IF3058 Kriptografi, Sem. II Tahun 2009/2010

Studi mengenai Video Watermarking serta Contoh Implementasinya

Oleh: Nicky Irawan 13507078

Abstraksi

Perkembangan dari layananan multimedia dan teknologi internet dewasa ini sangat maju dan memberikan kemudahan bagi pengguna untuk melakukan akses serta pendistribusian informasi dalam format digital. Produk-produk video merupakan karya intelektual manusia yang mencakup film dan musik atau yang disebut multimedia. Berbagai masalah dapat terjadi dengan produk tersebut seperti penggandaan, pembacaan pengubahan (manipulasi) yang semuanya dilakukan secara ilegal. Oleh karena itu salah satu solusi yang ditawarkan adalah menggunakan video watermarking.

Kata kunci: video, digital, watermarking, streaming, broadcast, steganography, copy protection,

1. Pendahuluan

Watermarking digital merupakan teknologi untuk memberikan dan membuktikan hak kepemilikan atas karya digital, mendeteksi *copy* yang sah, mengontrol penggunaan data dan menganalisis penyebaran melalui jaringan dan server. Tujuan utama digital watermarkin adalah merancang sebuah algoritma yang dapat digunakan untuk semua jenis video dan dapat menyisipkan jenis kode informasi tertentu.

Video watermarking juga dapat diimplementasikan pada streaming video (broadcast) sehingga bagi stasiun televisi yang melakukan penyiaran tidak mengalami ketakutan apakah yang disiarkannya akan disiarkan ulang atau direkam oleh pihak yang tidak berwenang. Selama ini biasanya stasiun televisi hanya memberikan logo stasiunnya di pojok kiri atau kanan bawah untuk menandakan bahwa yang memiliki hak siar hanya stasiun tersebut, tetapi teknik ini dapat dipecahkan dengan mudah dengan menghapus logo dan atau menambahkan logo sendiri untuk menutupi logo stasiun televisi.

2. Dasar Teori

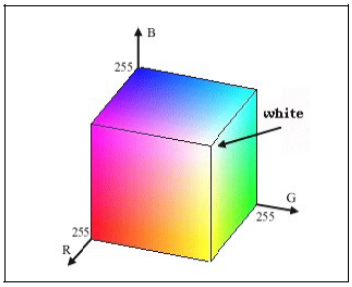
2.1. Watermarking

Istilah *watermarking* ini muncul dari salah satu cabang ilmu yang disebut dengan steganography. *Steganography* merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi “rahasia” di dalam suatu informasi lainnya. Steganography mempunyai sejarah yang hampir sama dengan *cryptograhpy*, keduanya banyak digunakan terutama pada zaman perang.

Watermarking atau tanda air dapat diartikan sebagai suatu teknik penyembunyian data atau informasi “rahasia” kedalam suatu data lainnya untuk “ditumpangi” (kadang disebut *host* data), tetapi orang lain tidak menyadari adanya kehadiran data tambahan pada host-nya. Jadi seolah-olah tidak ada perbedaan antara data *host* sebelum dan sesudah proses watermarking. Disamping itu data yang ter-*watermark* harus tahan (*robust*) terhadap serangan-serangan baik secara sengaja ataupun tidak di sengaja untuk menghilangkan data *watermark* di dalamnya. *Watermark* juga harus tahan terhadap berbagai jenis pengolahan/proses bisa berupa text, image, audio, maupun video.

2.2. RGB

Warna pada dasarnya adalah hasil persepsi cahaya dalam spektrum wilayah yang terlihat oleh retina mata, dan memiliki panjang gelombang antara 400nm sampai dengan 700 nm. Ruang warna RGB dapat divisualisasikan sebagai sebuah kubus seperti Gambar 1 , dengan tiga sumbunya yang mewakili komponen warna merah (*red*) R, hijau (*green*) G, biru (*blue*) B. Salah satu pojok alasnya yang berlawanan menyatakan warna hitam ketika R = G = B = 0, sedangkan pojok atasnya yang berlawanan menyatakan warna putih ketika R = G = B = 255 (sistem warna 8 bit bagi setiap komponennya). RGB sering digunakan di dalam sebagian besar aplikasi komputer karena dengan ruang warna ini tidak diperlukan transformasi untuk menampilkan informasi di layar monitor. Alasan ini juga yang menyebabkan RGB banyak dimanfaatkan sebagai ruang warna dasar bagi sebagian besar aplikasi.



