BAB II

LANDASAN TEORI

2.1 Keamanan data

Masalah keamanan merupakan salah satu aspek yang sangat penting dari sebuah sistem informasi. Tapi yang sangat di sayangkan, masalah keamanan ini kurang mendapat perhatian. Seringkali masalah keamanan menjadi urutan kedua atau bahkan urutan yang terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performansi system, masalah keamanan ini sering dikurangi atau bahkan ditiadakan.

Kemampuan untuk mengakses untuk menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan maupun individual (pribadi). Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi computer dan telekomunikasi. Dahulu jumlah komputer sangat terbatas dan belum digunakan untuk menyimpan hal-hal yang sifatnya sensitif. Penggunaan komputer untuk menyimpan informasi yang sifatnya *classified,* baru dilakukan sekitar tahun 1950-an.

Sangat pentingnya sebuah nilai informasi menyebabkan seringkali informasi di inginkan hanya boleh diakses oleh orang-orang tertentu saja. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Sebagai contoh, banyak informasi dalam sebuah perusahaan yang hanya boleh diakses oleh orang-orang tertentu di

dalam perusahaan tersebut, seperti misalnya informasi tentang produk yang sedang development, algoritma-algoritma dan teknik yang digunakan untuk menghasilkan produk tersebut. Untuk itu keamanan dari sistem informasi harus terjamin dalam batas yang bisa diterima.

Jaringan computer, seperti LAN dan internet, memungkinkan untuk menyediakan informasi secara cepat. Ini salah satu alasan perusahaan atau organisasi mulai membuat LAN untuk sistem informasinya dan menghubungkan LAN tersebut ke internet.

Terhubungnya LAN atau computer ke internet membuka potensi adanya lubang keamanan (*security hole*) yang tadinya bisa ditutupi dengan mekanisme keamanan secara fisik. Ini sesuai dengan ungkapan bahwa kemudahan (kenyamanan) mengakses sistem informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri. Semakin tinggi tingkat keamanan semakin sulit (tidak nyaman) untuk mengakses informasi.

2.2 *Watermarking*

2.2.1 Digital *watermarking*

Digital *watermarking* adalah suatu teknik untuk menyembunyikan pesan seperti hak cipta pada data digital yang meliputi audio, video dan gambar. Pesan tersembunyi tersebut berupa kumpulan *bit* yang disisipkan pada *bit-bit* data digital. Hal ini dilakukan untuk menghindari atau mencegah modifikasi data digital atau menjaga keaslian dari suatu data digital.

2.2.2 Sejarah *watermarking*

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

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

2.2.3 Perbedaan *watermarking* dengan *steganografi*

Watermarking merupakan aplikasi dari *steganografi*, namun ada perbedaan antara keduanya yaitu :

1. Jika pada *steganografi* informasi rahasia di sembunyikan kedalam media digital dimana media penampung tidak berarti apa-apa.
2. Melainkan pada *watermark*ing media penampung untuk penyembunyian data sangat berarti apabila media penampung lebih kecil dari data yang disisipkan maka proses *watermark* tidak bisa dilakukan.

2.2.4 Fungsi utama *watermarking*

Berikut ini merupakan fungsi utama dari *watermarking* :

1. Proteksi Hak Cipta

   Tujuan *watermark* dalam perlindungan hak cipta adalah sebagai bukti otentik atas hak kepemilikan pencipta atas content yang dibuat atau diproduksinya

