BAB II
LANDASAN TEORI

2.1 Kriptografi

Kriptografi yang berasal dari suatu Bahasa yaitu Bahasa Yunanim yang memiliki dua arti kata yang pertama yaitu kripto dan yang kedua graphia. Kripto sendiri memiliki arti rahasia (*secret*) dan graphia yaitu tulisan (*writing*). Kriptografi bisa diartikan yaitu "tulisan yang dirahasiakan" yang terdapat dalam kamus hacker (Ariyus, 2005),, Kriptografi juga dapat diartikan menjadi ilmu yang mempelajari suatu penulisan secara rahasia. Umumnya kriptografi memiliki arti sebagai suatu ilmu yang dapat mempelajari teknik-teknik matematika yang memiliki hubungan aspek suatu keamanan informasi yang dapat menjaga kerahasian suatu data, keabsahan data, integritas data, dan juga autentifikasi suatu data[5]. Ketika ada seseorang yang ingin bertukar pesan (contoh : surat) pada orang lain, seseorang yang ingin mengirim pesan itu tetap aman. Adapun istilah yang penting didalam kriptografi, sebagai berikut :

1. Pesan (*Chipertect* dan *Plaintext*)

   Pesan atau *message* merupakan suatu informasi yang didalam nya dapat dibaca dan dimengerti maknanya oleh penerima pesan tersebut, pesan asli dapat disebut dengan plainteks (*plaintext*) bisa disebut juga dengan pesan tak jelas sedangkan untuk pesan yang telah disandikan dapat disebut dengan chiperteks (*chipertext*).

2. Pengirim pesan dan penerima pesan

   Pesan yang dikirim yaitu sebagai komunikasi yang melibatkan pesan ditukar antara satu dengan orang lainnya. Pengirim (*Sender*) merupakan orang yang menerima suatu pesan dan penerima (*receiver*) merupakan seseorang yang menerima pesan tersebut.

3. Penyadap (*eavesdropper*)

   Seseorang yang ingin mencoba mengetahui pesan tersebut secara tersembunyi.

4. Kriptanalisis (*cryptanallysis*)

   Kriptanalis memiliki arti ilmu dan seni yang dapat memecahkan suatu chiperteks menjadi plainteks yang tidak mengetahui suatu kunci yang digunakan

didalamnya, pelakunya tersebut dapat disebut dengan kriptanalis. Kriptologi (*cryptology*) yang dapat membahas tentang studi kriptografi dan kriptanalisis.

5. Enkripsi dan Deskripsi

   Enskripsi dan Deskripsi adalah proses yang membuat sandi plainteks yang akan dijadikan cipherteksyang bisa disebut dengan enkripsi (*encryption*) atau *enciphering.* Sedangkan untuk proses mengembalikan suatu cipherteks menjadi plainteks seperti pada awalnya dapat dinamakan dengan dekripsi (*decryption*) atau *deciphering.*

6. *Chiper* dan kunci

   Algoritma kriprografi yang dapat disebut sebagai *cipher* yang didalamnya terdapat aturan *enchipering* dan *dechipering* yaitu kunci (*key*). Kunci yang bisa diterapkan yaitu *string* ataupun deretan bilangan [6].

2.2 Steganografi

Steganografi memiliki suatu arti yang didalamnya terdapat suatu seni komunikasi antara satu orang atau lebih yang dapat menyembunyikan pesan tersebut kedalam suatu objek sehingga orang lain yang tidak tergabunng dalam komunikasi tersebut tidak mengetahui maksud dari pesan yang ada di dalam objek tersebut karena merupakan rahasia. Kata Steganos itu sendiri berasal dari Bahasa yunani yaitu tertutup dan Graphia adalah menulis [6].

Steganografi yaitu digunakan untuk komunikasi anatara seseorang dengan orang lainnya yang dilakukan secara tersembunyi, yang artinya yaitu “tulisan tertutup”. Terdapat pesan yang bisa dibuka, bida dilihat tetapi tidak dapat diketahui bahwa pesan didalam pesan atau data tersebut terdapat pesan rahasia. Kata popular untuk steganografi yaitu *Hidden in Plain Sight* yang artinya orang lain dapat melihat data tersebut tetapi tidak bisa melihat ada pesan tersembunyi didalamnya, sedangkan untuk kriptografi yaitu digunakan sebagai teempat pesan acak, data atau pesan tidak bisa dibaca dan juga tidak tahu keberadaan pesang yang sering dikenal [6].

