BAB II

LANDASAN TEORI

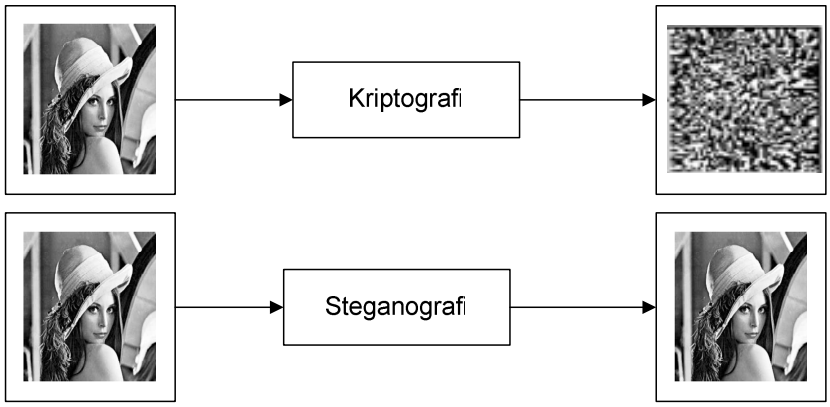
2.1 Steganography

Steganografi (*steganography*) berasal dari bahasa Yunani yaitu *Steganós* yang berarti menyembunyikan dan *Graptos* yang artinya tulisan sehingga secara keseluruhan artinya adalah tulisan yang disebunyikan. Secara umum steganografi merupakan salah satu cara untuk menyembunyikan suatu pesan rahasia (*hiding message*) di dalam data atau pesan lain yang tampak tidak mengandung apa-apa, sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia kecuali bagi orang yang mengerti kuncinya.

Steganografi membutuhkan dua properti: wadah penampung (*cover*) dan data rahasia yang akan disembunyikan. Steganografi *digital* menggunakan media *digital* sebagai *cover*, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video. Media yang telah disisipi data disebut *stegodata* atau *stegofile*. Proses penyembunyian data ke dalam media disebut penyisipan (*embedding*), sedangkan proses sebaliknya disebut ekstraksi (*extraction*).

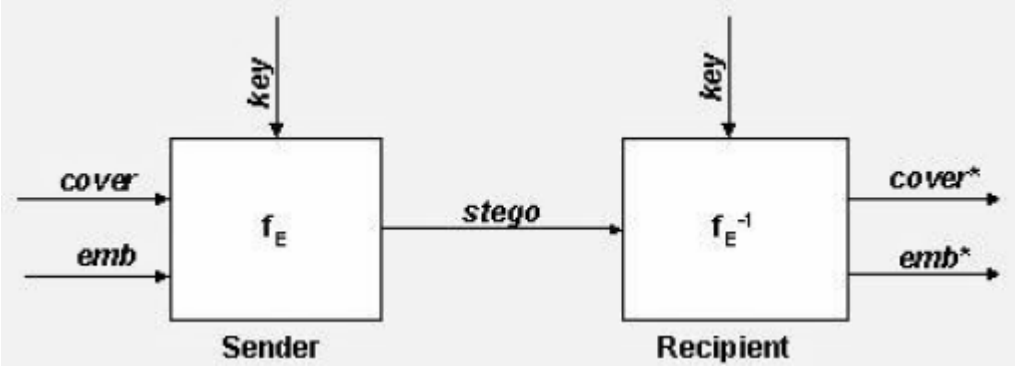
Dalam bidang keamanan komputer, steganografi berbeda dengan kriptografi dimana steganografi digunakan untuk menyembunyikan data rahasia saat enkripsi tidak dapat dilakukan atau bersamaan dengan enkripsi. Jadi, walaupun enkripsi berhasil dipecahkan (decipher) pesan / data rahasia tetap tidak terlihat dan pesan “disamarkan” dalam bentuk yang relative “aman” sehingga tidak terjadi

kecurigaan itu. Sedangkan pada kriptografi, dimana pihak ketiga dapat mendeteksi adanya data (*chipertext*) karena hasil dari kriptografi berupa data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan tetapi dapat dikembalikan ke bentuk semula. Ilustrasi mengenai perbedaan kriptografi dan steganografi dapat dilihat pada Gambar 2.1.



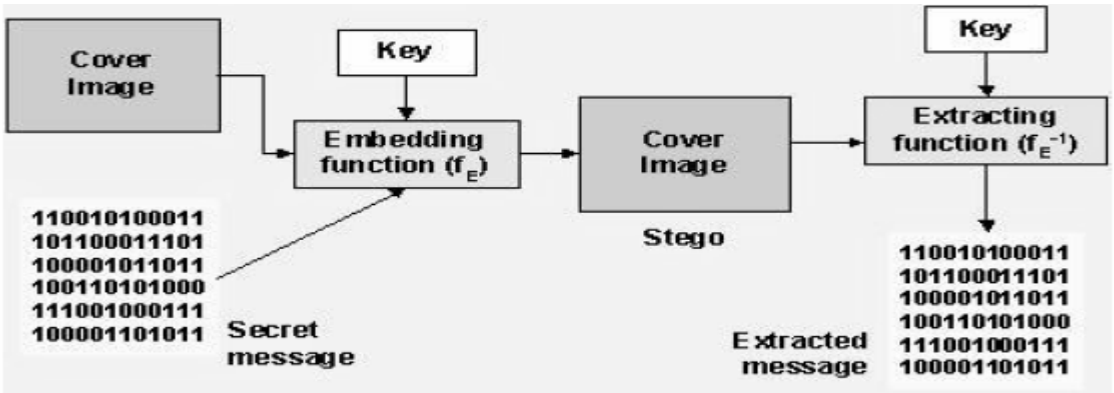
Gambar 2.1 Ilustrasi kriptografi dan steganografi

