BAB II

LANDASAN TEORI

2.1 Pengenalan *Watermarking*

Watermarking sudah ada sejak 700 tahun yang lalu. Pada akhir abad 13, pabrik kertas di Fabriano, Italia, membuat kertas yang diberi *watermark* atau tanda air dengan cara menekan bentuk cetakan gambar atau tulisan pada kertas yang baru setengah jadi. Ketika kertas dikeringkan terbentuklah suatu kertas yang ber-*watermark*. Kertas ini biasanya digunakan oleh seniman atau sastrawan untuk menulis karya mereka. Kertas yang sudah dibubuhi *watermark* tersebut sekaligus dijadikan identifikasi bahwa karya seni di atasnya adalah milik mereka (*Munir, 2004*).

Ide *watermarking* pada data digital sehingga disebut digital *watermarking* dikembangkan di Jepang tahun 1990 dan di Swiss tahun 1993. Digital *watermarking* semakin berkembang seiring dengan semakin meluasnya penggunaan internet, objek digital seperti video, citra, dan suara yang dapat dengan mudah digandakan dan disebarluaskan.

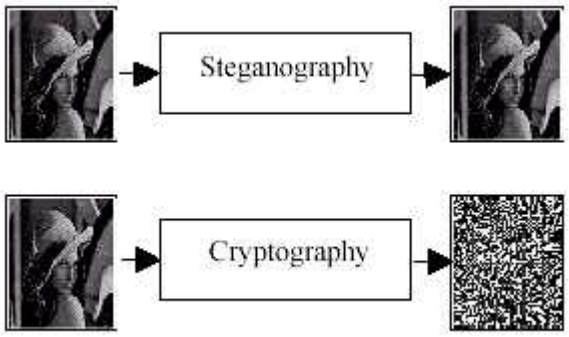
2.1.1 Defenisi *Watermarking*

Watermarking merupakan suatu bentuk dari *steganography*, *yaitu* ilmu yang mempelajari bagaimana menyembunyikan suatu data pada data atau *file* digital lainnya (*Suhono dkk, 2000*). *Watermarking* atau tanda air dapat diartikan sebagai suatu teknik penyembunyian data atau informasi rahasia kedalam suatu data lainnya untuk ditumpangi, tetapi tidak disadari kehadirannya oleh indera manusia, yaitu indera penglihatan dan indera pendengaran. Disamping itu data yang ter-*watermark* harus tahan (*robust*) terhadap serangan-serangan baik secara sengaja maupun tidak sengaja untuk menghilangkan data *watermark* yang terdapat didalamnya. *Watermark* juga harus tahan terhadap berbagai jenis

pengolahan atau proses digital yang tidak merusak kualitas data yang ter-*watermark*. Akan tetapi dari berbagai penelitian yang sudah dilakukan belum ada suatu metode *watermarking* ideal yang bisa tahan terhadap semua proses pengolahan digital yang mungkin terjadi. Biasanya masing masing penelitian memfokuskan pada hal-hal tertentu yang dianggap penting. Penelitian dibidang *watermarking* masih terbuka luas dan semakin menarik, salah satunya karena belum ada suatu standar yang digunakan sebagai alat penanganan masalah hak cipta ini.

Watermarking berbeda dengan tanda air pada uang kertas. Tanda air pada uang kertas masih dapat kelihatan oleh mata manusia, tetapi *watermarking* pada media digital dimaksudkan agar tidak dapat dirasakan kehadirannya oleh manusia tanpa alat bantu mesin pengolah digital seperti komputer. *Watermarking* memanfaatkan kekurangan-kekurangan sistem indera manusia seperti mata dan telinga. Dengan adanya kekurangan inilah, metode *watermarking* dapat diterapkan pada berbagai media digital (*Suhono dkk, 2000*). Jadi *watermarking* merupakan suatu cara untuk penyembunyian data atau informasi tertentu kedalam suatu data digital lainnya, tetapi tidak diketahui kehadirannya oleh indera manusia yaitu indera penglihatan dan indera pendengaran serta mampu menghadapi proses proses pengolahan sinyal digital.

Ilmu yang memiliki kesamaan dengan *watermarking* lainnya adalah *steganography* dan *cryptography*. *Steganography* berbeda dengan *cryptography*, letak perbedaannya adalah hasil keluarannya. Hasil dari *cryptography* biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan (tetapi dapat dikembalikan ke bentuk semula) sedangkan hasil keluaran dari *steganography* ini memiliki bentuk persepsi yang sama dengan bentuk aslinya, tentunya persepsi disini oleh indera manusia, tetapi tidak oleh komputer atau perangkat pengolah digital lainnya.