Steganografi memiliki istilah yang berasal dari Bahasa Yunani, yaitu “Steganos” yang mempunyai arti dapat membuat pesan atau data tersebut menjadi tersembunyi dan “*Graphein”* yaitu pesan atau data bisa berbentuk tulisan. Dari dua

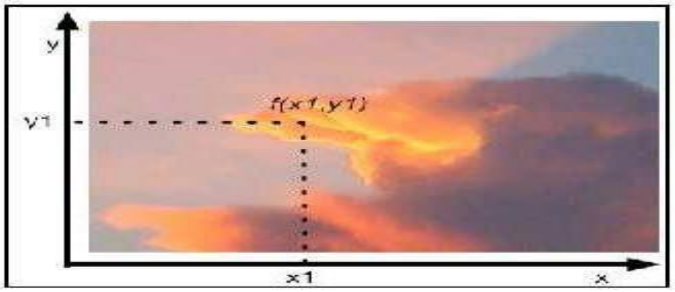
makna kata tersebut dapat diartikan yaitu suatu komunikasi yang memiliki seni yang bisa menyembunyikan pesan didalam suatu data lainnya, dan tidak mengubah tampilan data yang aslinya sehingga setelah diproses data yang asli tetap sama seperti data sebelum diproses [6].

Steganografi yaitu yang dapat menyembunyikan keberadaan suatu komunikasi dengan suatu seni dan menggunakan ilmu komunikasi supaya pesan tersebut tidak diketahui maknanya oleh orang lain, sedangkan kriptografi orang yang tidak memiliki hak untuk mengetahui makna data tersebut diperbolehkan untuk mendeteksi, menangkal ataupun memodifikasi pesan tersebut tanpa melanggar keamanan tertentu dan juga dijamin oleh *cryptosystem,* steganografi memiliki suatu tujuan yaitu menyembunyikan pesan dalam pesan yang berbahaya lainnya yang musuh tidak akan tahu bahwa data tersebut memiliki makna didalamnya. Steganografi umumnya memiliki bentuk ataupun *imperceptibility statistic* yang cukup baik dan *payload* yang bisa mencukupi sehingga steganografi dapat diterapkan [6].

2.3 Citra Digital

Citra jenis digital memiliki sebuah fungsi dua variabel yaitu f(x,y). Dimana variabel x dan y sebagai koordinat spasial dan nilai dari fungsi f(x,y) sebagai intensitas daripada citra koordinat itu sendiri,Pada hal ini bisa di ilustrasikan dalam gambar 2.1.

Pada dasarnya,Teknologi yang bisa menciptakan serta menampilkan warna pada sebuah citra digital menggunakan tiga warna dasar yang terdiri dari merah, hijau dan biru yang biasanya disingkat dengan RGB(Red ,Green, Blue) [7].



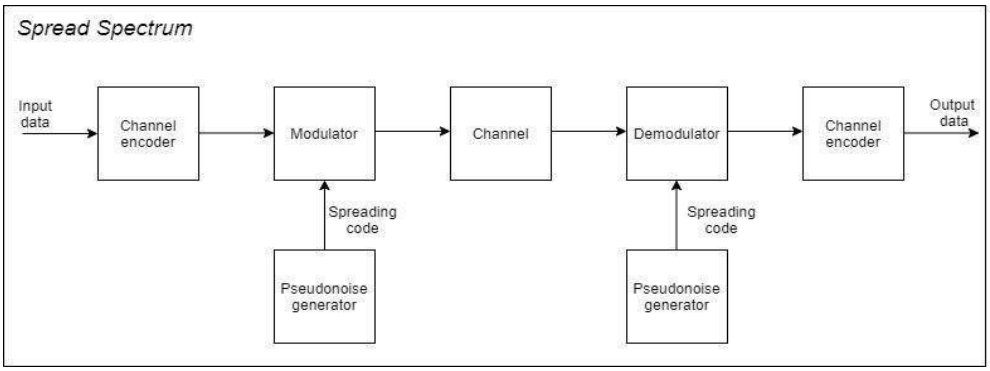
Gambar 2.1 Citra Digital [7]

2.4 MP4

MP4 adalah salah satu format file video yang lebih umum digunakan untuk mengunduh dan streaming video dari internet.File dengan ekstensi file .mp4 adalah format file video MPEG-4. Ini adalah format video yang sangat fleksibel dan terkompresi yang juga dapat menyimpan audio, terjemahan, dan gambar foto [6].