Steganografi juga membahas bagaimana sebuah pesan dapat disisipkan ke dalam sebuah berkas media sehingga pihak ketiga tidak menyadarinya. Steganografi memanfaatkan keterbatasan sistem indera manusia seperti mata dan telinga. Dengan adanya keterbatasan inilah metode steganografi ini dapat diterapkan pada berbagai media *digital*. Hasil keluaran dari steganografi ini memiliki bentuk persepsi yang sama dengan bentuk aslinya, tentunya persepsi di sini sebatas oleh kemampuan indera manusia, tetapi tidak oleh komputer atau perangkat pengolah *digital* lainnya.



Gambar 2.2 Sistem steganography

Gambar 2.2 menunjukkan sebuah sistem *steganography* umum dimana dibagian pengirim pesan (**sender**), dilakukkan proses *embedding* (**fE**) pesan yang hendak dikirim secara rahasia (**emb**) ke dalam data cover sebagai tempat meyimpannya (**cover**), dengan menggunakan kunci tertentu (**key**), sehingga dihasilkan data dengan pesan tersembunyi di dalamnya (**stego**). Di bagian penerima pesan (**recipient**), dilakukkan proses *extracting* (**fE-1**) pada **stego** untuk memisahkan pesan rahasia (**emb**) dan data penyimpan (**cover**) tadi dengan menggunakan kunci yang sama seperti pada proses *embedding* tadi. Jadi hanya orang yang tahu kunci ini saja yang dapat mengekstrak pesan rahasia tadi. Proses tadi dapat direpresentasikan secara lebih jelas pada gambar 2.3 di bawah.



Gambar 2.3 Graphical Version of a Steganographic System

2.1.1 Sejarah Steganografi

Steganografi sudah digunakan sejak dahulu kala untuk kepentingan politik, militer, diplomatik, serta untuk kepentingan pribadi sebagai alat. Beberapa contoh penggunaan steganografi:

1. Steganografi pada tubuh budak: Pada jaman Yunani Kuno, Herodotus (sejarawan Yunani) menyampaikan pesan dengan cara mencukur kepala budak dan mentato kepalanya dengan pesan tersebut. Kemudian saat rambutnya tumbuh kembali, budak dikirimkan pada tempat tujuan dan saat rambutnya kembali digunduli maka pesan akan terbaca.
2. Steganografi dalam lapisan lilin: Masih pada jaman Yunani Kuno, pesan rahasia di ukir pada kayu kemudian diberi lapisan lilin untuk menutupi pesan tersebut, dengan begitu pesan dapat disampaikan tanpa menimbulkan kecurigaan.
3. Steganografi pada kertas: Pada Perang Dunia II, pemerintah Amerika Serikat menulis pesan rahasia pada tentaranya yang di tawan oleh Jerman dengan menggunakan tinta tak terlihat di atas atau di bagian kosong pesan lainnya dan untuk mendeteksinya digunakan air.
4. Steganografi dengan *microdots*: Masih pada Perang Dunia II, agen mata-mata menggunakan *microdots* untuk mengirimkan informasi. Penggunaan teknik ini biasa digunakan pada *microfilm* chip yang harus diperbesar sekitar 200 kali.
5. Steganografi dunia *digital*: Pada suatu pengarahan yang dilakukan oleh FBI pada akhir September 2001, asisten direktur FBI, Ron Dick menyatakan

kemungkinan para pembajak pesawat pada serangan 11 September ke gedung *World Trade Center* menggunakan teknologi internet seperti *website* perusahaan palsu atau *website* porno, *e-mail*, *chat rooms*, *bulletin boar*ds untuk mengkoordinasi serangan.

2.1.2 Steganalysis

Steganalysis merupakan suatu teknik atau yang digunakan untuk mengungkapkan keberadaan pesan tersembunyi atau tersamar dari steganografi. Steganalysis menjadi suatu misteri tersendiri untuk dapat diketahui bagaimana teknik untuk melakukan proses dekripsi atau pemecahan atau penemuan pesan tersebut. Terdapat beberapa *software* yang dapat melakukan analisa adanya penggunaan teknik steganografi. Dalam praktiknya cara pemecahan teknik apa yang digunakan dalam steganalysis sendiri secara empirik berkisar diantara :

1. Menganalisa dari perubahan yang dilakukan terhadap meta data *file* tersebut.
2. Menganalisa dari ciri-ciri *file* telah menggunakan *software* tertentu untuk steganografi.
3. Membandingkan *file* asli, lalu dicari perbedaannya dan pola yang digunakan sehingga dengan cara ini bukan saja dapat diketahui *file* telah mengalami proses steganografi dapat pula diketahui pesan yang disembunyikan.

Tetapi teknik steganalysis tidak dapat digunakan untuk mengetahui pesan yang disembunyikan bila ternyata pesan tersebut mengalami kriptografi atau pengkodean pesan lagi. Jadi cara yang baik untuk melakukan steganografi adalah dengan melakukan asumsi bahwa orang akan tahu bahwa ada pesan yang

disembunyikan sehingga dilakukan pengamanan lagi dengan kriptografi. Pemilihan kriptografi juga jangan dilakukan dengan sembarangan dan gunakan yang sudah terbukti keampuhannya seperti 3DES dan SHA-1.