2. *Fingerprinting*

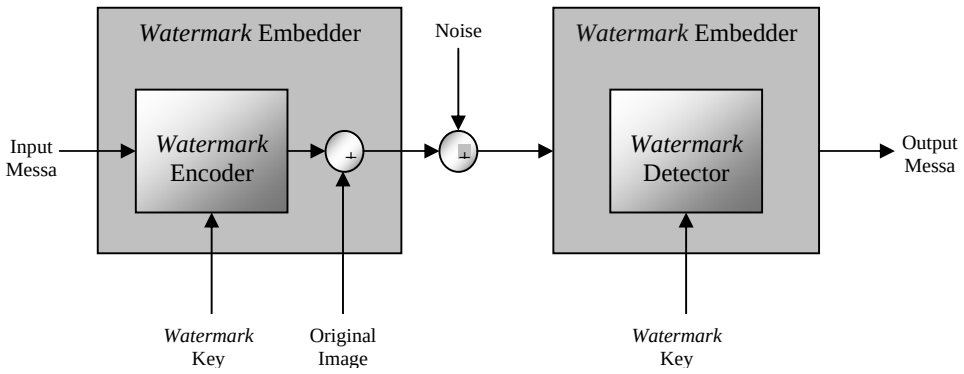
   Fungsi *watermark* pada fingerprinting mirip dengan serial number S/N. tujuan *watermark* adalah mengidentifikasi setiap penggunaan dan distribusi suatu content.

3. Proteksi terhadap penggandaan (*copy protection*)

   Watermark berfungsi melindungi *content* dari duplikasi dan pembajakan.

4. Autentikasi citra

   Watermark berfungsi dalam proses autentikasi, sehingga modifikasi dari suatu citra dapat terdeteksi



Gambar 2.1 Skema *watermarking*

Pada gambar 2.1, sistem *watermarking* terdiri dari dua komponen utama yaitu *watermark embedder* dan *watermark detector. Embedder* berfungsi untuk menanamkan data (*watermark*) pada suatu media digital, sedangkan *watermark detector* berfungsi melakukan ekstraksi data-data yang disembunyikan dengan atau tanpa menggunakan parameter atau key yang telah ditentukan sebelumnya.

2.2.5 Tipe *watermarking*

Watermark dapat digolongkan menjadi beberapa tipe berdasarkan tingkat *visibilitas* dari data yang disembunyikan (*watermark*), lokasi suatu *watermark* di domain ukuran data tersembunyi yang ditanamkan, tingkat ketahanan *watermark* terhadap suatu serangan dan distorsi serta proses ekstraksi.

1. *Visibilitas*

   Berdasarkan criteria visibilitas, *watermark* dapat digolongkan menjadi 2 jenis yaitu :

   a. *Perceptible* : *watermark* dapat terlihat oleh mata manusia secara langsung
   b. *Imperceptible* : *watermark* tidak dapat terlihat oleh mata manusia secara langsung.

2. *Domain*

   Lokasi peletakan data *watermark* terdiri dari dua jenis yaitu :

   a. *Domain Pixel* : *watermark* ditanamkan dengan melakukan modifikasi pada *pixel-pixel* dari suatu media.

b. *Domain* Frekuensi (*transformasi*) : *Watermark* ditanamkan pada *koefisien* hasil transformasi. *Domain* frekuensi diperoleh dengan melakukan *transformasi* citra.

3. *Robustness*

Berdasarkan tingkat ketahanan suatu *watermark* terhadap serangan dan distorsi maka *watermark* dapat digolongkan menjadi 3 jenis yaitu :

a. *Fragile* : *watermark* tidak tahan terhadap serangan dan distorsi. Tipe ini dapat digunakan dalam autentikasi. Jika suatu *watermark* tidak terdeteksi atau salah maka media telah mengalami perubahan atau tidak asli lagi.
b. *Semi-fragile* : *watermark* tahan terhadap beberapa serangan dan distorsi yang telah didefinisikan sebelumnya.
c. *Robust* : *watermark* tahan terhadap usaha-usaha untuk menghilangkan *watermark* dan tahan terhadap distorsi

3. *Ekstraksi*

Berdasarkan proses deteksi *watermark* atau proses ekstraksi *watermark*ing dapat digolongkan menjadi tiga jenis, yaitu :

a. *Blind* : pada proses ekstraksi data sistem *blind watermarking* tidak membutuhkan video atau media aslinya, yang dibutuhkan hanyalah suatu kunci atau parameter-parameter untuk melakukan ekstraksi.
b. *Semi-blind* : proses ekstraksi dilakukan dengan menggunakan suatu kunci dan juga data *watermark*.

c. *Non-blind* : proses ekstraksi dilakukan dengan menggunakan video asli atau parameter-parameter yang telah ditentukan (key).