Gambar 2.1 Ilustrasi *Steganography* dan *Cryptography* Pada Citra

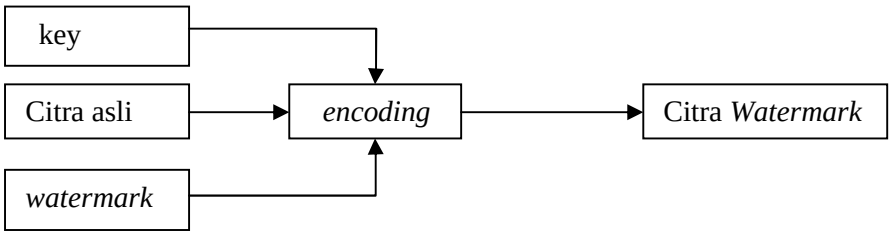
2.1.2 Perbedaan *Watermarking* dan *Steganography*

Steganography (dalam bahasa Yunani disebut *Steganos,* "tersembunyi/ disembunyikan", dan *grapphein,* "menulis") adalah sebuah seni dan ilmu *(science)* tentang berkomunikasi dengan cara menyembunyikan eksistensi informasi dari komunikasi tersebut. *Steganography* menyembunyikan eksistensi suatu pesan dengan cara menanamkan/melekatkan *(embedding)* pesan ke dalam sebuah media yang disebut *carrier file (Sujay dkk, 2010).*

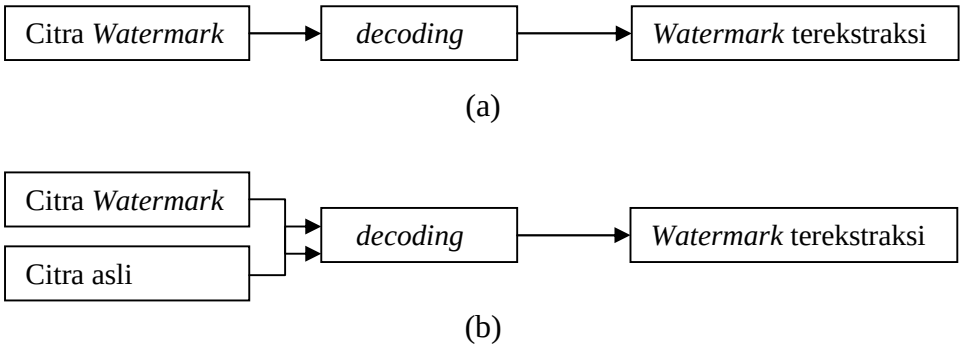
Dalam prinsif kerjanya, ilmu *steganography* hampir sama dengan *watermarking,* dimana keduanya menerapkan prinsip penyembunyian pesan atau informasi di dalam media digital. Namun perbedaan diantar keduanya, jika pada *steganography* informasi rahasia disembunyikan didalam media digital dimana media penampung tidak berarti apa-apa, maka pada *watermarking* justru media digital tersebut yang akan dilindungi kepemilikannya dengan pemberian label hak cipta.

2.1.3 Proses *Watermark* dan Verifikasi *Watermark*

Proses penyisipan *watermark* ke dalam citra disebut *encoding/embedding*. *Encoding* dapat disertai dengan pemasukan kunci atau tidak memerlukan kunci. Kunci diperlukan agar hanya dapat diekstraksi oleh pihak yang sah. Kunci juga bermanfaat untuk mencegah *watermark* dihapus oleh pihak yang tidak berhak atau bertanggung jawab. Sedangkan ketahanan terhadap proses-proses pengolahan lainnya, itu tergantung pada metode *watermarking* yang digunakan.



Gambar 2.2 Proses penyisipan *watermark* pada citra digital (*Suhono dkk, 2000*)



Gambar 2.3 (a) Proses ekstraksi tanpa citra asli (*Suhono dkk, 2000*)
(b) Proses ekstraksi dengan citra asli (*Suhono dkk, 2000*)

Verifikasi *watermark* dilakukan untuk membuktikan status kepemilikan citra *digital*. Pada sub-proses ekstraksi disebut juga *decoding/extraction*, yang bertujuan untuk mengungkap data *watermark* yang disisipkan dalam citra *digital*. Pada proses *decoding* dapat mengikutsertakan citra asli (*non blind watermarking*) atau tidak sama sekali (*blind watermarking*), karena beberapa skema *watermarking* memang menggunakan citra asli dalam proses *decoding.*

2.1.4 Tujuan *Watermarking*

Ada berbagai tujuan yang ingin dicapai dari penggunaan *watermarking*, sebagai suatu teknik penyembunyian data pada data digital lainnya yaitu :

a. *Tamper-proofing*; *watermarking* digunakan sebagai alat untuk mengidentifikasikan atau alat indikator yang menunjukkan data digital telah mengalami perubahan dari aslinya.
b. *Feature location*; menggunakan metoda *watermarking* sebagai alat untuk identifikasikan isi dari data digital pada lokasi-lokasi tertentu, seperti

contohnya penamaan objek tertentu dari beberapa objek yang lain pada suatu citra digital.

c. *Annotation/caption*; *watermarking* hanya digunakan sebagai keterangan tentang data digital itu sendiri.
d. *Copyright-Labeling*; *watermarking* dapat digunakan sebagai metoda untuk penyembunyikan label hak cipta pada data digital sebagai bukti otentik kepemilikan karya digital tersebut.