2.1.3 Manfaat Stenaganography

Steganography adalah sebuah pisau bermata dua, ia bisa digunakan untuk alasan-alasan yang baik, tetapi bisa juga digunakan sebagai sarana kejahatan. Steganography juga dapat digunakan sebagai salah satu metode watermarking pada image untuk proteksi hak cipta, seperti juga digital watermarking (fingerprinting). Steganography juga dapat digunakan sebagai pengganti hash.

Dan yang terutama, seperti disebutkan sebelumnya, steganography dapat digunakan untuk menyembunyikan informasi rahasia, untuk melindunginya dari pencurian dan dari orang yang tidak berhak untuk mengetahuinya. Sayangnya, steganography juga dapat digunakan untuk mencuri data yang disembunyikan pada data lain sehingga dapat dikirim ke pihak lain, yang tidak berhak, tanpa ada yang curiga. Steganography juga dapat digunakan oleh para teroris untuk saling berkomunikasi satu dengan yang lain. Sehubungan dengan keamanan sistem informasi, steganography hanya merupakan salah satu dari banyak cara yang dapat dilakukan untuk menyembunyikan pesan rahasia. Steganography lebih cocok digunakan bersamaan dengan metode lain tersebut untuk menciptakan keamanan yang berlapis. Sebagai contoh steganography dapat digunakan bersama dengan enkripsi. Windows dan Unix juga menggunakan steganography dalam mengimplementasikan hidden directory.

2.1.4 Faktor Penting Dalam Steganografi

Penyembunyian data rahasia ke dalam media *digital* mengubah kualitas media tersebut. Faktor penting dalam penyembunyian data diantaranya adalah:

1. *Fidelity*. Mutu media penampung tidak jauh berubah. Setelah penambahan data rahasia pengamat tidak mengetahui kalau di dalam media tersebut terdapat data rahasia.
2. *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*). karena tujuan steganografi adalah menyembunyikan data, maka sewaktu-waktu data rahasia didalam media penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

2.1.5 Media Steganografi

Steganografi menggunakan sebuah *cover*, tujuannya sebagai kamuflase dari pesan yang sebenarnya. Banyak format berkas digital yang dapat dijadikan media untuk menyembunyikan pesan. Pada jaman modern seperti saat ini, steganografi biasanya dilakukan dengan melibatkan berkas-berkas seperti teks, citra, suara dan video.

2.1.6 Teknik Steganografi

Saat ini setidaknya terdapat 6 teknik steganografi, yaitu:

1. Teknik substitusi *(Substitution Techniques),* yaitu dengan melakukan substitusi piksel-piksel tertentu dari berkas *cover* dengan piksel-piksel informasi yang disimpan. Contohnya adalah metode BPCS (*Bit Plane*

Complexity Segmentation),metode LSB (*Least Significant Bit*).

2. Teknik Domain Transformasi *(Domain Transform Techniques),* yaitu dengan cara menyimpan informasi rahasia pada transformasi ruang (misalnya domain frekuensi) dari berkas *cover*. Contoh algoritma yang tergolong teknik ini adalah steganografi pada domain DCT *(Discrete Cosine Transform).*
3. Teknik Spread Spectrum *(Spread Spectrum Techniques),* ide dari teknik ini mengadopsi teknik *spread spectrum* pada saluran komunikasi. Dalam teknik ini informasi rahasia yang disimpan disebarkan pada suatu frekuensi tertentu dari berkas *cover.*
4. Teknik Statistik *(Statistical Techniques)* Dengan teknik ini data di *encoding* melalui pengubahan beberapa informasi statistik dari berkas *cover*. Berkas *cover* di bagi dalam blok-blok dimana setiap blok tersebut menyimpan satu piksel informasi rahasia yang disembunyikan. Jika piksel yang ditemukan pada suatu blok untuk menyimpan data adalah piksel T maka tidak dilakukan perubahan nilai piksel, jika sebaliknya maka dilakukan perubahan nilai piksel. Meskipun secara teoritis mungkin untuk dilakukan, pada kenyataannya teknik ini agak sulit untuk diimplementasikan.
5. Teknik Distorsi *(Distortion Techniques),* informasi yang hendak disembunyikan disimpan berdasarkan distorsi sinyal.
6. Teknik Pembangkitan Wadah *(Cover Generation Techniques),* Teknik ini menyembunyikan informasi rahasia dengan jalan (atau sejalan) dengan pembangkitan *cover*. Misalnya aplikasi pembangkitan teks.