2.2.6 *Watermarking* untuk pelabelan hak cipta

Masalah Hak Cipta dari dahulu sudah menjadi hal yang utama dalam segala ciptaan manusia, ini digunakan untuk menjaga *originalitas* atau *kreatifitas* pembuat akan hasil karyanya. Hak cipta terhadap data-data digital sampai saat ini belum terdapat suatu mekanisme atau cara yang handal dan efisien, dikarenakan adanya berbagai faktor-faktor tadi (faktor-faktor yang membuat data digital banyak digunakan). Beberapa cara yang pernah dilakukan oleh orang-orang untuk mengatasi masalah pelabelan hak cipta pada data digital, antara lain:

1. *Hearder Marking*; dengan memberikan keterangan atau informasi hak cipta pada header dari suatu data digital.
2. *Visible Marking*; merupakan cara dengan memberikan tanda hak cipta pada data digital secara eksplisit.
3. *Encryption*; mengkodekan data digital ke dalam representasi lain yang berbeda dengan representasi aslinya (tetapi dapat dikembalikan ke bentuk semula) dan memerlukan sebuah kunci dari pemegang hak cipta untuk mengembalikan ke representasi aslinya.
4. *Copy Protection*; memberikan proteksi pada data digital dengan membatasi atau dengan memberikan proteksi sedemikian rupa sehingga data digital tersebut tidak dapat diduplikasi.

Cara-cara tersebut diatas memiliki kelemahan tersendiri, sehingga tidak dapat banyak diharapkan sebagai metoda untuk mengatasi masalah pelabelan hak citpa ini. Contohnya :

1. *Header Marking*; Dengan menggunakan software sejenis Hex Editor, orang lain dengan mudah membuka file yang berisi data digital tersebut, dan menghapus informasi yang berkaitan dengan hak cipta dan sejenisnya yang terdapat di dalam header file tersebut.
2. *Visible Marking*; Penandaan secara eksplisit pada data digital, memang memberikan sejenis tanda semi-permanen, tetapi dengan tersedianya software atau metoda untuk pengolahan, maka dengan sedikit ketrampilan dan kesabaran, tanda yang semipermanen tersebut dapat dihilangkan dari data digitalnya. (lihat Gambar 3.)
3. *Encryption*; Penyebaran data digital dengan kunci untuk decryption tidak dapat menjamin penyebarannya yang legal. Maksudnya setelah data digital terenkripsi dengan kuncinya telah diberikan kepada pihak yang telah membayar otoritas (secara legal), maka tidak dapat dijamin penyebaran data digital yang telah terdekripsi tadi oleh pihak lain tersebut.
4. *Copy Protection*; Proteksi jenis ini biasanya dilakukan secara hardware, seperti halnya saat ini proteksi hardware DVD, tetapi kita ketahui banyak data digital saat ini tidak dapat diproteksi secara hardware (seperti dengan adanya Internet) atau dengan kata lain tidak memungkinkan dengan adanya proteksi secara hardware.

Dengan demikian, kita memerlukan suatu cara untuk mengatasi hal yang berkaitan dengan pelanggaran hak cipta ini, yang memiliki *sifat-sifat* seperti :

1. *Invisible atau inaudible*; Tidak tampak (untuk data digital seperti citra, video, text) atau tidak kedengaran (untuk jenis audio) oleh pihak lain dengan menggunakan panca indera kita (dalam hal ini terutama mata dan telinga manusia).
2. *Robustness*; Tidak mudah dihapus/diubah secara langsung oleh pihak yang tidak bertanggung jawab, dan tidak mudah terhapus/terubah dengan adanya proses pengolahan sinyal digital, seperti kompresi, filter, pemotongan dan sebagainya.
3. *Trackable*; Tidak menghambat proses penduplikasian tetapi penyebaran data digital tersebut tetap dapat dikendalikan dan diketahui.