2.5 Spread Spectrum

Spread Spectrum (SS) merupakan sebuah teknik transmisi yang dimana kode *pseudonoise* dan *independent* dari suatu data informasi yang dapat digunakan untuk gelombang modulasi untuk "menyebarkan" energi sinyal yang dapat melalui sebuah *bandwith* yang jauh lebih besar daripada *bandwith* sinyal informasi nya. Pada penerima sinyal dapat dikumpulkan menggunakan replica kode *pseudonoise* yang telah disinkronisasikan [4].



Gambar 2.2 Konsep Spread Spectrum [8]

Pada gambar 2.2 menggambarkan tentang karakteristik suatu kunci beberapa sistem spektrum penyebaran.Input data dimasukan ke suatu *channel encoder* yaitu suatu pengkodean saluran untuk menghilangkan digit biner yang berlebihan dari suatu sinyal digital. Kemudian di modulasikan menggunakan deretan digit-digit yang tidak beraturan disebut juga dengan *pseudonoise sequence.* Yang terjadi pada saat modulasi efeknya yaitu meningkatkan secara signifikan *bandwith* (yang menyebarkan spektrum tersebut) suatu sinyal yang akan ditransmisikan. Untuk ujung penerima, deretan digit yang sama digunakan untuk memodulasikan sinyal spektrum penyebaran, kemudian sinyal dimasukkan ke dalam suatu channel decoder yang digunakan untuk melindungi data [8].

Spread Spectrum memanfaatkan domain frekuensi, yang melakukan proses modulasi yang dilakukan dengan cara yang setiap bit nya diwakili oleh berbagai bit

yang menggunakan *spreading code* yang bisa disebarkan pada frekuensi yang lebih luas [5]. Adapun proses *spread spectrum* sebagai berikut :

1. Sebelum melakukan proses *pseudonoise,* nilai yang ada pada gambar diubah terlebih dahulu kedalam bentuk biner.
2. Melakukan proses *spread* yaitu setiap nilai biner pada baris pertama dengan kolom pertama ditambah dengan baris pertama dengan kolom kedua kemudian hasilnya ditambahkan pada baris pertama kolom ketiga dan seterusnya sampai biner pada baris terakhir dan kolom terakhir dan menghasilkan biner baru.
3. Untuk langkah selanjutnya dilakukan proses *pseudonoise* yaitu dengan melakukan perhitungan bilangan acak pada persamaan (1) yang sesuai dengan rumus LCG (*Linear Congruential Generator*) pembangkitan bilangan acak yaitu:

   $X_{n+1} = (a.X_n + B) \bmod C$ (1)

   Dengan :

   X_n = bilangan bulat ke n;

   a= untuk faktor pengali;

   B = bilangan prima dari faktor pengali;

   C = jumlah citra;
4. Setelah dilakukan proses *pseudonoise* yaitu melakukan proses modulasi dengan cara XOR hasil dari proses LCG bentuk biner di XOR dengan biner gambar yang digunakan.
5. Setelah semua proses sudah dilakukan maka selanjutnya penyisipan gambar ke dalam video yang akan digunakan [9].

2.6 Implementasi SS Pada *Watermarking*

Spread spectrum memiliki proses penyisipan yaitu dibagi menjadi tiga, yang pertama akan dilakukan proses spreading selanjutnya dilakukan proses modulasi yaitu proses pengacakan yang akan disebar dengan bilangan pseudonoise dan untuk bilangan yang terakhir yaitu pseudonoise, sedangkan untuk proses penyisipan ktu sendiri dibagi menjadi tiga proses, yang pertama penentuan wilayah penyisipan, kemudian menambahkan suatu informasi, yang terakhir menyisipkan pesan pada matriks frekuensi [8]. Metode SS yaitu metode yang lebih robust pada gangguan noise yang ada didalam citra atau serangan noise seperti kompresi, cropping dan

low pass filtering [4]. Adapun perbandingan pada tabel 2.1 metode SS dengan metode lainnya [10]:

Tabel 2.1 Perbandingan metode SS dengan metode lainnya

Kategori	LSB	*Patchwork*	*Spread Spectrum*
Dapat terlihat dengan kasat mata manusia (*invisibility*)	Sedang	Tinggi	Tinggi
Kemampuan untuk menampung banyak pesan	Sedang	Rendah	Sedang
Ketahanan terhadap serangan	Rendah	Tinggi	Tinggi
Ketidakbergantungan pada format file yang digunakan	Rendah	Tinggi	Tinggi
Tidak adanya perubahan dalam file	Rendah	Tinggi	Tinggi

2.7 Discret Wavelet Transform (DWT)

Discerete Wavelet Transform (DWT) untuk proses transformasi wavelet ini pertama kali dapat diwakili dengan proses yang melewatkan sinyal asli kedalam *low pass filter* (LPF) dan *high pass filter* (HPF). Setelah itu, untuk nilai skala dari *wavelet* dapat diubah menggunakan proses *up sampling* dan *down sampling* [11]. DWT dapat menggambarkan sebuah skala waktu sinyal digital yang didapatkan dengan menggunakan filterisasi digital, yaitu proses yang melewatkan sebuah sinyal yang akan dianalisis pada suatu *filter* dengan adanya frekuensi dan skala tertentu yang berbeda [12].

Transformasi diskrit menggunakan dua komponen yang penting dalam melakukan transformasi, yaitu :

1. Fungsi Skala (*scalling function*) : Disebut juga dengan *low pass filter* yang dapat mengambil citra dengan sebuah gradiasi intensitas yang halus dan perbedaan intensitas yang tinggi dapat dikurangi atau dibuang.

2. Fungsi *Wavelet* (*wavelet function*) : Disebut juga dengan *high pass filter* yang dapat mengambil citra dengan gradiasi intensitas yang tinggi dan perbedaan intensitas yang rendah dapat dikurangi atau dibuang. DWT adalah pentransformasian sinyal diskrit yang menjadi koefisien-koefisien *Wavelet* yang diperoleh dengan cara menapis sinyal yang menggunakan dua buah tapis yang berlawanan. Kedua tapis yang dimaksud yaitu :

- Tapis penyekala atau dapat disebut dengan tapis lolos rendah (*low pass filter*)
- Tapis detail atau dapat disebut dengan tapis lolos tinggi (*high pass filter*)

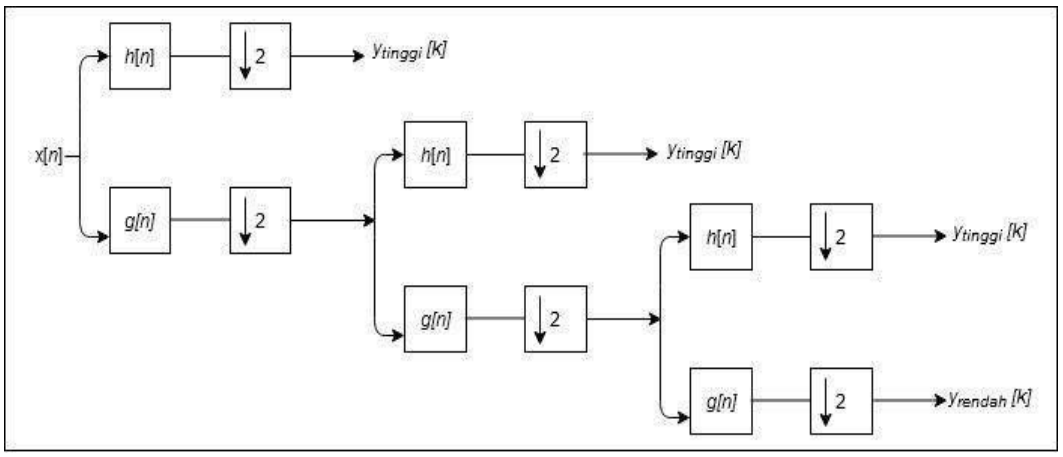
Metode Transformasi *Wavelet* Diskrit dapat menghasilkan rekontruksi sinyal yang sempurna sehingga dapat meningkatkan ketahanan (*robutness*) [13].