2.1.7 Steganography pada Video

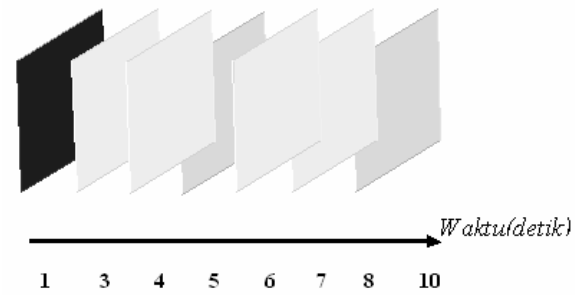
Seperti dikatakan sebelumnnya, video merupakan kumpulan dari image yang "bergerak", jadi sebagian besar metode yang digunakan pada image steganography dapat digunakan pada video steganography. Dapat dikatakan bahwa video steganography merupakan turunan dari image steganography. Pada video steganography ini, yang umum digunakan adalah metode *Bit Plane Complexity Segmentation* Hal ini dikarenakan modifikasi BPCS akan menghasilkan stego yang berukuran sangat besar sedangkan metode masking dan filtering akan mengubah tampilan visual dari video secara langsung. Untuk menyembunyikan pesan pada cover video, prinsipnya sama seperti pada image steganography. Pertama-tama dilakukan transformasi pada masing-masing frame image cover video untuk memperoleh koefisien-koefisien yang akan dipilih berdasarkan nilai treshold tertentu. Koefisien tersebut akan diganti dengan bit-bit data pesan yang akan disembunyikan. Setelah seluruh pesan di-embed, koefisien tadi ditransformasi balik untuk menghasilkan stego video. Untuk mengekstrak pesan dari stego video, prinsipnya juga sama seperti pada image steganography. Pertama-tama dilakukan transformasi pada masing-masing frame image stego video untuk memperoleh koefisien-koefisien yang akan dipilih berdasarkan nilai treshold tertentu. Koefisien tersebut akan merupakan bit-bit data pesan yang telah disembunyikan dan akan ditulis ke file output yang berisi pesan yang disembunyikan tersebut. Keuntungan dari video steganography adalah banyaknya data yang dapat disembunyikan di dalamnya, serta fakta bahwa video merupakan "streams" dari image-image menyebabkan adanya distorsi pada salah satu frame

image tidak akan dilihat dengan mudah dengan mata manusia. Akan tetapi, semakin banyak data pesan yang disembunyikan, bukan hal yang mustahil jika perubahan pada video menjadi semakin mudah terlihat.

2.2 Video

Video merupakan gabungan gambar-gambar mati yang dibaca berurutan dalam suatu waktu dengan kecepatan tertentu. Gambar-gambar yang digabung tersebut dinamakan *frame* dan kecepatan pembacaan gambar disebut dengan *frame rate*, dengan satuan *fps* (*frame per second*). Karena dimainkan dalam kecepatan yang tinggi maka tercipta ilusi gerak yang halus, semakin besar nilai frame rate maka akan semakin halus pergerakan yang ditampilkan.

Video pada dasarnya tersusun atas serangkaian *frame* yang ditunjukan pada gambar 2.4 Rangkaian *frame* tersebut ditampilkan pada layar dengan kecepatan tertentu, bergantung kepada laju *frame* yang diberikan (dalam *frame*/detik). Jika laju *frame* cukup tinggi, maka manusia dapat menangkap gambar per *frame* secara berkelanjutan seolah-olah melihat gambar bergerak



Gambar 2.4 Aliran *frame*

2.2.1 Fundamental Video

Pelayanan televisi di Eropa yang sekarang ini menyiarkan video pada suatu bingkai tingkat 25 Hz. Masing-Masing bingkai terdiri dari dua bidang dijalin, memberi suatu bidang tingkat 50 Hz. Bidang yang pertama dari tiap bingkai hanya berisi bentuk yang bernomor gasal bingkai (nomor, jumlah garis bingkai puncak garis satu). Bidang yang kedua hanya berisi genap bentuk yang dinomori bingkai dan *sample* kamera video 20 m setelah bidang yang pertama.

Dalam sistem video selain televisi, Di dalam video tidak dijalin, semua baris suatu bingkai adalah *sample* di saat tertentu yang sama pada waktunya. Merah, biru dan hijau (RGB) merupakan syarat yang berasal dari suatu kamera televisi berwama dapat dinyatakan seperti serian (Y) dan krominans (UV) komponen. Krominans Luas bidang mungkin dikurangi dengan serian tanpa mempengaruhi mutu gambar. Karena video definisi baku, CCIR rekomendasi 601 menggambarkan bagaimana komponen (YUV) syarat video dapat *digitised* dan *sample* untuk membentuk piksel terpisah. Istilah 4:2:2 dan 4:2:0 adalah sering digunakan untuk menguraikan struktur sampling gambaran digital. 4:2:2 krominans secara horisontal *subsample* dari suatu faktor dua relatif kepada serian 4:2:0 krominans secara horisontal dan tegak lurus *subsample* oleh suatu faktor dua relatif kepada serian.

Daerah aktif suatu bingkai televisi digital, sample menurut CCIR rekomendasi 601, adalah 720 piksel oleh 576 bentuk untuk suatu bingkai tingkat 25 Hz. Penggunaan 8 bit untuk masing-masing Y, U atau V piksel, bit yang tidak dimampatkan untuk serian 4:2:2 dan 4:2:0 dijelaskan sebagai berikut.