Teknik *watermarking* tampaknya memiliki ketiga sifat-sifat diatas, karena faktor-faktor *invisibility* dan *robustness* dapat kita atur, dan data yang ter*watermark* dapat diduplikasi seperti layaknya data digital. *Watermarking* sebagai metoda untuk pelabelan hak cipta dituntut memiliki berbagai kriteria (ideal) sebagai berikut agar memberikan unjuk kerja yang bagus:

1. Label hak cipta yang unik mengandung informasi pembuatan, seperti nama, tanggal, dst, atau sebuah kode hak cipta seperti halnya ISBN (*International Standard for Book Notation*) pada buku-buku.

2. Data terlabel tidak dapat diubah atau dihapus (*robustness*) secara langsung oleh orang lain atau dengan menggunakan software pengolahan sinyal sampai tingkatan tertentu.
3. Pelabelan yang lebih dari satu kali dapat merusak data digital aslinya, supaya orang lain tidak dapat melakukan pelabelan berulang terhadap data yang telah dilabel.

Berbagai pengolahan sinyal digital yang mungkin dilakukan terhadap berbagai tipe data digital, antara lain:

1. Untuk Citra
    a. Filter (seperti blur).
    b. Konversi DA/AD.
    c. Crop (Pemotongan), Scaling, Rotasi, Translasi.
    d. Kompresi loosy (contohnya JPEG).
    e. Konversi Format.
    f. Perubahan Tabel Warna.

2. Untuk Video
    a. Crop.
    b. Kompresi loosy (contohnya MPEG).
    c. Konversi Format.
    d. Konversi DA/AD.

3. Untuk Audio
    a. Crop, filter, Equalisasi
    b. Kompresi loosy (contohnya MP3).
    c. Konversi Sample Rate, Format.
    d. Konversi DA/AD.
    e. Pengaruh Echo, Noise, dan Sinyal lain.

2.2.7 Aplikasi *watermarking*

Watermarking sebagai suatu teknik penyembunyian data pada data digital lain dapat dimanfaatkan untuk berbagai tujuan seperti:

a. *Tamper-proofing*; *watermarking* digunakan sebagai alat untuk mengidentifikasikan atau alat indicator yang menunjukkan data digital (host) telah mengalami perubahan dari aslinya.
b. *Feature location*; menggunakan metoda *watermark*ing 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.

2.3 Video

Video adalah teknologi untuk menangkap, merekam, memproses, mentransmisikan dan menata ulang gambar bergerak. Biasanya menggunakan film seluloid, sinyal elektronik, atau media digital yang berkaitan dengan “penglihatan dan pendengaran”.

Aplikasi video pada multimedia mencakup banyak aplikasi

-Entertainment : roadcast TV, VCR/DVD recording

-Interpersonal : video telephony, video conferencing

-Interactive : windows

Digital video adalah jenis sistem video recording yang bekerja menggunakan sistem digital dibandingkan dengan analog dalam hal representasi videonya. Biasanya digital video direkam dalam tape, kemudian didistribusikan melalui optical disc, misalnya VCD dan DVD.

2.3.1 *AVI*

Audio Video Interleave, biasa disingkat AVI, adalah format file multimedia ynag diperkenalkan oleh microsoft pada tahun 1992. File AVI dapat mengandung audio dan video dalam suatu media yang memungkinkan audio dan video dimainkan bersamaan. Seperti *DVD,* file AVI mendukung *streaming* , baik audio dan video, walaupun jarang dilakukan. Hampir semua file AVI menggunakan format ekstensi .AVI. File-file ini didukung oleh microsoft dan disebut “AVI 2.0”.

2.4 Citra digital

Citra merupakan fungsi intensitas dalam bidang dua dimensi. Intensitas yang dimaksud berasal dari sumber cahaya. Pada hakekatnya citra yang dilihat oleh mata manusia terdiri atas berkas-berkas cahaya yang dipantulkan oleh benda-benda di sekitar kita.