2.1.5 Klasisfikasi *Watermarking*

Digital *watermarking* dapat dibagi ke dalam beberapa kategori (*Singh*, 2011) diantaranya adalah :

1. Berdasarkan media penyimpan
   a. Teks merupakan naskah atau karangan dalam bentuk digital yang dapat memberikan informasi atau petunjuk.
   b. Gambar/citra merupakan kombinasi warna yang dapat di olah oleh komputer
   c. *Audio* adalah *file* digital yang berbentuk suara yang dapat disimpan dalam format tertentu.
   d. *Video* merupakan gabungan dari citra dan audio sehingga menghasilkan suara dan gambar bergerak.
2. Berdasarkan kenampakan dari *watermark*
   a. Invisible watermarking

      Objek *watermark* yang dilekatkan pada citra digital secara visual tidak dapat terlihat tetapi dapat diekstrak oleh program atau komputer.

   b. Visible watermarking

      Visible watermarking merupakan salah satu jenis *watermarking*, dimana objek *watermak* yang dilekatkan pada citra digital secara visual dapat terlihat jelas oleh mata.

   c. Dual watermark

      Dual watermark adalah kombinasi dari *invisible* dan *visible watermarking* dalam sebuah media penampung. *Invisible watermark*

pada dual *watermark* digunakan sebagai *watermark* cadangan. Sehingga secara penglihatan manusia hanya terlihat satu *watermark* saja.

3. Berdasarkan Metode Cara Kerja
   a. Domain spasial

      Teknik *watermarking* dalam domain spasial bekerja dengan cara menanamkan *watermark* secara langsung kedalam piksel dari suatu citra. Istilah domain spasial sendiri mengacu pada piksel-piksel penyusun sebuah citra. Beberapa contoh teknik yang bekerja pada domain spasial adalah teknik penyisipan pada *least significant bit* (LSB), *patchwork*, *masking-filtering*.

   b. Domain frekuensi

      Teknik *watermarking* dalam domain frekuensi bekerja dengan cara menanamkan *watermark* pada koefisien frekuensi hasil transformasi citra asalnya. Terdapat beberapa transformasi untuk menghasilkan koefisien frekuensi, antara lain : *Discrete fourier transform* (DFT), *Discrate Cosine Transform* (DCT), *Discrete Wafalet Transform* (DWT), *Spreas Spectrum*, domain kompresi dan *hybrid*.

4. Berdasarkan Tingkat Kekokohan (*Robustness*)

   Berasarkan tingkat kekokohan, *watermark* dibedakan menjadi 3, yaitu *secure watermarking*, *robust watermarking* dan *fragile watermarking*.

   a. *Secure watermarking*.

      Secure watermarking artinya *watermarking* harus tahan terhadap *non-malicious attack* dan *malicious attack. Non-malicious attack* merupakan serangan berupa manipulasi yang normal terjadi terhadap sebuah citra ber-*watermark*, misalnya kompresi, penskalaan, penyuntingan, operasi geometri (translasi dan rotasi), dan *cropping.* Sedangkan *malicious attack* merupakan serangan yang bertujuan menghilangkan atau merubah *watermark* pada citra sehingga *watermark* tidak dapat dipergunakan sebagaimana mestinya.

b. *Robustness watermarking*

Watermark jenis ini harus mampu bertahan terhadap *non-malicious attack*. *Watermark* masih bisa diekstraksi setelah terjadi modifikasi pada citra.

c. *Fragile watermarking*

Pada *fragile watermarking*, *watermark* sengaja dibuat agar mudah berubah, rusak, atau bahkan hilang ketika dilakukan modifikasi pada citra ber-*watermark*. *Fragile watermarking* digunakan pada aplikasi yang bertujuan untuk memverifikasi isi (*content*) citra, misalnya untuk *image authentication* atau *tamper detection* (deteksi manipulasi). *Watermark* yang telah rusak atau hilang adalah pertanda bahwa citra sudah mengalami manipulasi dan tidak otentik lagi.