Serian 4:2:2

720 x 576 x 25 x 8 + 360 x 576 x 25 x (8 + 8) = 166 Mbit/s

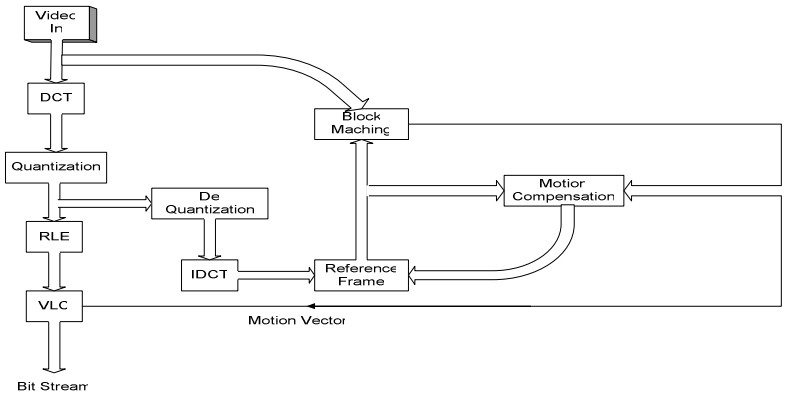
Serian 4:2:0

720 x 576 x 25 x 8 + 360 x 288 x 25 x (8 + 8) = 124 Mbit/s

MPEG 2 mampu untuk memampatkan bit tingkat *standard-definition* 4:2:0 video hingga sekitar 3-15 Mbit/S. Di bit yang lebih rendah ini mencakup, perusakan atau pelemahan diperkenalkan oleh MPEG-2 persandian dan memecahkan proses menjadi yang tak dapat disetujui. Karena penyiaran televisi *standard-definition* video terestrial digital, sedikit tingkat di sekitar 6 Mbit/S untuk menjadi kompromi baik antara mutu gambar dan efisiensi luas bidang transmisi.

2.2.2 Sekilas Kompresi Video

Pada proses *encoding* untuk data video, merupakan proses yang dilakukan oleh video encoder untuk mengubah sinyal video digital menjadi bit – bit stream untuk proses transmisi. Untuk memperjelas proses *encoding* dapat dilihat gambar 2.5 *encoder* pada gambar berikut ini.

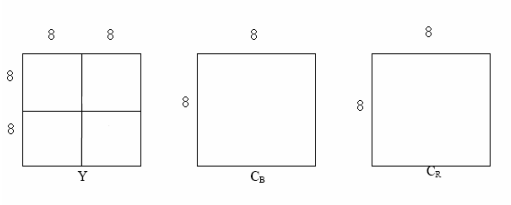


Gambar 2.5 *Encoder* kompresi

Penjelasan dari gambar di atas akan diuraikan sebagai berikut :

1. Video In

Format gambar yang digunakan dalam konferensi video ini adalah CIF (360 x 270 *pixel*). *Frame* video sebagai masukan dari tangkapan *webcam* dikelompokkan menjadi dua bagian, *frame* I dan *frame* P, untuk *frame* I masuk ke proses kompresi *Intraframe*, sedangkan untuk frame P masuk ke proses kompresi *Interframe*. *Frame* I dibagi – bagi menjadi sebuah *macroblocks* yang terdiri dari empat buah blok Y (*Luminance* / kecerahan) berukuran 8 x 8 *pixel*, sebuah blok Cb (*Chrominance Blue* / warna biru) berukuran 8 x 8 *pixel*, sebuah blok Cg (*Chrominance Green* / warna hijau) berukuran 8 x 8 *pixel* dan sebuah blok Cr (*Chrominance Red* / warna merah) berukuran 8 x 8 *pixel*. seperti yang ditunjukkan pada gambar 2.6 Kumpulan dari *macroblock* ini disebut sebagai sebuah *Group of Block* (GOB),



Gambar 2.6 *Macroblocks*

2. DCT

Pada proses DCT, masukan berupa matriks data dua dimensi NxN, merupakan nilai koefisien yang menyusun setiap blok, sedangkan keluarannya juga merupakan matriks dua dimensi.

3. *Quantization*

Keluaran proses DCT masuk ke proses kuantisasi dengan cara mengurangi jumlah bit yang diperlukan dengan menggunakan fungsi - fungsi *weighting* (pembobotan) yang dioptimalkan sehingga mendekati sistem visual manusia.

Kuantisasi dimaksudkan untuk menyederhanakan bobot angka - angka, yakni senilai 256 yang menunjukkan keseluruhan palet warna dari putih murni sampai hitam murni.

4. *De Quantization*

Proses ini dibutuhkan untuk mengembalikan data *frame* hasil kuantisasi ke bentuk semula agar dapat digunakan menjadi *frame* referensi bagi proses kompresi *interframe*.

5. IDCT

Proses ini sama seperti dekuantisasi, untuk mengembalikan data frame hasil proses DCT ke bentuk semula agar dapat digunakan menjadi *frame* referensi bagi proses kompresi *interframe*.

6. *Reference Frame*

Tempat penyimpanan hasil dekuantisasi dan IDCT dari proses sebelumnya (sebelum data dikodekan). *References frame* ini menjadi referensi bagi proses *interframe.*

7. *Motion Estimation*

Untuk P *frame*, dilakukan proses kompresi *interframe*, yaitu proses *motion estimation* atau estimasi gerak, karena hanya bagian kecil saja dari *frame* yang berubah bila dibandingkan dengan *frame* sebelum atau sesudahnya. Proses ini mengestimasi gerakan blok – blok antar *frame*, tiap blok dibandingkan dengan blok – blok berukuran sama, pada *frame* sebelumnya dengan melakukan pencocokan blok (*block matching)*. Proses ini dilakukan sampai seluruh *frame.*

8. *Prediction*

Proses ini dilakukan untuk memprediksi lokasi dari blok yang paling mirip atau *match* pada *frame* referensi (*reference frame*) dengan lokasi blok target (*target block*) pada *frame* sesudahnya. Perbedaan relatif posisi ini disebut vektor gerak (*motion vector*)

9. RLE (*Run Length Encoding*)

Hasil proses kuantisasi yang cenderung bernilai nol dan berulang secara berurutan, oleh RLE serangkaian simbol yang berurutan tersebut dikodekan menjadi suatu kode yang terdiri dari simbol tersebut dan jumlah perulangannya yang dibaca secara linier dengan metode *zig zag scanning* dari frekuensi terendah sampai frekuensi tertinggi.