Suatu citra digital adalah suatu gambar kontinu yang diubah dalam bentuk diskrit, baik koordinat maupun intensitas cahayanya. Kita dapat menganggap suatu citra digital sebagai suatu matriks dimana indeks baris dan kolomnya menyatakan koordinat sebuah titik pada citra tersebut dan masing-masing elemennya menyatakan intensitas cahaya pada titik tersebut. Suatu titik pada sebuah citra digital sering disebut sebagai “image-element” (elemen citra) “picture-element” (elemen gambar) ataupun “*pixel*”.

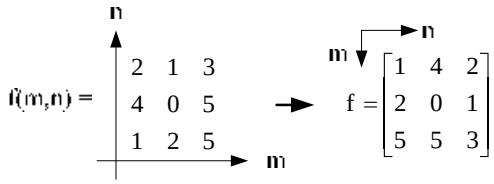
Untuk mengubah suatu citra kontinu ke dalam suatu representasi numerik dilakukan dengan proses digitalisasi oleh suatu *digitizer*, misalnya *scanner*, sehingga citra ini dapat diproses oleh sebuah komputer.

Digitalisasi sebuah citra dilakukan baik terhadap ruang (koordinat (x,y)), maupun terhadap skala keabuannya (f(x,y)). Proses digitalisasi koordinat (x,y) dikenal sebagai "pencuplikan citra" *(image sampling)*, sedangkan proses digitalisasi skala keabuan f(x,y) disebut sebagai "kuantisasi derajat keabuan" *(grey-level quantization)*.

Sebuah citra kontinu f(x,y) akan didekati oleh cuplikan-cuplikan yang seragam jaraknya dalam bentuk matriks MxN, M adalah baris dan N adalah kolom. Nilai elemen-elemen matriks menyatakan derajat keabuan citra, sebangkan posisi elemen tersebut (dalam baris dan kolom) menyatakan koordinat titik-titik (x,y) dari citra. Bentuk matriks di bawah ini dikenal sebagai suatu citra digital.

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & \dots & f(1,N-1) \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ f(M\text{-}1,0) & . & \dots & f(M-1,N-1) \end{bmatrix}$$

Matriks di atas dapat disajikan dalam bentuk 2 dimensi dalam sistem koordinat Cartesius dengan memutar posisi matriks di atas sejauh 90° derajat searah jarum jam.



Sedangkan derajat keabuan [0,L] dibagi kedalam G selang dengan panjang selang yang sama, yaitu: $\mathbf{G = 2^m}$ dimana m adalah kedalaman *bit* dan m bilangan bulat positif, bila hal ini diterapkan pada penyimpanan maka sebuah citra digital membutuhkan sejumlah b *bit*, dengan :

$$\mathbf{b = M \times N \times m}$$

Dalam suatu proses pencuplikan dan kuantisasi sering terjadi permasalahan, yaitu jumlah cuplikan dan derajat keabuan yang diperlukan untuk memperoleh suatu citra yang “baik”, makin tinggi nilai MxN dan m, maka citra kontinu f(x,y) akan makin didekati oleh citra digital yang dihasilkan. Tapi hal ini seringkali dibatasi oleh kemampuan hardware dari suatu komputer.

2.4.1 *BMP*

BMP atau *DIB* (*device independent bitmap*), adalah sebuah format grafik yang digunakan secara internal oleh microsoft windows dan subsistem OS/2, dan sering digunakan sebagai format file grafik sederhana pada *flatform-flatform* tersebut.

Gambar secara umum disajikan dalam ketajaman warna 2 (1-*bit*), 16 (4-*bit*), 256 (8-*bit*), 65.536 (16-*bit*), 16.7 juta (24-*bit*) warna (*bit-bit* ini mempresentasi *bit-bit* per-*pixel*). Sebuah gambar 8-*bit* juga dapat diubah ke warna *grayscale* disamping warna indeks. Sebua *channel alpha* (untuk warna transparan)

boleh disajikan dalam *file* terpisah, dimana sama dengan gambar *grayscale*. Versi 32-*bit* dengan *channel alpha* terintegrasi telah diperkenalkan oleh Windows XP dan digunakan untuk sistem *login* dan *theme*.