2.2 Label Hak Cipta

Hak cipta berasal dari bahasa inggris *copyright* yang dalam terjemahannya (to) *copy* berarti menggandakan dan *right* berarti hak. Dengan demikian secara bahasa, *copyright* pada prinsipnya adalah hak untuk menggandakan atau menyebarluaskan suatu hasil karya. Istilah *copyright* diartikan kedalam bahasa Indonesia sebagai hak cipta. Hak cipta merupakan salah satu jenis perlindungan hak kekayaan intelektual (HKI) yang desediakan untuk melindungi karya pengetahuan, seni dan sastra. Pasal 1 UU No.19/2002 tentang hak cipta menyatakan : " Hak cipta adalah hak eksklusif bagi pencipta atau penerima hak untuk mengumumumkan atau memperbanyak ciptaanya atau memberikan izin untuk itu dengan tidak mengurangi pembatasan-pembatasan menurut peraturan perundangan-undangan yang berlaku" (Pusat Inovasi LIPI, 2012).

Perlindungan hak cipta semakin dibutuhkan karena semakin banyaknya peniruan dan penyebarluasan tanpa memperhatikan aspek hak cipta oleh pihak lain. Dan juga hak cipta juga merupakan pengakuan terhadap status *authorship* yang mampu mengangkat nilai dari suatau karya sehingga dapat meningkatkan daya kompetensi atas suatu karya.

Dengan alasan untuk tujuan pembuktian atas tuntutan pelanggaran, sangat disarankan kepada penulis atau pencipta karya seni untuk menuliskan peringatan hak cipta atas semua karya yang dimaksudkan untuk publikasi. Peringatan tersebut meliputi nama pemilik hak cipta, tahun dipublikasikan pertama, baik dengan simbol © atau kata “hak cipta”.

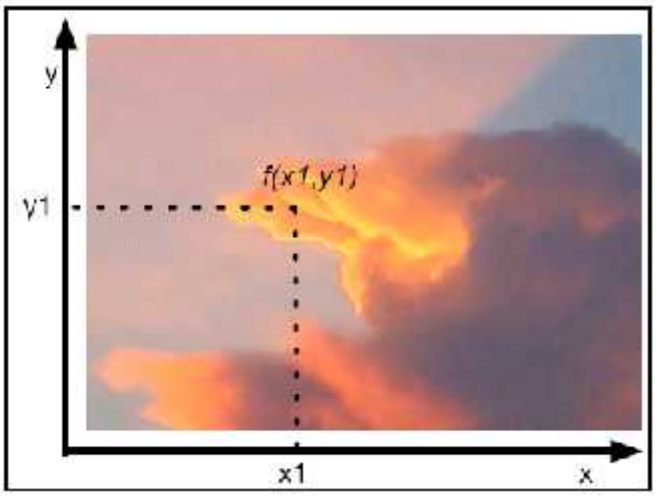
2.3 Pengertian Citra

Citra (*image*) adalah gambar yang terletak pada bidang dwimatra (dua dimensi). Ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (*continue*) dari intensitas cahaya pada bidang dwimatra. Sumber cahaya menerangi objek, objek memantulkan kembali sebagian dari berkas cahaya tersebut. Pemantulan cahaya ini ditangkap oleh alat-alat optik antara lain layaknya mata pada manusia atau hewan, alat sensor cahaya, kamera, pemindai (*scanner*), dan sebagainya, sehingga bayangan objek tersebut dapat terekam atau tersimpan kedalam format digital maupun analog.

Citra juga sebagai keluaran suatu sistem perekam data dapat bersifat optik berupa foto, bersifat analog berupa sinyal-sinyal video seperti gambar pada monitor televisi atau bersifat digital yang dapat langsung disimpan pada suatu media penyimpanan

2.4 Pengertian Citra Digital

Citra digital dapat didefinisikan sebagai fungsi dua variabel, *f(x,y)*, dimana *x* dan *y* adalah koordinat spasial dan nilai *f(x,y)* adalah intensitas citra pada koordinat tersebut, hal tersebut diilustrasikan pada gambar 2.3. Teknologi dasar untuk menciptakan dan menampilkan warna pada citra digital berdasarkan pada penelitian bahwa sebuah warna merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau, dan biru (*Red, Green, Blue* - RGB).



Gambar 2.4 Citra Digital *(Siraith, 2009)*

2.4.1 Elemen Elemen Citra Digital

Citra digital mengandung beberapa elemen dasar yang perlu diketahui sebagai dasar manipulasi dan pengolahan citra (Munir, 2004), elemen dasar tersebut adalah:

1. Kecerahan (*brightness*)

   Kecerahan adalah kata lain untuk intensitas cahaya. Kecerahan pada sebuah titik (piksel) didalam citra bukanlah intensitas yang riil, tetapi sebenarnya adalah intensitas rata-rata dari suatu area yang melingkupinya. Sistem visual manusia mampu menyesuaikan tingkat kecerahan (*brightness level*) yang ditangkapnya mulai dari yang paling rendah sampai yang pailing tinggi.