10. VLC (*Video Length Coding*)

Setelah rangkaian simbol tersebut dikodekan, setiap kode memiliki panjang yang berbeda-beda. Oleh VLC kode yang jarang muncul dikodekan dengan kode yang panjang sedangkan yang sering muncul dikodekan dengan kode yang pendek. Dengan demikian, secara keseluruhan bit yang dibutuhkan menjadi lebih sedikit. Keluaran proses dari VLC bit-bit *stream frame* kemudian disimpan dalam *buffer* untuk disinkronkan dengan informasi dari *motion vector* yang merupakan keluaran dari proses *block macthing.* Hasil proses tersebut berupa *bit stream* yang telah terkodekan dan siap untuk ditransmisikan atau dikirimkan.

2.2.3 Jenis cover video

Di dalam video, terdapat tiga jenis gambar. Ini menggambarkan gaya ramalan yang mungkin digunakan untuk kode masing-masing blok.

***Intra* (*I-Pictures*)** adalah *coded* tanpa memandang lain gambaran. Tekanan moderat dicapai dengan mengurangi pemborosan mengenai ruang, tetapi bukan pemborosan sementara. Mereka dapat digunakan pada waktu tertentu untuk menyediakan akses menunjuk *bitstream* di mana memecahkan kode kaleng dimulai.

prediksi (*P-Pictures*) dapat menggunakan yang sebelumnya atau *P-Picture* untuk ganti-rugi gerakan dan mungkin digunakan sebagai suatu acuan untuk ramalan lebih lanjut . Masing-Masing blok di dalam suatu *P-Picture* dapat yang manapun diramalkan atau *intra-coded*. Dengan mengurangi pemborosan sementara dan mengenai ruang, *P-Pictures* penawaran meningkat tekanan yang dibandingkan ke *I-Pictures*.

***Bidirectionally-Predictive* (*B-Pictures*)** dapat menggunakan berikutnya dan yang sebelumnya atau *P-Pictures* untuk *motion-compensation*, dan menawarkan tingkat tekanan tertinggi. Masing-Masing blok di dalam suatu *B-Picture* dapat maju, mundur atau *bidirectionally* meramalkan atau *intra-coded*. Untuk memungkinkan ramalan mundur dari suatu bingkai masa depan, memesan lagi gambaran dari alami pajangan memesan untuk *bitstream* sedemikian sehingga *B-Picture* dipancarkan setelah gambar berikutnya dan yang sebelumnya acuan. Ini memperkenalkan suatu memesan lagi bergantung penundaan atas banyaknya berurutan *B-Pictures*.

Jenis gambar yang berbeda secara khas terjadi mengulangi urutan, memasukkan kelompok gambar atau GOP. Suatu GOP *packet* didalam visual adalah:

B1 B2 I3 B4 B5 P6 B7 B8 P9 B10 B11 P12

Bersesuaian *bitstream* adalah:

I3 B1 B2 P6 B4 B5 P9 B7 B8 P12 B10 B11

Suatu GOP struktur reguler dapat diuraikan dengan dua parameter: N, yang mana banyaknya gambaran didalam GOP, dan M, adalah pengaturan jarak *P-Pictures*. GOP memberi di sini diuraikan seperti N=12 dan M=3. MPEG-2 tidak meminta dengan tegas atas suatu GOP struktur reguler. Sebagai contoh, suatu *P-Picture* yang mengikuti suatu *shot-change* mungkin sangat buruk diramalkan karena gambar acuan untuk ramalan dengan sepenuhnya berbeda dari gambar diramalkan. Seperti itu, mungkin saja pengaruh baik bagi kode sebagai suatu *I-Picture* sebagai gantinya.

Karena mutu gambar dikodekan ditentukan, masing-masing penggunaan persandian menggambar hasil jenis adalah suatu jumlah berbeda bit. Didalam suatu urutan contoh khas, suatu *I-Picture coded* adalah tiga kali lebih besar dari suatu *P-Picture coded*, 50% lebih besar dari suatu *B-Picture coded*.

2.2.4 Sekilas Video Digital Editing

Sebelum muncul teknologi digital editing, semua proses penyuntingan dilakukan dengan menggunakan 1 player video dan 1 recorder video. Cara ini hanya mengijinkan transisi cut to cut saja. Lalu muncul penggunaan 2 player dan 1 recorder yang dilengkapi mixer, teknik penyuntingan ini menyediakan transisi dissolve. Teknologi editing seperti ini disebut **A/B roll editing** atau **Linear Editing**. Dengan teknologi editing yang lama, akibat sifat video yang linier, jika

pada saat editing ada satu segmen di tengah cerita yang ingin diperpanjang atau diperpendek maka seluruh rangkaian editing dibelakangnya harus diulang kembali.