Komponen Warna RGB sebagai Vektor Intensitas Warna

2.3. Video Watermarking

Video pada dasarnya merupakan susunan dari beberapa frame, dan tiap frame ini dipandang sebagai sebuah citra diam. Oleh karena itu sebagian besar metode pada image *watermark*ing dapat digunakan pada video *watermarking*. Penyisipan *watermark* pada *watermark* video dapat dilakukan pada bagian frame *motion* dan/atau *motionless*. Dalam penggunaannya, *watermarking* terdiri dari dua tipe yaitu identik *watermark* dan independen *watermark*. Agar dapat terhindar dari penghilangan *watermark* oleh pihak-pihak yang tidak berhak maka peyisipan *watermark* dilakukan dengan menggunakan identik *watermark* pada bagian *frame motionless*.

2.4. MPEG

MPEG atau Moving Picture Experts Group merupakan mekanisme yang dapat diterima secara universal dalam penyandian (maupun penyimpanan/*storage* yang bersifat optional) serta penyaluran program-program video yang dikompresi secara digital pada laju bit yang lebih besar dari 1 Mbps. "Program video" atau singkatnya disebut "program" di sini didefinisikan sebagai gambar-gambar bergerak yang disertai dan tersinkronisasai dengan audio. Misalnya adalah suara dari *soundtrack* stereo yang dinikmati dengan irama yang sinkron dengan gambar-gambar yang sedang dilihat, iklan-iklan komersial, serta video klip seperti item-item katalog *video home shopping.*

3. Aplikasi Watermarking

3.1. Broadcast Monitoring

Pernah ada kejadian pada tahun 1997 di jepang mengenai periklanan di televisi, pemasang iklan dikenakan biaya terhadap iklan yang tidak pernah ditayangkan. Hal ini karena tidak ada mekanisme untuk mengawasi penayangan iklan yang sedang berlangsung. Para musisi dan aktor-aktor juga ingin dibayar atas penayangan pertunjukan mereka. Demikian juga pemilik hak cipta tidak ingin miliknya ditayangkan secara illegal oleh stasiun yang membajak.

Watermarking dapat digunakan dalam *broadcast monitoring* dengan menambahkan *watermark* yang unik kedalam tiap video ataupun suara sebelum ditayangkan oleh stasiun televisi atau disiarkan oleh stasiun radio. Dan sebuah stasiun pengamat otomatik akan menerima tayangan tersebut sehingga dapat mengekstrak informasi *watermark* yang dibawanya dan mencatat kapan dan dimana tayangan tersebut muncul.

Selain itu, setiap stasiun pemancar tentunya harus membayar mahal untuk sebuah penyiaran acara langsung, acara sinetron maupun film action dan sebagainya. Semua biaya ini tentunya ditutupi dengan adanya sponsor iklan dalam acara tersebut.

Acara yang disiarkan tersebut tentunya takut direkam oleh orang lain, terutama stasiun televisi lainnya yang kemudian disiarkan kembali. Dengan demikian, stasiun televisi yang melakukan tindakan perekaman dan siar ulang tersebut hanya mengeluarkan biaya yang lebih kecil, karena tidak perlu membeli hak siar acara tersebut, apalagi acara tersebut tadinya merupakan suatu acara langsung misalnya acara pertandingan sepak bola bergengsi di luar negeri. Karena itu, stasiun televisi yang melakukan penyiaran acara tersebut sering memberikan logo stasiun televisi mereka pada sudut atas atau bawah baik kanan maupun kiri layar. Tetapi cara tesebut sebenarnya mudah diakali dengan menghapus logo tersebut dan kemudian ditambahkan dengan logo yang baru.

3.2. Proof of Ownership

Watermarking selain dapat digunakan untuk tanda pengenalan pemilikan (*owner identification*) seperti yang disebutkan diatas, juga dapat digunakan untuk pembuktian kepemilikan. Pembuktian kepemilikan ini diperlukan pada saat dua orang memperebutkan hak kepemilikan atau menyatakan bahwa data digital tersebut adalah miliknya. Jadi untuk membuktikannya dapat digunakan *watermarking*. Tentunya segala sesuatu relugasi hukumnya harus ditentukan secara benar dan semua ini memerlukan usaha yang sulit.

4. Karakteristik Watermarking

4.1. Robustness

Watermark harus robust artinya *watermark* di dalam *host* data harus tahan terhadap beberapa operasi pemrosesan digital yang umum seperti penkonversian dari digital ke analog dan sebagai dari analog ke digital, dan kompresi terutama kompresi lossy.