Umumnya file *BMP* menggunakan model warna *RGB.* Pada model ini sebuah warna terbentuk dari campuran intensitas yang berbeda (bervariasi dari 0 sampai 255), warna merah (R), hijau (G), dan biru (B). Dengan kata lain sebuah warna akan didefinisikan menggunakan 3 nilai, yaitu R, G dan B. Blok dari *bit* mendeskripsikan gambar secara *pixel* per *pixel*. *Pixel* disajikan mulai dari sudut kiri bawah berjalan dari kiri ke kanan dan kemudian baris per baris dari bawah ke atas. Setiap *pixel* dideskripsikan menggunakan satu atau lebih *bit*.

2.5 Video *watermarking*

2.5.1 Video *watermarking secara umum*

Video *watermarking* adalah upaya penyembunyikan informasi lewat konten video digital, tujuan utamanya adalah mengendalikan penyebaran dari konten video digital tersebut, dan membuat otorisasi dari pembuat video tersebut. Hal ini erat kaitannya dengan hak atas kekayaan intelektual, dan hak atas karya cipta. Beberapa teknik yang bisa dilakukan dalam video *watermark*ing adalah *Robust* dan *Blind* Video *watermark*ing.

a. *Robust watermarking*

Robust watermarking adalah sebuah sistem *watermark* yang tangguh dari serangan-serangan yang biasa dilakukan untuk mengagalkan pengungkapan dari *watermark. Robustness* dari sebuah *watermark* bisa ditentukan dengan mudah tetapi sulit untuk menilai kualitasnya. Sebuah sistem *watermark* yang *robust* adalah ketika sebuah pesan disisipkan tidak bisa dihapus atau diubah isinya kecuali dengan merusak isi data aslinya juga, sehingga *watermark* yang sudah disisipkan tidak dapat diungkap lagi.

b. *Blind watermarking*

Blind disini berarti untuk mengetahui ada tidaknya sebuah *watermark* yang disisipkan, atau ketika ingin mengungkap sebuah *watermark* tidak perlu adanya sebuah video asal sebelum *diwatermark*. Ada beberapa kasus dimana *blind watermarking* harus diterapkan, misalnya pada *video on demand*, *pay-per-view* atau siaran TV kabel lainnya. Tidaklah mungkin menyimpan keseluruhan konten video dalam sistem waktu nyata (video streaming), sehingga *watermark* harus bisa didteksi dari segmen manapun yang ada dalam konten digital tersebut.

Dan dalam penelitian tugas akhir ini data digital yang akan disisipkan kedalam video digital adalah citra digital.

2.5.2 Aspek yang perlu diperhatikan dalam *watermarking* pada video digital

a. Ketidaktampakan *watermark* citra diam dalam video.
b. Ketidaktampakkan *watermark* dalam frame yang berhenti.
c. Penyisipan *watermark* yang sama dalam frame, mengakibatkan mudah diserang.
d. Penekanan kepada frame-frame yang berurutan dalam sebuah cuplikan video yang akan diberi *watermark*, *attacker* bisa mendapatkan informasi dari kedua frame yang bersesuaian.
e. Kapasitas *watermark* dalam video, tentukan batas-batas kritisnya. Dimana video tidak dapat menampung berkas berukuran tertentu.
f. Sinkronisasi video dan audio setelah di*watermark* tetap menjadi pertimbangan, seharusnya setelah disisipi *watermark*, tidak terjadi ketidaksesuaian antara video, audio juga subtitle (optional) pada video yang di*watermark*.