2. Kontras (*contrast*)

   Kontras menyatakan sebaran terang (*lightness*) dan gelap (*darkness*) di dalam sebuah gambar. Citra dengan kontras rendah memiliki komposisi sebagian besar terang atau sebagian besar gelap. Sedangkan citra dengan kontras yang baik memiliki komposisi gelap dan terang tersebar secara merata.

3. Kontur (*countur*)

   Kontur adalah keadaan yang ditimbulkan oleh perubahan intensitas pada piksel yang bertetangga. Karena adanya perubahan intensitas inilah maka kita mampu mendeteksi tepi-tepi objek dalam citra.

4. Warna (*colour*)

   Warna adalah spectrum tertentu yang terdapat di dalam suatu cahaya sempurna (berwarna putih). Identitas suatu warna ditentukan panjang gelombang cahaya tersebut. Warna juga dapat dinyatakan sebagai persepsi yang dirasakan oleh sistem visual manusia terhadap panjang gelombang yang berbeda. Didalam pengolahan citra, model warna dapat dibagi menjadi beberapa model, diantaranya adalah:

   a. Model warna RGB (*Red, Green, Blue*)

      Model warna RGB disebut juga dengan *additive color*. Dimana pada model warna ini memiliki tiga warna primer, yaitu *Red, Green* dan *blue*. Model warna RGB digunakan pada citra yang ditampikan pada layar monitor dan kamera video.

   b. Model warna CMYK

      CMYK adalah sebuah model warna berbasis pengurangan sebagian gelombang cahaya (*substractive colour model*) dan yang umum dipergunakan dalam pencetakan berwarna (*printer*). Istilah CMYK juga biasanya digunakan untuk menjelaskan proses pencetakan itu sendiri.

   c. Model warna HIS

      Model HIS merupakan sistem warna yang paling mendekati cara kerja mata manusia. HIS menggabungkan informasi baik warna maupun *grayscale* dari sebuah citra.

   d. Model warna YCbCr

      Ruang warna YCbCr digunakan untuk video digital. Dalam format ini, informasi luminasi diwakili oleh komponen tunggal Y dan informasi warna disimpan sebagai komponen warna yang berbeda, yaitu Cb dan Cr.

e. Model warna *Grayscale*

Model warna *Grayscale* adalah model warna hitam putih yang tiap piksel memiliki warna dari 0 sampai dengan 255 dimana 0 adalah warna hitam dan 255 adalah warna putih.

5. Bentuk (*Shape*)

Shape adalah *property* intrinsic dari objek 3 dimensi, dengan pengertian bahwa bentuk merupakan *property* intrisnsik utama untuk system visual manusia.

6. Teksture (*Texture*)

Tekstur dicirikan sebagai distribusi spasial dari derajat keabuan didalam sekumpulan pixel yang bertetangga. Oleh karena itu tekstur tidak dapat didefenisiskan untuk sebuah piksel. Sistem visual manusia tidak dapat menerima informasi secara independen pada setiap piksel, melainkan citra dianggap sebagai suatu kesatuan dari beberapa piksel.

2.4.2 Representasi Citra

Komputer hanya dapat mengolah isyarat-isyarat elekronik digital yang merupakan kumpulan sinyal biner yang bernilai 0 dan 1 (Balza, 2005). Untuk itu, citra digital harus memiliki format tertentu yang sesuai sehingga dapat merepresentasikan objek pencitraan dalam bentuk kombinasi data biner.

Pada kebanyakan kasus, terutama untuk keperluan penampilan secara visual, nilai data digital tersebut merepresentasikan warna dari citra yang diolah, dengan demikian format data citra digital berhubungan erat dengan warna. Citra digital terdiri dari tiga (Munir, 2004) yaitu:

1. Citra biner (*monochrome*)

Pada citra biner hanya memiliki dua nilai yaitu nilai 0 yang merepresentasikan warna putih dan nilai 1 yang merepresentasikan warna hitam. Jadi pada citra biner latar belakang berwarna putih sedangkan objek berwarna hitam. Ada beberapa alasan penggunaan citra biner, salah satunya adalah kebutuhan memori kecil karena hanya membutuhkan representasi 1 bit.

2. Citra *grayscale*

   Citra *grayscale* memberikan kemungkinan warna yang lebih banyak dari pada citra biner, karena ada *range* nilai lain diantara nilai minimum dan nilai maksimumnya. Banyaknya kemungkinan nilai tersebut tergantung pada jumlah bit yang digunakan. Format citra ini disebut *grayscale* (skala keabuabuan) karena pada umumnya warna yang dipakai adalah antara hitam sebagai warna minimal dan warna putih sebagai warna maksimalnya, sehingga warna diantaranya adalah abu-abu.