Metode DWT untuk matlab terdapat *library* pada matlab dapat dilihat pada link Image Watermarking using DWT - File Exchange - MATLAB Central (mathworks.com), untuk rumus umumnya pada proses dekomposisi yang dapat melalui satu atau lebih tingkatan. Untuk dekomposisi satu tingkat itu sendiri dapat ditulis dengan tingkat persamaan sebagai berikut :

$$\square_{\square\square\square\square\square\square} = \sum_{\square} \square[\square] h[2\square - \square] \quad (2)$$

$$\square_{\square\square\square\square\square h} = \sum_{\square} \square[\square] \square[2\square - \square] \quad (3)$$

untuk $y_{tinggi}[k]$ dan $y_{rendah}[k]$ merupakan dari sebuah hasil *high pass filter* dan *low pass filter*, kemudian $x[n]$ adalah sinyal asalnya, untuk h[n] adalah *high pass filter*, dan untuk g[n] merupakan *low pass filter*. Sehingga untuk dekomposisi lebih dari satu tingkat maka prosedur pada persamaan (2) dan (3) bisa digunakan untuk masing-masing pada tingkatan. Untuk contoh penggambaran dekomposisinya bisa dilihat pada gambar 2.3 yang menggunakan dekomposisi tiga tingkat.



Gambar 2.3 Konsep Discrete Wavelet Transform [8]

Pada gambar 2.3 $y_{tinggi}[k]$ dan $y_{rendah}[k]$ adalah hasil dari *high pass filter* dan *low pass filte*, dengan $y_{tinggi}[k]$ itu sendiri sebagai koefisien *Discrete Wavelet Transform*. $y_{tinggi}[k]$ adalah detail dari suatu informasi sinyal sedangkan untuk $y_{rendah}[k]$ adalah taksiran kasar dari suatu fungsi penskalaan. Dengan menggunakan koefisien DWT ini maka dapat melakukan proses *Inverse Discrete Wavelet Transform* (IDWT) yang dapat merekontruksikan menjadi sinyal asal.

$$□[□] = \sum_□(□_{□□□□□□}[□]h[-□ + 2□] + □_{□□□□□□h}[□]□[-□ + 2□]) \quad (4)$$

Pada proses rekontruksi yang merupakan kebalikannya dari suatu proses dekomposisi yang sesuai dengan tingkatan pada proses dekomposisi nya [14].

2.8 Penerapan DWT Pada *Watermarking*

Metode DWT dapat digunakan untuk citra digital yang sebaiknya di dekomposisi agar *watermark* dapat disisipkan ke dalam citra digital, setelah melakukan dekomposisi pada citra metode DWT dapat dilakukan atau diproses. Pada penyisipan *watermark dapat* dimodifikasi koefisiennya yaitu LL, LH, HL,HH rentang frekuensi dekomposisi pada citra yang menggunakan *wavelet.* Pada Data *watermark* rangkaian bilangan *W* yang digunakan adalah panjang *L* yang akan disisipkan pada koefisien rentang frekuensi yang akan dipilih[1].

Perbandingan DWT dengan metode lain pada tabel 2.2 berikut [15] :

Tabel 2.2 Perbandingan metode DWT

Kategori	DWT	DCT
Kemiripan hasil dari proses steganografi	Tinggi	Sedang
Sedikit waktu yang digunakan pada proses steganografi	Sedang	Tinggi
Tidak mudah diserang seperti kompresing terhadap citra yang telah	Tinggi	Rendah

dilakukan proses steganografi		

2.9 MATLAB

MATLAB (*Matrix Laboratory*) yaitu merupakan bahasa pemograman yang level nya tinggi memiliki kemampuan untuk komputasi teknis dalam memecahkan persoalan dengan notasi matematik. Matlab pada awalnya dibuat oleh proyek LINPACK dan EISPACK untuk mempermudah dalam melakukan pengembangan *software* yang berbasis matriks. Pada pembuatan aplikasi *watermarking* ini menggunakan Matlab versi R2015b. Setiap membuka aplikasi Matlab, maka akan diperoleh beberapa *form* atau *window*. *Command window* adalah *window* utama dalam Matlab. Matlab akan menyimpan *mode* atau *setting* terakhir lingkungan kerja yang digunakan sebagai *mode / setting* lingkungan kerja pada saat membuka aplikasi Matlab diwaktu bersamaan [14].