Kadang-kadang sebuah *watermark* hanya tahan terhadap sebuah proses tetapi rentan terhadap proses yang lain. Tetapi untungnya dalam banyak aplikasi, ketahanan *watermark* terhadap semua proses yang mungkin tidak diperlukan dan dianggap terlalu berlebihan. Biasanya *watermark* harus tahan terhadap pemrosesan sinyal yang

terjadi hanya antara proses *embedding* (penyembunyian *watermarking* dalam data) dan deteksi. Contohnya aplikasi *watermarking* pada televisi, jadi yang ditekankan disini adalah proses kompresi lossy, transmisi analog, dan sebagainya. Sedangkan aplikasi *watermarking* pada suara yang melalui kanal telepon berarti batasan bandwidth sekitar 4000 Hz, tipe data analog, dan *sampling* atau *resampling* pada beberapa *central telepon office* (CTO).

Tetapi untuk aplikasi *autenthication*, justru *watermark* diharapkan serentan mungkin terhadap proses pengolahan sinyal digital yang mungkin terjadi atau hampir seluruh proses pengolahan sinyal digital yang dapat dilakukan.

Jadi ukuran robustness terhadap proses tertentu yang diperlukan untuk aplikasi tertentu mungkin tidak diperlukan dalam aplikasi yang lain. Untuk menentukan ukuran robustness harus terlebih dahulu dipikirkan aplikasi apa yang akan menggunakan sistem *watermarking*.

4.2. Tamper Resistance

Yang dimaksud dengan tamper resistance adalah ketahanan sistem *watermarking* terhadap kemungkinan adanya serangan (attack) atau usaha untuk menghilangkan, merubah bahkan untuk memberikan *watermark* palsu terhadap suatu *host* data.

Ada beberapa jenis serangan (attack) terhadap sistem *watermarking* [3]:

- *Active attacks*. Merupakan serangan dimana seseorang berusaha untuk menghilangkan *watermark* yang terdapat didalam *host* data.
- *Passive attacks*. Serangannya hanya ditujukan untuk mengetahui apa isi *watermark* tersebut, jika memang ada di dalam *host* data.
- *Collusion attacks*. Serangan ini merupakan usaha seseorang untuk menghasilkan sebuah *copy* dari *host* data yang tidak memiliki *watermark* dengan memanfaatkan beberapa *host* data yang memiliki berbagai *watermark*, seperti pada aplikasi *fingerprinting*. Serangan ini merupakan serangan khusus yang termasuk dalam *active attacks.*
- *Forgery attacks.* Serangan ini tidak hanya bertujuan untuk membaca atau menghilangkan *watermark* yang ada, tetapi juga menanamkan suatu *watermark* yang baru (tentunya yang valid) ke dalam suatu *host* data. Serangan ini cukup menjadi perhatian yang serius terutama untuk aplikasi bukti kepemilikan (*proof of ownership*)

4.3. Fidelity

Yang dimaksud dengan *fidelity* disini adalah derajat degradasi *host* data sesudah diberikan *watermark* dibandingkan dengan sebelum diberikan *watermark*. Biasanya bila *robustness* dari *watermark* tinggi maka memiliki *fidelity* yang rendah sebaliknya *robustness* yang rendah dapat membuat *fidelity* yang tinggi. Jadi sebaiknya dipilih *trade-off* yang sesuai, sehingga keduanya dapat tercapai sesuai dengan tujuan aplikasi. Untuk *host* data yang berkualitas tinggi maka *fidelity* dituntut setinggi mungkin sehingga tidak merusak data aslinya, sedangkan *host* data yang memiliki *noise* (kualitas kurang) maka *fidelitynya* bisa rendah seperti pada suara pada siaran radio, suara pada telepon ataupun *broadcast* acara televisi.

5. Watermarking untuk Broadcast Monitoring

Penemuan gambar hidup (1891) dan televisi (1923) merupakan salah satu temuan yang cukup berpengaruh dalam sejarah hidup manusia disamping telepon, tape radio dan sebagainya [5]. Selain itu, penemuan teknik komunikasi tanpa kabel (1895) juga memberikan terobosan yang cukup berarti dalam hidup ini. Dengan temuan-temuan ini, kita tidak hanya menikmati gambar-gambar diam tetapi juga gambar-gambar (seolah-olah) gerak pada tempat-tempat yang jauh dan berbeda.