3. Citra warna (*true color*)

   Pada citra warna, setiap titik mempunyai warna yang spesifik merupakan kombinasi dari 3 warna dasar, yaitu : merah, hijau dan biru. Format citra ini sering disebut sebagai citra RGB (*red, green,* dan *blue*). Setiap warna dasar mempunyai intensitas sendiri dengan nilai maksimum 256 (8-*bit*). Jumlah kombinsi warna yang mungkin untuk format citra ini adalah 2^{24} atau lebih dari 16 juta warna, dengan demikian bisa dianggap mencakup semua warna yang ada, inilah sebabnya format ini dinamakan *true color*.

2.4.3 Format Citra

Pemrosesan citra menggunakan komputer membutuhkan citra digital sebagai masukannya. Oleh karena itu, kita mengenal beberapa macam format citra digital, antara lain:

1. Format berkas *bitmap* (bmp)

   Citra disimpan dalam berkas (*file*) dengan format terntentu. Bmp merupakan format citra yang baku di lingkungan sistem operasi *windows* dan *IBM* OS/2). Format ini memiliki ukuran berkas lebih besar dari pada format citra lainnya seperti GIF, PNG dan JPEG karena pada format ini tidak mengalami proses pemanfaatan. Citra dalam format bmp lebih bagus daripada citra dalam format lainnya, karena citra dalam format bmp umumnya tidak dimanfaatkan sehingga tidak ada informasi yang hilang (Munir, 2004)

2. Format format standar kompresi pada citra digital

   a. *Graphic Interchange Format* (GIF)

      GIF dibuat oleh *Compuserve* pada tahun 1987 untuk menyimpan berbagai *file* bitmap manjadi *file* lain yang mudah diubah dan ditransmisikan pada jaringan komputer. GIF merupakan format citra web yang tertua yang mendukung kedalaman warna sampai 8 bit (256 warna).

   b. *Portable Network Graphic* (PNG)

      Format png digunakan di internet dan merupakan format terbaru setelah gif, bahkan menggantikan gif untuk internet karena gif terkena patent LZW yang dilakukan oleh Unisys. Format PNG mendukung kedalaman warna 48bit dan memiliki teknik pencocokan warna yang lebih canggih dan akurat.

   c. *Joint Photographic Expert Group* (JPEG)

      Format jpeg mampu mengkompres objek dengan tingkat kualitas sesuai dengan pilihan yang disediakan, format jpeg sering dimanfaatkan untuk menyimpan gambar yang akan digunakan untuk keperluan halaman web, multimedia, dan publikasi elektronik lainnya. Format jpeg mampu meyimpan gambar dengan mode warna RGB, SMYK dan *grayscale*. Format jpeg juga mampu menyimpan alpha chanel, namun karena orintasinya ke publikasi elektronik maka format ini berukuran relatif lebih kecil dibandingkan dengan format *file* lainnya. Format jpeg merupakan salah satu hasil kompresi *lossy*.

2.5 Metode *Masking-Filtering*

Metode *Masking-Filtering* termasuk kedalam domain spasial, dimana penyembunyian *watermark* dilakukan dengan memanipulasi nilai *luminance* citra. *Masking* berfungsi sebagai penandaan tempat pada citra yang bisa disisipkan *watermark* yang menghasilkan *image mask. Image mask* sama seperti *binery image* (citra biner) dimana nilainya terdiri dari dua bagian, yaitu hitam (0) dan

putih (1). Nilai 1 atau putih merupakan area yang akan digunakan untuk menyisipkan *watermark* ke citra asli.

Metode *masking-filtering* ini biasanya dibatasi pada *image* 24 bit *color* atau citra *grayscale*. Penerapan metode *masking-filtering* pada *watermarking* adalah dengan memberi tanda (*marking*) pada citra untuk menyembunyikan pesan atau informasi, pesan atau informasi yang disembunyikan seperti *paper watermark*. Hal ini dapat dilakukan, misalnya dengan memodifikasi *luminance* beberapa bagian dari citra.

Secara umum penerapan metode *masking filtering* pada *watermarking* dapat dilihat dibawah ini.

1. Konversi RGB ke YCbCr

   Citra pada dasarnya tersusun atas piksel (titik). Tiap piksel terdapat 3 komponen dasar, yiatu RGB (*red green Blue*). Adapun cara Konversi RGB ke ruang warna YCbCr adalah dengan rumus :

   $Y = 0.257R' + 0.504G' + 0.098B' +16$……(2.1)

   $Cb = -0.148R' - 0.291G' + 0.439B' + 128$……..…..(2.2)

   $Cr = 0.439R' - 0.368G' - 0.071B' + 128$……..(2.3)

2. Konversi Teks ke Citra Biner

   Citra biner merupakan citra yang tersusun atas dua warna, yaitu 0 dan 1 yang menjelaskan tentang warna hitam dan putih. Citra biner disini digunakan untuk menandai citra asli dan sekaligus merupakan tempat penyimpanan *watermark* pada Citra asli. Cara untuk mendapatkan Citra Biner tesebut adalah dengan mengkonversi teks yang dijadikan *watermark* ke Citra biner.