2.9.1 Bagian-bagian Penting MATLAB

Antarmuka penting saat menggunakan aplikasi MATLAB [7]:

1. Jendela Perintah (Command Window)- Memungkinkan menuliskan suatu perintah dan akan di ekseskusi secara langsung, Perintah bisa ini bisa berupa perhitungan,menjalankan suatu fungsi, melihat iformasi pada fungsi tertentu dan lainnya.Format perintah ini di tandai dengan syntax ">>" pada MATLAB.
2. Workspace (Ruang Kerja)- dapat diartikan sebagai window yang biasa digunakan untuk navigator bagi pengguna yang ingin mengetahui informasi variabel yang akan digunakan pada saat pemakaian MATLAB. Workspace window seperti perpustakaan yang memiliki informasi variabel dan perintah yang akan digunakan oleh pengguna yang sedang aktif.
3. Command History adalah Berisi daftar riawayat perintah yang sudah pernah di eksekusi oleh pengguna.
4. Current Directory - Window ini sebagai browser Directory aktif yang hampir sama dengan window explorer

5. Preferences adalah fiter yang memungkinkan pengguna untuk mengubah berbagai pengaturan seperti font , warna ,komentar , error , keyword dan lain sebagainya

2.9.2 Simbol-simbol dalam MATLAB

Beberapa symbol perintah yang dapat digunakan dalam MATLAB [7]:

1. % : Berfungsi untuk memberikan komentar dalam penulisan kode,Komentar sangat berguna untuk memberikan informasi atau keterangan pada suatu program.
2. >> : emungkinkan menuliskan suatu perintah dan akan di ekseskusi secara langsung pada Jendela Perintah (Command Window).
3. ; : Berfungsi untuk mencegah hasil dari program agar tidak muncul pada Command Window.
4. Tanda ini memberitahu bahwa suatu perintah dapat diterukan untuk baris berikutnya, Tanda ini digunakan pada akhir baris.
5 : ^C : Control + C merupakan perintah yang berfungsi untuk menghentikan program yang sedang di jalankan.

2.10 Label Hak Cipta

Hak cipta atau dalam bahasa inggris disebut *copyright* berasal dari 2 kata yaitu: *copy* berarti menggandakan dan *right* yang artinya hak. Dengan demikian secara bahasa, *copyright* pada hakikatnya merupakan hak untuk menggandakan atau menyebarluaskan sebuah hasil karya. Istilah pada *copyright* diartikan kedalam Bahasa Indonesia sebagai hak cipta. Hak cipta yaitu salah satu jenis perlindungan hak kekayaan intelektual (HKI) yang sudah disediakan untuk melindungi karya pengetahuan, seni dan sastra. Dalam Pasal 1 UU No.19/2020 tentang hak cipta yang berbunyi: “Hak Cipta adalah hak eksklusif bagi pencipta atau penerima hak untuk mengumumkan atau memperbanyak ciptaannya atau memberikan izin untuk itu dengan tidak mengurangi pembatasan-pembatasan menurut peraturan perundang-undangan yang berlaku ” (Pusat Inovasi LIPI,2012)

Perlindungan hak cipta sangat diperlukan bagi pemilik citra dikarenakan pada zaman sekarang teknologi yang sudah canggih banyak sekali orang lain yang mengakui karya seseorang tanpa mencantumkan sumber asli atau pemilik dari citra digital tersebut, sehingga membuat pemilik hak cipta tersebut susah untuk

membuktikan bahwa citra digital tersebut milik dia sendiri, maka dengan adanya pembuktian hak cipta dengan menyisipkan *watermark* didalam file citra digital yang akan di publikasi maka sangan disarankan untuk pemilik hak cipta menuliskan peringatan hak cipta terhadap karya yang telah dibuatnya untuk dipublikasi kan, untuk peringatan tersebut dapat meliputi nama pemilik hak cipta, tahun dipublikasikan pertama, baik dengan simbol © atau kata " hak cipta"[2].

2.11 Serangan-Serangan Pada *Watermarking*

Serangan yang dilakukan pada *watermark* digunakan untuk menguji ketahanan dari suatu teknik *watermarking* yang digunakan pada video tersebut. Serangan yang diberikan pada sebuah *watermarked video* sebelum melakukan proses ekstraksi *watermark*. Ada beberapa contoh serangan yang akan diberikan yaitu Kompresi, dan *cropping*. Berikut adalah penjelasan tentang serangan-serangan tersebut :

a. Kompresi merupakan suatu proses untuk memperkecil suatu ukuran citra digital dengan mengubah *bit rate* dari sebuah citra digital tersebut. Apabila semakin kecil *bit rate* citra digital maka akan semakin kecil ukuran citra digitalnya.
b. *Cropping* adalah suatu gangguan atau noise yang disebabkan dengan memotong Panjang sinyal atau durasi satu detik atau lebih pada suatu file video [16].