2.6 Perhitungan PSNR

Perhitungan kualitas video digital yang merupakan hasil modifikasi, terhadap video digital yang asli, dapat dilakukan dengan menghitung nilai MSE (*Mean Square Error*) dan juga nilai PSNR (*Peak Signal-to-noise ratio*). Perhitungan nilai MSE dari video digital berukuran N x M, dilakukan sesuai dengan rumus berikut:

$$MSE = \frac{1}{N.M}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\left[\left| f(i,j) - f'(i,j)\right|^2\right] \qquad \textbf{(2.1)}$$

f(i,j) menyatakan citra digital yang asli sebelum dikompresi, sedangkan *f'(i,j)*, merupakan citra digital hasil kompresi nilai MSE yang besar, menyatakan bahwa penyimpangan atau selisih antara video hasil modifikasi dengan video aslinya cukup besar. Sedangkan untuk perhitungan nilai PSNR, dapat dilakukan dengan rumus berikut:

$$PSNR = 10\log\left(\frac{(255)^2}{MSE}\right) \qquad \textbf{(2.2)}$$

Semakin besar PSNR, maka kualitas video hasil modifikasi akan semakin baik, sebab tidak banyak data yang mengalami perubahan, dibandingkan aslinya.

2.7 Teknik penyembunyian data

2.7.1 *LSB* (*Least Significant Bit*)

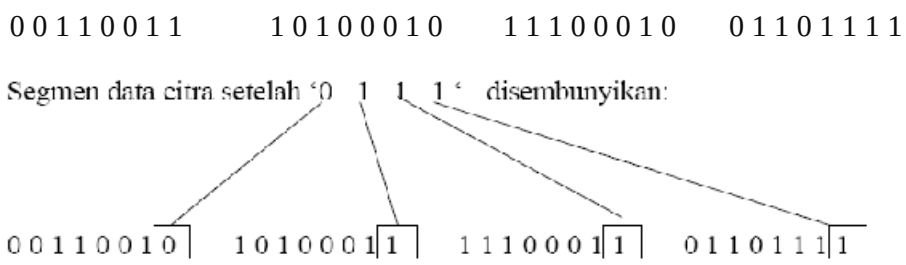
LSB (Least Significant Bit) Coding. Metoda ini merupakan metoda yang sederhana. Metoda ini akan mengubah nilai LSB (*Least Significant Bit*) komponen luminansi atau warna menjadi *bit* yang bersesuai dengan *bit* label yang akan disembunyikan. Memang metoda ini akan menghasilkan video rekontruksi yang sangat mirip dengan aslinya, karena hanya mengubah nilai *bit* terakhir dari data. Metoda ini paling mudah diserang, karena bila orang lain tahu maka tinggal membalikkan nilai dari LSB-nya maka data label akan hilang seluruhnya.

1. Penyembunyian data dilakukan dengan mengganti *bit-bit* data di dalam segmen citra dengan *bit-bit* data rahasia. Metode yang paling sederhana adalah metode **LSB** (*Least Significant Bit Modification*).
2. Pada susunan *bit* di dalam sebuah *byte* (1 *byte* = 8 *bit*), ada *bit* yang paling berarti (*most significant bit* atau *MSB*) dan *bit* yang paling kurang berarti (*least significant bit* atau *LSB*).
3. Perhatikan contoh sebuah susunan *bit* pada sebuah *byte*:



Bit yang cocok untuk diganti adalah *bit LSB*, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan 6 *byte* tersebut menyatakan warna merah, maka perubahan satu *bit* LSB tidak mengubah warna merah tersebut secara berarti. Lagi pula, mata manusia tidak dapat membedakan perubahan yang kecil.

4. Misalkan segmen data citra sebelum perubahan:



5. Untuk memperkuat teknik penyembunyian data, *bit-bit* data rahasia tidak digunakan mengganti *byte-byte* yang berurutan, namun dipilih susunan

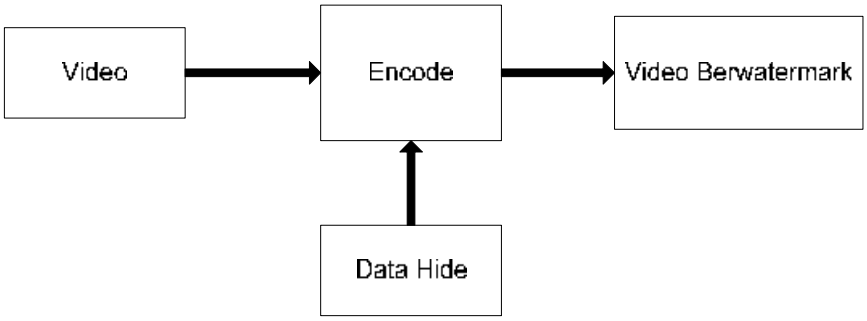
byte secara acak. Misalnya jika terdapat 50 *byte* dan 6 *bit* data yang akan disembunyikan, maka maka *byte* yang diganti *bit LSB*-nya dipilih secara acak, misalkan *byte* nomor 36, 5, 21, 10, 18, 49.