Dengan hadirnya teknologi digital video editing, maka persoalan ini bisa diatasi dengan **Non-Linear Editing (NLE)**. Dengan metode editing ini video disimpan dalam harddisk terlebih dahulu sehingga bisa dilakukan proses editing yang lebih fleksibel. Satu segmen video bisa dipindahkan atau bisa dipakai secara berulang-ulang. Kita tinggal melakukan drag and drop klip video, gambar, dan audio. Selain video capture card, maka kita membutuhkan perangkat komputer yang memiliki spesifikasi yang cukup untuk melakukan proses capturing dan editing. Pemilihan processor (CPU), RAM (Random Access Memory), dan harddisk sebagai media penyimpanan perlu diperhatikan sesuai dengan kebutuhan kita. Untuk processor sangat dianjurkan untuk menggunakan processor yang memiliki kecepatan diatas 1 Ghz dan memiliki cache memory sebesar 512Kb. Demikian juga dengan memory atau RAM, sangat dianjurkan untuk melengkapi komputer kita dengan RAM bekapasitas minimal 256 Mb. Sedangkan kebutuhan media penyimpanan disesuaikan dengan durasi dari proyek video digital kita. Untuk format video NTSC (29.97 fps) dengan durasi 1 menit video dibutuhkan 1,5 GB, maka untuk durasi 1 jam kita membutuhkan penyimpanan sebesar 90 GB. Teknologi Non-Linear Editing (NLE) menggunakan software/aplikasi untuk melakukan proses capture dan editing.

2.2.5 Perbedaan Video Analog dan Video Digital

Analog video tersusun dari gelombang bersambung yang bervariasi, dengan kata lain nilai sinyal akan memiliki angka yang beragam tetapi terbatas pada batas maksimum dan minimum yang diijinkan. Sedangkan *digital video* ditransmisikan hanya berupa titik presisi yang dipilih pada interval dalam kurva. Tipe sinyal digital yang dapat dipakai oleh komputer kita adalah tipe *binary*. Data binary diwakili dengan angka 1 dan 0, angka 1 mewakili nilai maksimum dan angka 0 mewakili nilai minimum.

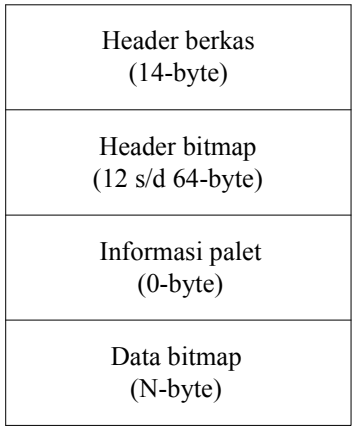
Digital video memiliki banyak kelebihan dibandingkan dengan analog video, yang paling penting adalah ketepatan yang tinggi dalam proses transmisi (*high fidelity*) dibandingkan dengan sinyal analog. Pada sinyal analog, saat penerimaan akhir transmisi akan sulit membedakan antara sinyal asli dan *noise* yang mungkin diperkenalkan selama transmisi. Transmisi yang diulang-ulang maka akumulasi noise tidak dapat dihindari. Lain halnya dengan sinyal digital yang dapat membedakan antara sinyal asli dengan noise. Sinyal digital juga dapat ditransmisikan berulang-ulang sebanyak yang kita inginkan tanpa mempengaruhi kualitasnya.

Dunia video kini telah mengalami perubahan dari analog ke digital. Perubahan ini terjadi pada setiap tingkatan industri. Pada konsumen rumahan dan perkantoran kita dapat menikmati kualitas video yang prima lewat hadirnya teknologi VCD dan DVD (*Digital Versatile Disc*), sedangkan dunia broadcasting kini juga lambat laun mengalihkan teknologinya kearah DTV (*Digital Television*). Sebagian besar rumah tangga di Amerika Serikat telah menggunakan penerimaan

sinyal kabel digital dan sinyal satelit untuk menikmati siaran televisi digital.

2.2.6 Struktur Berkas Citra Bitmap

Citra bitmap 24-bit digunakan sebagai *cover* pada sistem steganografi yang akan di bangun. Struktur data citra tersebut adalah sebagai berikut:



Gambar 2.7 Struktur berkas citra bitmap 24-bit

a. *Header* berkas

Merupakan data yang terdapat pada bagian awal berkas citra. *header* berkas berisi informasi tipe berkas, ukuran ukuran berkas, dan informasi jumlah *offset* byte. Ukuran *header* berkas sama untuk semua versi citra bitmap yaitu 14-byte.

b. *Header* bitmap

Data *header* bitmap berguna untuk mengetahui bagaimana citra dalam format bitmap dikodekan dan disimpan. Data *header* bitmap misalnya informasi ukuran citra, kedalaman piksel, informasi apakah bitmap terkompresi atau tidak serta tipe kompresinya, jumlah data bitmap dalam byte dan jumlah warna yang digunakan. Ukuran *header* bitmap berbeda-beda untuk setiap versi, untuk versi lama, *header* bitmap berukuran 12-byte, untuk versi baru dari Microsoft Windows berukuran

40-byte, sedangkan untuk versi baru dari IBM OS/2, *header* bitmap berukuran 64-byte.

c. Informasi palet

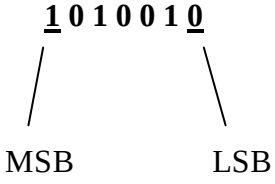
Informasi palet warna terletak sesudah *header* bitmap. Informasi palet warna dinyatakan dalam suatu tabel RGB. Setiap *entry* pada tabel terdiri atas tiga buah *field*, yaitu R *(red*), G (*green*) dan B (*blue*). Ukuran informasi palet pada citra bitmap 24-bit adalah 0-byte karena nilai RGB langsung diuraikan di dalam data bitmap.

d. Data bitmap

Setiap elemen data bitmap panjangnya 3-byte, masing-masing menyatakan komponen RGB. Data bitmap ini merupakan data berkas bitmap yang sebenarnya, pada bagian inilah informasi dapat disimpan dengan metode LSB.