Untuk contoh serangan yaitu pada *watermarked audio* dengan melakukan kompresi MP3 yang pada saat *bit rate* semakin besar, maka nilai BER nya semakin baik. Hal ini dikarenakan nilai *bit rate* yang digunakan berhubungan dengan nilai frekuensi *cut-off* LPF (*Low Pass Filter*) yang digunakan sebagai proses kompresi [17].

2.12 Pengujian Dalam Kelayakan *Watermark*

Metode-metode yang dapat diterapkan pada *watermarking* yang memiliki suatu kelebihan dan kekurangan nya. Untuk menentukan suatu kelebihan dan kekurangan suatu metode itu dapat dilakukan dengan cara pengujian. Pengujian pada suatu *watermarking* dapat juga dilakukan dengan beberapa tahapan yaitu : pengujian kualitas citra, pengujian keamanan atau *security*, pengujian *recovery*, pengujian ketahanan atau *robustness* dan juga pengujian kapasitas suatu citra. Pengujian ketahanan atau juga bisa disebut *robustness* adalah pengujian yang

menggunakan cara memodifikasi suatu citra digital yang sudah di *watermark* sehingga file tersebut dapat bertahan dari serangan atau *attack* yang dapat membuat hancur *watermarked* yang sudah ada di file tersebut.

Pengujian ini bisa dilakukan dengan menggunakan *tools* tambahan seperti yang ada di *adobe primer* atau *camtasia*, atau *tools* yang lainnya yang digunakan untuk pengujian citra digital tersebut. Untuk pengujian keamanan atau *security* yang mengacu pada pencegahan untuk orang biasa yang tidak bisa untuk mendeteksi informasi yang tersembunyi didalam citra digital tersebut.

Pada pengujian keamanan juga bisa menggunakan *tools* seperti *StegSpy*. Kemudian untuk pengujian *recovery* adalah pengujian terhadap pesan (*watermark*) yang disisipkan atau disembunyikan harus dapat dikembalikan lagi atau diungkap Kembali (*reveal*). Tujuan dari *steganografi* adalah *hiding*, maka kapan pun pesan rahasia yang ada didalam citra penampung harus dapat diambil kembali untuk digunakan oleh seseorang. Untuk pengujian kapasitas yaitu mengacu pada suatu jumlah informasi yang dapat tersembunyi di dalam sampul media. Pengujian kapasitas yaitu bisa dengan cara membandingkan ukuran atau kapasitas antara suatu citra yang belum disisipkan *watermark* dengan citra yang sudah disisipkan *watermark.*

Untuk pengujian kualitas citra sendiri dapat dilakukan dengan cara melakukan perbandingan antara *file* yang masuk dan *file* yang keluar. Pengujian ini juga menggunakan rumus PSNR (*Peak Signal to Noise Ratio*) yang memiliki satuan *decibel* (dB) yang memkiliki nilai 255 yang merupakan nilai tertinggi intensitas suatu piksel, dan juga terdapat MSE (*Mean Square Error*) yang merupakan nilai rata-rata dari kuadrat *Absolute Error* antara media yang ingin disisipkan *watermark* dan *image watermaking* nya [18].

2.13 PSNR dan MSE

Peak Signal to Noise Ratio (PSNR) memiliki fungsi untuk menentukan kualitas citra. Pada perhitungan PSNR dan *Mean Square Error* (MSE). Nilai PSNR dapat digunakan untuk mengetahui perbedaan suatu nilai puncak sinyal dengan *noise, noise* yang dimaksud yaitu gambar terstego (*stego-image*) sedangkan untuk sinyal yang dimaksud adalah video asli atau (*cover video*). Nilai MSE digunakan untuk mengetahui perbedaan *error* antara gambar *stego-image*

dengan *cover-video*. Nilai PSNR berasal dari perbandingan antara citra asli dengan citra rekonstruksi. Untuk menentukan nilai PSNR dengan persamaan :

$$\square\square\square\square = 10 \log_{10} \frac{\square\square\square\square^2}{\square\square\square} \quad (5)$$

Dengan Rumus MSE :

$$\square\square\square = \frac{1}{\square\square} \sum_{\square=1}^{\square} \sum_{\square=1}^{\square} (\square_{\square\square} - \square_{\square\square})^2 \quad (6)$$

Keterangan :

x dan y = koordinat dari gambar

M dan N = dimensi dari gambar

S_xy = menyatakan stego-image

C_xy menyatakan cover-image

C_{max}^2 = Nilai maksimum dalam gambar yaitu nilai maksimum dari nilai piksel adalah 255 [19].