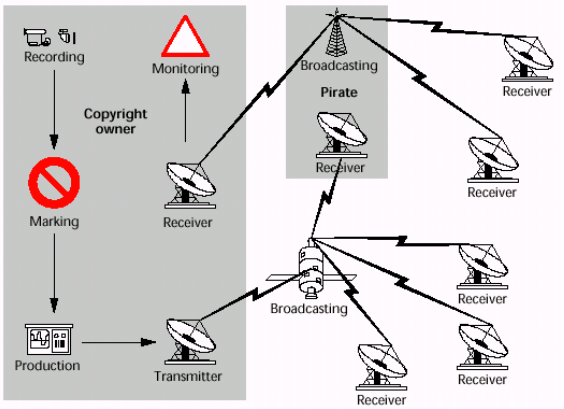
Dewasa ini hampir setiap rumah memiliki sebuah televisi untuk menyaksikan acara-acara kesayangan yang dipancarkan dari satu atau beberapa stasiun televisi. Stasiun-stasiun pemancar berlomba-lomba untuk menayangkan berbagai acara yang bagus-bagus, dengan tujuan menarik pemirsa yang banyak sehingga para sponsor (iklan) juga mau mengiklankan produk mereka pada stasiun pemancar mereka.

Saat ini banyak sekali stasiun pemancar acara televisi bermunculan. Stasiun pemancar nasional di Indonesia saat ini saja sudah muncul begitu banyak, ditambah lagi penggunaan parabola kita dapat mendapatkan siaran dari negara-negara lain.

Acara-acara yang disiarkan baik berupa berita, pertandingan sepak bola yang disiarkan langsung, pentas musik sampai dengan film-film box office yang sudah beredar dibioskop. Tentunya semua itu melibatkan sejumlah uang yang cukup besar, apalagi hak menyiarkan suatu acara itu dibeli dengan mahal sekali, contohnya siaran langsung acara sepak bola liga Itali yang dibeli oleh RCTI, atau pembelian hak siar suatu film box office oleh suatu stasiun televisi.

Disamping masalah isi dari acara, sponsor-sponsor acara dalam bentuk periklanan juga mengalami permasalahan. Pemasangan sebuah iklan dengan durasi 30 detik saja tentunya sudah memakan biaya jutaan rupiah. Sebuah perusahaan mungkin memasangkan iklannya sekian puluh kali dengan durasi sekitar 30 – 90 detik. Dengan demikian harganya pasti ratusan juta rupiah. Bagaimana pemasang iklan mengetahui bahwa iklan tersebut disiarkan sesuai dengan perjanjian (durasi, waktu, serta repetisinya). Tentu saja ini

memerlukan suatu mekanisme pengecekan. Pemasang iklan (biasanya perusahaan) tentu saja dapat menyewa seseorang atau lebih untuk melakukan pengecekan terhadap siaran yang berlangsung dan mencatat informasi-informasi yang berkaitan, tetapi masalahnya siaran dari suatu pemancar dari pagi hingga tengah malam kadang melebihi 18 jam, bahkan ada yang non-stop 24 jam. Bagaimana kalau pemasang iklan tidak hanya memasangkan iklan pada satu stasiun pemancar tetapi lebih dari satu, tentunya pemeriksaan secara manual akan memakan biaya tambahan karena banyaknya orang yang diperlukan.



Mekanisme Watermarking pada Broadcast Monitoring

Apalagi saat ini banyak sekali materi video atau bahan siaran yang disiarkan, hal ini membuat pengawasan secara manual tidak dimungkinkan lagi. Suatu mekanisme untuk pengawasan secara otomatis dirasakan sangat perlu saat ini. Pengawasan secara otomatis (*automatic broadcast monitoring*) akan melakukan pemantauan terhadap siaran seluruh dunia, mencatat waktu penyiaran, oleh stasiun pemancar yang mana, lamanya penyiaran, bahkan mungkin juga bagian mana saja dari sebuah acara disiarkan, karena mungkin suatu siaran ulang tidak disiarkan secara keseluruhan lagi.

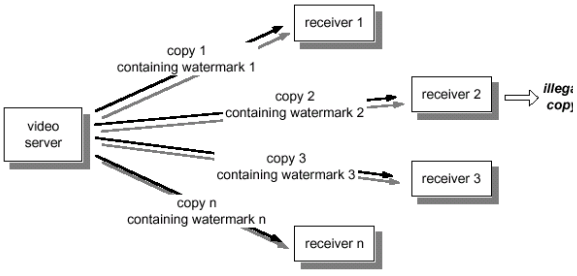
Mekanisme *watermarking* dalam hal ini tampaknya cukup menjanjikan dalam membantu proses automatic broadcast monitoring. Karena *watermarking* akan menyisipkan suatu informasi mengenai isi suatu acara ke dalam data acara itu sendiri, sehingga pada waktu penyiaran acara tersebut secara tidak langsung *watermark* juga akan ikut serta. Sehingga sistem broadcast monitoring dapat melakukan pemantauan terhadap sinyal yang dipancarkan dan mengekstrak informasi *watermark* yang terdapat dalam sinyal yang diterima serta melakukan tugas-tugas yang sesuai dengan diprogramkan.