6. Bilangan acak dapat dibangkitkan dengan program *pseudorandom-number-generator* (*PRNG*). *PRNG* menggunakan kunci rahasia untuk membangkitkan posisi *pixel* yang akan digunakan untuk menyembunyikan *bit-bit*.
7. *PRNG* dibangun dalam sejumlah cara, salah satunya dengan menggunakan algoritma kriptografi berbasis blok (*block cipher*). Tujuan dari enkripsi adalah menghasilkan sekumpulan bilangan acak yang sama untuk setiap kunci enkripsi yang sama. Bilangan acak dihasilkan dengan cara memilih *bit-bit* dari sebuah blok data hasil enkripsi.

2.7.2 Penyisipan *watermark* dan pengungkapan *watermark*

a. Penyisipan *Watermark*

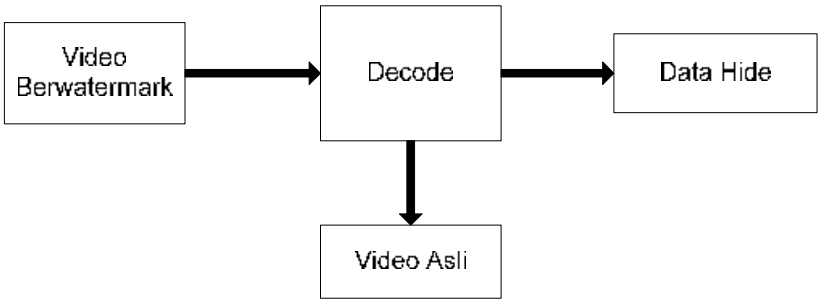
Proses pennyisipan data kedalam video disebut enkode dan ditunjukan pada gambar 2.2 dibawah ini.



Gambar 2.2 Proses penyisipan

b. Pengungkapan *watermark*

Pengungkapan *watermark* dilakukan untuk membuktikan stastus kepemilikan video digital yang disengketakan. Teknik pengungkapan video disebut decode ditunjukan pada gambar 2.3.



Gambar 2.3 Proses pengungkapan *watermark* pada video digital.

2.8 *Coding* dan *decoding*

Coding merupakan teknik untuk mendapatkan kode-kode tertentu (*encoder*), dari kode-kode tersebut dapat diaplikasikan untuk pemampatan data dan keamanan data. Dari data-data yang telah dikodekan tersebut, format-format isi dari data tersebut berbentuk kode-kode yang tidak bisa kita baca. Agar kode-kode tersebut bisa kita baca maka kita kodekan ulang data tersebut, hal ini dikenal dengan decoding (*decoder*).

Secara umum pemampatan data merupakan merubah suatu simbol-simbol menjadi suatu kode-kode. Pemampatan dikatakan efektif jika ukuran perolehan kode-kode tersebut sangat kecil dibandingkan dengan ukuran kode simbol aslinya. Dari suatu kode-kode atau simbol-simbol dasar suatu model akan dinyatakan dalam kode khusus. Secara model sederhana suatu kumpulan data dan aturan-aturan untuk memproses masalah suatu simbol-simbol untuk menentukan suatu kode-kode sebagai hasil keluaran.

Sebaliknya proses *decoding*, yaitu proses pengembalian kode-kode yang telah dibuat menjadi simbol-simbol yang kita kenal. Proses decoder ini membaca header dari kode-kode yang berisi informasi simbol dan jumlah simbol yang digunakan, setelah pembacaan header proses enkoder akan dilakukan dari *bit* yang terpanjang sampai *bit* terpendek.