2.14 Tabel Penelitian Sebelumnya

Pada penelitian ini terdapat tinjauan Pustaka dari penelitian-penelitian yang berkaitan dengan perkembangan ilmu pengetahuan dan teknologi pada steganografi yang tentunya dapat dijadikan acuan untuk mempertimbangkan suatu metode yang akan digunakan dalam penelitian ini, dan berikut beberapa penelitian- penelitian sebelumnya yang terkait dengan steganografi pada tabel 2.3.

Tabel 2.3 Penelitian Sebelumnya

No	Judul	Nama Peneliti	Yang dikerjakan oleh peneliti
1.	Implementasi Metode *Spread Spectrum* Dalam *Steganografi* Pada File MP3 Berbasis Android	Azkar Kumala, Bambang Pramono, Rahmat Ramadhan	Pada penelitian ini perangkat lunak dibuat dengan mengimplementasikan steganografi dengan teknik *spread spectrum* pada berkas audio MP3, untuk ukuran file yang dihasilkan sebelum disisipkan dan setelah

			di ekstraksi hasilnya sama, kualitas berkas audio juga dapat dihasilkan bergantung dari besarnya ukuran pesan tersebut. Untuk penelitian selanjutnya diharapkan dapat melakukan bermacam-macam tipe file seperti citra video dan format citra digital lainnya [20].
2.	Digital *Watermarking* pada Citra Digital Fotografi Metode Discrete Wavelet Transform	Mohamad Sulthon Fitriansyah, Cahya Rahmad	Tulisan ini menggunakan metode DWT pada sebuah citra dengan citra penampung dan citra watermark adalah gambar dengan format jpg . Hasil eksperimen menunjukkan bahwa Kualitas citra penampung dan penempatan penyisipan pada frekuensi sangat lah berpengaruh pada penyisipan watermark, maka semakin tinggi kualitas citra penampung, tingkat *imperecbility* nya semakin tinggi juga. Saran untuk penelitian

			selanjutnya diharapkan citra penampung juga menggunakan citra warna atau rgb dan juga diharapkan bisa untuk format citra digital lainnya seperti video dan audio [21].
3.	Analisis Perbandingan Metode *Discrete Wavelet Transform* dan *Spread Spectrum* dalam *Watermarking* Citra *Digital* Berwarna	Muhammad Ardiansyah Agusstiawan, Nerfita Nikentari, ST., M.Cs, Hendra Kurniawan, S.Kom., M.Sc.Eng	Penelitian ini membandingkan metode *Discrete Wavelet Transform Spread* dan *Spectrum*, Metode *Discrete Wavelet Transform* menghasilkan nilai MSE yang tinggi dibandingkan metode *Spread Spectrum.* Penelitian ini hanya melakukan pada citra digital yaitu gambar dengan format JPG. Penelitian berikutnya dapat dikembangkan juga penyisipan pada file GIF/animasi, audio dan video [4].
4.	Implementasi Watermark Pada Citra Menggunakan Metode Spread Spectrum	Isninda Situmorang	Dalam penelitian ini metode *spread spectrum* yang diimplementasikan membantu untuk memenuhi kriteria *fidelity* karena pada penyisipan *watermark* tidak menyebabkan perubahan *watermarking*, yang membuat citra hasil

			watermarking sulit dibedakan dengan citra aslinya [22].
5.	Audio Watermarking Dengan Discrete Wavelet Transform dan Histogram Menggunakan Optimasi Algoritma Genetika	Vera Noviana Sulistyawan, Yohana Karina, Gelar Budiman	Penelitian ini menggunakan metode DWT dan histogram dengan algoritma genetika untuk melindungi citra digital yaitu audio dengan format .wav, dengan audio yang diuji menggunakan serangan seperto *low pass filter, resampling*, semakin banyak bit yang disisipkan maka nilai SNR akan semakin berkurang, maka kualitas pada citra pun berkurang [16].