untuk hasil perhitungan DCT dari nilai matriks yang diketahui maka akan didapatkan nilai DCT seperti pada Tabel 2.3 [12]

Tabel 2.3 Perhitungan DCT 2 dimensi

Nilai (i, j)	DCT(i, j)
(1,1)	44
(1,2)	5.3072
(1,3)	6.3640
(2,1)	-7.3485
(2,2)	-13.5
(2,3)	-7.7942
(3,1)	-1.4142
(3,2)	17.6092
(3,3)	-6.5

2.2.6 Discrete Cosine Transformation (DCT)

Discrete cosine transformation secara signifikan dapat digunakan untuk mengurangi ruang yang ada pada gambar dengan tetap menjaga kualitas gambar yang ada [8]. *Discrete Cosine Transformation* (DCT) atau Transformasi Cosinus Diskrit merupakan salah satu jenis dari transformasi *fourier* pada fungsi diskrit.

DCT bekerja dengan mengubah sinyal atau gambar dan mentransformasikannya dari domain waktu/spasial ke domain frekuensi [9]. Frekuensi DCT yang rendah berada pada kiri atas dari matriks DCT, dan frekuensi DCT yang tinggi berada pada kanan bawah dari matriks DCT. Sistem penglihatan manusia tidak begitu sensitif dengan error-error yang berada pada frekuensi tinggi dibandingkan dengan frekuensi rendah. Oleh karena itu frekuensi yang lebih tinggi dapat dikuantisasi (Faruqi & Rozi, 2015).

Gambar 2.3 Distribusi frekuensi pada blok DCT
(Sumber: Faruqi & Rozi [6])

Kelebihan penggunaan algoritma DCT ini adalah tahan terhadap kompresi yang dilakukan terhadap gambar/citra yang digunakan [6]. DCT dari n bilangan real *f(n)* adalah *F(k), k=1,…,N* dengan persamaan sebagai berikut [9].

$$F(k) = \sum_{n-1}^{N} f(n)\ cos\ (2\pi nk/N), \quad \text{dengan k=1,…N}$$

Ada delapan varian DCT standar, empat yang umum digunakan diantaranya sebagai berikut [7]:

- DCT-I $X_k = \frac{1}{2}(\chi_0 + (-1)^k \chi_{N-1} + \sum_{n=1}^{N-2} \chi_n cos\left[\frac{\pi}{N-1} nk\right]$

  $k = 0, \dots, N-1.$
- DCT-II $X_k = \sum_{n=0}^{N-1} \chi_n cos\left[\frac{\pi}{N}(n+\frac{1}{2})k\right]$

  $k = 0, \dots, N-1.$
- DCT-III $X_k = \frac{1}{2}\chi_0 + \sum_{n=1}^{N-1} \chi_n cos\left[\frac{\pi}{N} n(k+\frac{1}{2})\right]$

  $k = 0, \dots, N-1.$
- DCT-IV $X_k = \sum_{n=0}^{N-1} \chi_n cos\left[\frac{\pi}{N}(n+\frac{1}{2})\left(k+\frac{1}{2}\right)\right]$

  $k = 0, \dots, N-1.$

2.2.7 Penilaian Secara Objektif

Penilaian secara objektif didasarkan pada proses perhitungan matematis yang dilandaskan pada parameter berikut ini:

2.2.7.1 Mean Square Error (MSE)

Mean Square Error (MSE) merupakan nilai error kuadrat antara citra asli dan citra rekonstruksi (citra yang sudah disisipi pesa) (Zulfikar & Harjoko, 2016). Untuk mendapatkan nilai PSNR maka perlu menghitung nilai MSE terlebih dahulu dengan persamaan sebagai berikut [4]:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(Sxy - Cxy)^2$$

Keterangan:

MSE : nilai *Mean Square Error* citra rekonstruksi

M : panjang hasil citra ektraksi (piksel)

N : lebar hasil citra ektraksi (piksel)

x dan y: koordinat titik pada citra

S : citra yang sudah disisipi pesan (*stego image*)

C : citra asli

Setelah didapatkan nilai MSE maka kita dapat melakukan perhitungan PSNR untuk mengetahui kualitas gambar yang dihasilkan.

2.2.7.2 Peak Signal to Noise Ratio (PSNR)

Peak Signal to Noise Rasio (PSNR) merupakan perbandingan antara nilai maksimum piksel citra yang diukur dengan besarnya derau (nilai kuadrat error rata-rata antara citra asli dan citra rekonstruksi atau MSE) yang berpengaruh pada citra tersebut, dengan satuan decibel (dB) (Sahata Pandapotan & Zebua, 2016).

PSNR dihitung dengan menguadratkan nilai maksimum piksel citra dibagi dengan nilai MSE yang didapatkan sebelumnya. PSNR digunakan untuk mengetahui perbandingan kualitas citra asli dengan citra rekonstruksi. PSNR dapat dihitung dengan menggunakan persamaan sebagai berikut [4]:

$$PSNR = 10 \times log_{10}\left[\frac{Max_{i^2}}{MSE}\right]$$

Keterangan:

MSE : nilai MSE

Maxi : nilai maksimum dari piksel citra

Apabila nilai MSE yang didapatkan semakin rendah maka kualitas citra yang dihasilkan akan semakin baik. Sedangkan untuk PSNR berbanding terbalik, dimana dua buah citra dikatakan memiliki tingkat kemiripan yang rendah bila nilai PSNR berada di bawah 30 dB. Suatu citra dikatakan baik bila memiliki nilai PSNR ≥ 30 dB (Patel & Dave, 2012) [4].

2.2.8 Penilaian secara Subjektif

Mean Opinion Score (MOS) merupakan penilaian subjektif berkenaan dengan nilai yang didapatkan dari hasil pengamatan responden terhadap perbandingan antara citra asli dengan citra hasil steganografi, Adapun kriteria MOS menggunakan skala seperti pada tabel 2.4 berikut ini [3]:

Tabel 2.4 Kriteria Penilaian MOS

Nilai	**Kualitas Image**
5	Sangat Baik
4	Baik
3	Cukup Baik

2	Buruk
1	Sangat Buruk

$$MOS = \sum_{i=1}^{n} \frac{\text{Opinion score ke} - \text{i}}{n}$$

Keterangan:

n : jumlah pengamat yang memberikan respon

i : *opinion score* yang diberikan

2.3 Citra Digital

Citra merupakan fungsi dua dimensi *f(x,y)* dengan x dan y sebagai koordinat dan f sebagai koordinat gabungan *(x,y)*. Citra terbentuk dari kumpulan koordinat yang mempunyai lokasi dan nilai yang disebut pixel (F.A.Hermawati, 2013).

2.3.1 Serangan / Manipulasi Citra

Serangan / manipulasi citra adalah proses yang dilakukan terhadap citra hasil dari proses enkripsi dan *embedding* (encoder). Serangan yang dilakukan pada penelitian ini adalah sebagai berikut:

a. Kompresi citra

   Kompresi citra adalah mengurangi redudansi dari data-data yang terdapat pada citra sehingga dapat disimpan atau ditransmisikan secara efisien.

b. Rotasi citra

   Rotasi citra adalah pemutaran citra atau mengubah posisi citra dengan posisi terbaru yang diinginkan.

c. Pemotongan citra atau *cropping*

   Cropping adalah proses pemotongan citra pada bagian tertentu.

d. *Brightness*

   Brightness adalah proses pengubahan tingkat kecerahan pada citra.