Watermark yang diperlukan pada mekanisme sistem broadcast monitoring ini tentunya tidak hanya berupa sepotong informasi kecil seperti yang digunakan pada aplikasi *copy control/protection* (akan dijelaskan pada bagian berikutnya), tetapi setiap detiknya mungkin setiap *frame*-nya mengandung informasi *watermark* yang unik, hal ini dikarenakan persyaratan pada sistem *broadcast monitoring* yang akan mencatat info-info yang diperlukan. Proses *Watermarking* dapat dilakukan pada studio produksi (*non real time*) atau ditambah dengan *watermark* pada saat penyiaran (*real time*) untuk mempermudah jalur penelusuran.

6. Watermarking pada Streaming

Watermarking juga tidak hanya digunakan dalam *broadcasting* (penyiaran), tetapi juga dapat digunakan dalam service *video on demand*. Dengan kemajuan teknologi internet dan infrastrukturnya, nantinya semua orang di dunia dapat menikmati segala acara kesayangannya kapan saja tanpa digangu oleh kesibukan kerja di kantor, mengurus dapur atau bayi. Dengan adanya *watermarking* dalam isi video yang dikirimkan maka bila terjadi pengkopian secara ilegal serta terjadi penduplikasian dan distribusinya secara gelap di pasaran, maka dapat ditelusuri sumber kebocoran atau penduplikasian ilegalnya.

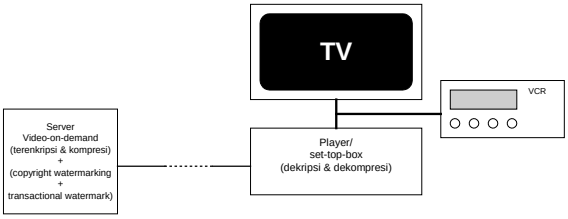
Contohnya dapat dilihat pada gambar di bawah ini, bila terdapat n orang yang memohon untuk menyaksikan suatu acara video, maka *server* akan mengirimkan ke pemirsa dimana sebelumnya *watermarking* telah memberikan informasi yang unik untuk masing-masing kopi yang dikirimkan. Informasi itu dapat berupa sumber atau pemilik atau penyedia service, waktu pengiriman, serta nama atau alamat pemohon. Misalnya penerima no. 2 melakukan pengkopian dan juga terjadi peredaran barang kopian tersebut di pasaran maka dengan mengekstrak *watermark* dari dalam video yang diduplikasikan tersebut dapat diketahui minimal sumber penduplikasian dari mana, dan dapat dilakukan pelacakan lebih lanjut, misalnya keterlibatan pihak lain dalam pendistribusiannya dan sebagainya.



Mekanisme Watermarking pada Service Video On Demand

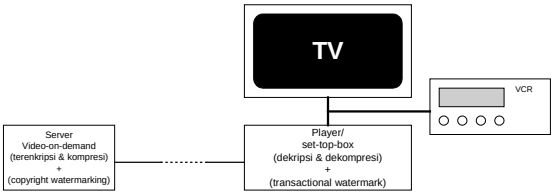
Salah satu tuntutan sistem *watermarking* untuk aplikasi ini (disebut juga dengan

transactional watermarks atau fingerprinting) adalah proses *watermarking* harus *real time*, tetapi mungkin tidak diperlukan proses deteksi pada bagian *decoder* penerimanya, kecuali bila ingin digabungkan dengan aplikasi *copy protection* yang akan dibicarakan pada bagian berikut. Gambaran sistem dapat dilihat pada gambar di bawah ini.



Peletakan transactional watermark pada sisi server

Sedangkan model lainnya adalah meletakkan *transactional watermark* pada player atau *set-top-box client*, sehingga tuntutan real-time akan berbeda dengan model yang diatas, dimana pada bagian server tidak perlu *real-time* karena *watermarking* dapat dilakukan pada saat *storing* (penyimpanan) jauh sebelum service diberikan, sedangkan pada bagian client harus diberikan rangkaian *watermark* embedding yang *real-time* tanpa memerlukan detektor *watermarking*.