3. Konversi YcbCr ke RGB

   Setelah proses penyisipan teks ke Citra Asli di lakukan, citra masih dalam bentuk YcbCr. Untuk merubah kembali ke ruang warna RGB, maka digunakan rumus sebagai berikut :

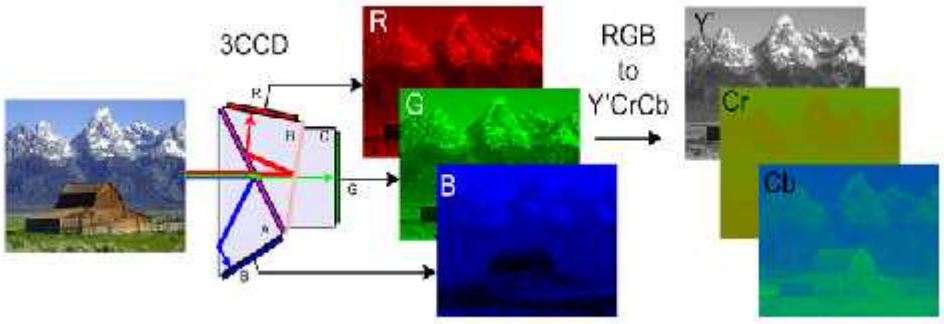
   $R = 1.164(Y-16)+1.596(Cr-128)$ .....(2.4)

   $G = 1.164(Y-16)-0.813(Cr-128)-0.391(Cb-128$ .....(2.5)

   $B = 1.164(Y-16)+2.018(Cb-128)$ .....(2.6)

Pemilihan ruang warna YCbCr didasarkan dari karakter ruang warna tersebut, dimana YCbCr memiliki komponen *Chrominance* dan *Luminance*. Nilai komponen *Chrominance* menggambarkan corak warna dan saturasi (*saturation*), nilai ini didapat dari Cb yang menggambarkan warna biru dan Cr yang menggambarkan warna merah. Sedangkan komponen *Luminance* (Y) merupakan nilai yang menggambarkan kontras gelap dan terang pada citra.

Pemilihan nilai *luminance* (Y) yang digunakan sebagai tempat penyembunyian *watermark* didasarkan dari kelebihan nilai *luminance* itu sendiri. Dimana jika penyembunyian dilakukan pada nilai RGB, maka perubahan yang terjadi pada citra asli akan dominan oleh salah satu komponen *Red*(R), *Green*(G) dan *Blue*(B). Sedangkan jika kita menggunakan nilai *luminance*, pengaruh ke citra asli hanya kontrasnya saja. Untuk lebih jelas bisa dilihat pada gambar ini:



Gambar 2.5 : RGB to YcbCr (sumber : *en.wikipedia*)

2.6 Pengujian Kelayakan *Watermark*

Metode-metode yang diterapakan pada *watermarking* memiliki kelebihan dan kekurangan masing-masing. Untuk menentukan kelebihan dan kekurangan suatu metode dapat dilakukan dengan cara pengujian. Pengujian pada *watermarking* dapat dilakukan dengan beberapa tahapan, yaitu pengujian kualitas citra, pengujian ketahanan (*robustness*), pengujian keamanan (*security*) pengujian *recovery* dan pengujian kapasitas citra. Pengujian ketahanan (*robustness*) merupakan pengujian dengan cara memodifikasi media (citra *watermark*) sehingga dapat bertahan terhadap suatu *attack* yang dapat menghancurkan informasi tersembunyi (*Ermadi dkk, 2004*). Aspek pengujian ini bisa dilakukan

dengan menggunakan *tools* tambahan untuk mendukung hasil penelitian, seperti menggunakan *tools Photoscape* dan *Photoshop CS3* atau *tools* pengolahan citra lainnya. Kemudian pengujian keamanan (*security*) adalah mengacu pada pencegahan bagi orang biasa yang tidak mampu untuk mendeteksi informasi tersembunyi didalam media (*Ermadi, dkk 2004*). Pada pengujian keamanan bisa menggunakan *tools* seperti *StegSpy*. Pada pengujian *recovery* merupakan pengujian terhadap pesan (*watermark*) yang disembunyikan harus dapat diungkap kembali (*reveal*). Karena tujuan steganografi/*watermarking* adalah data *hiding*, maka sewaktu-waktu pesan rahasia didalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut (*Munir, 2006, hal:307*). Pada pengujian kapasitas adalah mengacu pada jumlah informasi yang dapat tersembunyi di dalam sampul media (*Ermadi dkk, 2004*). Adapun cara pengujian kapasitas adalah dengan cara membandingkan ukuran atau kapasitas antara citra yang belum disisip *watermark* dengan citra yang sudah disisip *watermark.*