2.2.7 Least Significant Bit (LSB)

Metode steganografi yang paling umum pada tipe berkas citra adalah *least significant bit* (LSB). Metode ini menyembunyikan data dengan mengganti bit-bit data yang paling tidak berarti di dalam *cover* dengan bit-bit data rahasia. Pada susunan bit di dalam sebuah *byte* (1 *byte* = 8 bit), ada bit yang paling berarti *(most significant bit* (MSB) dan bit yang paling kurang berarti *least significant bit* (LSB).



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 pada cover *citra*, *byte* tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti, apalagi mata manusia tidak dapat membedakan perubahan yang kecil. Sebagai contoh, misalnya terdapat data *raster original file* citra yang akan digunakan sebagai *cover* sebagai berikut:

00100111 11101001 11001000

00100111 11001000 11101001

11001000 00100111 11101001

Sedangkan representasi biner huruf A adalah 01000001, dengan menyisipkannya ke dalam pixel di atas maka akan dihasilkan

00100111 11101001 11001000

00100111 11001000 11101000

11001000 00100111 11101001

Terlihat hanya tiga bit rendah yang berubah (cetak tebal), untuk penglihatan mata manusia sangatlah mustahil untuk dapat membedakan warna pada *file* citra yang sudah diisi pesan rahasia jika dibandingkan dengan *file* citra asli sebelum disisipi dengan pesan rahasia.

2.3 Pengkodean Data

Data disimpan di dalam komputer pada *main memory* untuk diproses. Sebuah karakter data disimpan dalam *main memory* menempati posisi 1 byte. Komputer generasi pertama, 1 byte terdiri dari 4 bit, komputer generasi kedua, 1 byte terdiri

dari 6 bit dan komputer generasi sekarang, 1 byte terdiri dari 8 bit. Suatu karakter data yang disimpan di *main memory* diwakili oleh kombinasi dari dijit biner (*binary digit* atau bit). Kode biner dapat digunakan untuk mewakili suatu karakter.

Suatu komputer yang berbeda menggunakan kode biner yang berbeda untuk mewakili suatu karakter. Komputer yang 1 byte terdiri dari 4 bit, menggunakan kode binary yang berbentuk kombinasi 4 bit, yaitu BCD (*Binary coded decimal*). Komputer yang menggunakan 6 bit untuk 1 bytenya, menggunakan kode biner yang terdiri dari kombinasi 6 bit, yaitu SBCDIC (*Standard Binary Coded Decimal Interchange Code*). Komputer yang terdiri dari 8 bit, menggunakan kode biner yang terdiri dari kombinasi 8 bit, yaitu EBCDIC (*extended Binary coded decimal interchange code*) / ASCII (*American standard code of information interchange*).

1. BCD (*Binary Coded Decimal*)

   BCD merupakan kode biner yang digunakan hanya untuk mewakili nilai desimal saja, yaitu angka 0 sampai dengan 9. BCD menggunakan kombinasi dari 4 bit, sehingga sebanyak 16 ($2^4 = 16$) kemungkinan kombinasi yang dapat diperoleh dan hanya 10 kombinasi yang dipergunakan. Kode BCD yang orisinil sudah jarang dipergunakan untuk komputer generasi sekarang, karena tidak dapat mewakili huruf atau simbol-simbol karakter khusus.

2. SBCDIC (*Standard Binary Coded Decimal Interchange Code*)

   SBCDIC merupakan kode biner perkembangan dari BCD. BCD dianggap tanggung, karena masih ada 6 kombinasi yang tidak dipergunakan, tetapi tidak dapat digunakan untuk mewakili karakter yang lainnya. SBCDIC menggunakan kombinasi 6 bit , sehingga lebih banyak kombinasi yang bisa

dihasilkan, sebanyak 64 kombinasi kode, yaitu 10 kode untuk digit angka, 26 kode untuk huruf alphabet dan sisanya karakter-karakter khusus yang dipilih.

Posisi bit di SBCDIC dibagi menjadi 2 *zone*, yaitu 2 bit pertama disebut dengan *alphabet position* dan 4 bit berikutnya disebut *numeric bit position*.

3. EBCDIC (*Extended Binary Coded Decimal Interchange Code*)

   EBCDIC terdiri dari kombinasi 8 bit yang memungkinkan untuk mewakili karakter sebanyak 256 kombinasi karakter. Pada EBCDIC, *high-order* bits atau 4 bit pertama disebut dengan zone bits dan *low order* bits atau 4 bit kedua disebut dengan numeric bit.

4. ASCII (*American standard code for information interchange*) 7 bit

   Kode ASCII yang standard menggunakan kombinasi 7 bit, dengan kombinasi sebanyak 127 dari 128 kemungkinan kombinasi. Kode ASCII 7 bit ini terdiri dari dua bagian, yaitu *control characters* dan *information characters* yang merupakan karakter-karakter yang mewakili data.

5. ASCII 8 bit

   Karakter graphic yang tidak dapat diwakili oleh ASCII 7 bit, dapat diwakili dengan ASCII 8 bit karena lebih banyak memberikan kombinasi karakter.