Sedangkan untuk pengujian kualitas citra dapat dilakukan dengan cara melakukan perbandingan terhadap *file* masukan dan *file* keluaran. Pengujian ini menggunakan formula PSNR (*Psedu Signal Number Ratio*) yang memiliki satuan *decibel* (dB). Secara matematis, nilai PSNR dapat dilihat pada formula dibawah ini:

$$PSNR = 10\ log_{10}\left(\frac{255}{MSE}\right) \text{dB} \quad \text{.....(2.8)}$$

Dimana nilai 255 merupakan nilai tertinggi intensitas suatu piksel. Sedang *Mean Sequer Error* (MSE) merupakan nilai rata-rata dari kuadrat *Absolute Error* antara media penyisipan *watermark* dengan *image watermark*. Untuk mendapatkan nilai MSE dapat dihitung dengan formula berikut:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(I\,(i,j) - K\,(i,j)\right)^n \quad \text{.....(2.9)}$$

Dimana m : Jumlah baris atau lebar citra

n : Jumlah kolom atau tinggi citra

I(i,j) : Nilai piksel pada citra asli

K(i,j) : Nilai piksel pada citra yang terdapat *watermark*

2.7 Bahasa Pemograman Matlab

Matlab merupakan bahasa pemograman yang hadir dengan fungsi dan karakteristik yang berbeda dengan bahasa pemrograman lain yang sudah ada lebih dahulu seperti Delphi, Visual Basic maupun C++.

Menurut Noore (2009) Matlab adalah sebuah bahasa pemrograman dengan kemampuan tinggi untuk melakukan komputasi teknis yang menggabungkan komputasi, visualisasi dan pemrograman dalam satu kesatuan yang mudah digunakan dimana masalah dan penyelesaiannya diekspresikan dalam notasi matematika yang sudah dikenal.

Nama Matlab merupakan singkatan dari *matrix labolatory*. Matlab awalnya dibuat untuk memudahkan dalam mengakses *software* matriks yang telah dikembangkan oleh LINPACK dan EISPACK. Dalam perkembangannya, Matlab mampu mengintegrasikan beberapa *software* matriks sebelumnya dalam satu *software* untuk komputasi matriks.

2.7.1 Bagian-bagian penting Matlab

Beberapa bagian penting didalam matlab (Aris, 2006):

1. Jendela Perintah (*Commond Window*)

   Pada jendela perintah, semua perintah matlab dituliskan dan dieksekusi. kita dapat menuliskan perintah yang diperlukan seperti perhitungan biasa, memanggil fungsi, mencari informasi tentang sebuh fungsi, demo program dan sebagainya. Setiap penulisan perintah disini selalu diawali dengan prompt “>>”.

2. Jendela Ruang Kerja (*Workspace*)

   Workspace merupakan sebuah jendela matlab yang berisi informasi pemakaian variabel di dalam memori matlab.

3. *Command History*

   Command History merupakan jendela yang berisi informasi tentang perintah yang pernah dituliskan sebelumnya. Jendela *history* memperlihatkan beberapa perintah yang pernah diketikkan. Kita bisa mengambil kembali perintah tersebut dengan meng-*copy-paste* ke jendela perintah.

4. *Current Directory*

   Current directory menampilkan isi dari direktori kerja saat menggunakan matlab. kita dapat mengganti direktori ini sesuai dengan tempat direktori kerja yang diinginkan. *Default* dari alamat direktori berada adalam didalam folder *works* tempat program *file* Matlab berada.

5. *Preferences*

   Preferences merupakan fasilitas yang digunakan untuk mengatur segala sesuatu tentang matlab. Misalnya pengaturan jenis, ukuran maupun warna *font* untuk *keyword*, komentar, *string*, *error* dan sebagainya.

2.7.2 Simbol-simbol dalam matlab

Berikut merupakan simbol-simbol yang ada didalam perintah matlab (Budi, 2007) :

1. % : semua teks sesudah tanda ini tidak akan dieksekusi atau dengan kata lain semua teks akan dianggap komentar. Dalam pemrograman, komentar sangat penting misalnya untuk memberitahu apa maksud suatu baris *command* atau memberi keterangan untuk apa suatu program ditulis.
2. >> ini adalah *default Matlab prompt*. Semua perintah yang akan dieksekusi didalam *Command Window* ditulis sesudah prompt ini.

3. ; Tanda *semicolon* diakhiri baris perintah ini digunakan untuk mencegah Matlab untuk tidak menampilkan hasilnya di *command Window*.
4. ... tanda titik tiga diakhiri baris memberitahu Matlab bahwa suatu perintah dilanjutkan dibaris berikutnya.
5. ^C kontrol C adalah perintah untuk menghentikan eksekusi Matlab dan kembali lagi ke *comman prompt*.