Peletakan transactional watermark pada sisi client

Dengan adanya *transactional watermark* tersebut, maka dapat dilihat bahwa segala usaha untuk mengduplikasi secara ilegal dengan menggunakan VCR, atau alat perekam lainnya tentunya akan turut merekam *watermark* yang terdapat didalamnya.

Penggunaan *watermark* sebagai *transactional watermark* tidak dapat mencegah terjadinya penduplikasian terhadap isi pelayanan yang diberikan, tetapi memberikan kemudahan untuk menelusuri kebocoran isi service yang diberikan. Berikut ini adalah aplikasi *watermark* sebagai *copy control/protection* untuk mencegah terjadinya penduplikasian ilegal.

7. Algoritma Watermarking

7.1. Algoritma Koch-Zhao yang diperbaiki

Algoritma Koch-Zhao sebenarnya merupakan algoritma yang diterapkan pada media digital dalam bentuk citra diam. Algoritma ini bekerja secara blok per blok dengan ukuran 8x8 pixel dalam domain DCT (*discrete cosine transform*). Dengan melihat domain kerja algoritma ini, berarti algoritma Koch-Zhao ini memiliki kemiripan dengan metoda kompresi JPEG untuk citra diam.

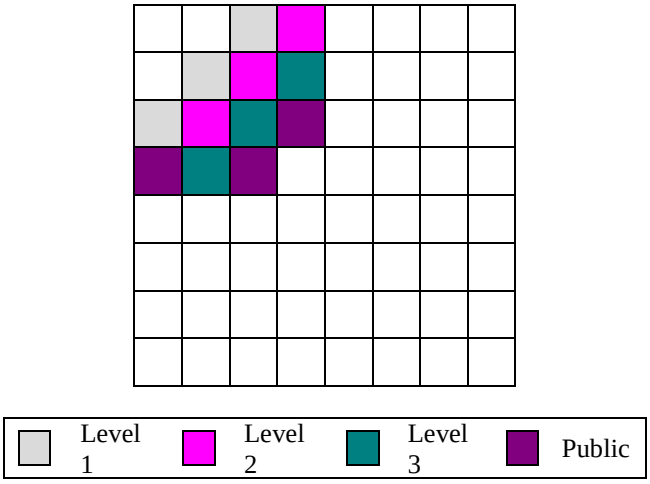
Hasil perbaikan algoritma Koch-Zhao ini diterapkan dalam video oleh [4] berdasarkan kemiripan setiap frame dari video seolah-olah merupakan sebuah citra diam. Penerapan algoritma *watermarking* ini pada stream-video yang belum dilakukan kompresi. Setiap frame video dianggap sebagai sebuah citra diam. Komponen luminance dari frame/citra dibagi atas blok-blok dengan ukuran 8x8. Algoritma akan memilih sederetan blok-blok tergantung banyaknya bit informasi yang akan ditanamkan, kemudian dilakukan transformasi DCT pada setiap blok yang terpilih. Hasil transformasi berupa koefisien-koefisien DCT kemudian dilakukan kuantisasi untuk mengantisipasi kompresi terhadap stream-video yakni MPEG-2 yang juga menerapkan prinsip yang hampir sama. Tahapan kuantisasi tersebut membagi koefisien DCT dengan sebuah bilangan bulat dalam sebuah matrix kuantisasi dibawah ini. Kemudian hasil kuantisasi dilakukan perubahan beberapa koefisien untuk coding sebuah bit informasi. Kemudian dilakukan sebaliknya inverse DCT.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Tabel kuantisasi standard JPEG

Dua komponen penting dalam algoritma ini adalah:

1. Posisi atau blok mana yang akan dilakukan *watermark embedding*. Pemilihan blok citra yang akan *diwatermark* dilakukan dengan sebuah kunci inisial untuk menghasilkan sederetan *pseudo-random* sehingga dapat ditentukan blok-blok mana yang dipilih.
2. Pelaksanaan *watermark* itu sendiri. Pelaksanan *watermark* terhadap blok yang terpilih dengan mengubah sepasang koefisien DCT dari blok tersebut. Pemilihan koefisien dapat dilihat pada gambar dibawah sesuai dengan tingkatannya menurut [4] yang dibagi atas beberapa *sub-band*.



Sub-band dalam watermarking

Dengan adanya pembagian atas 4 sub-band tersebut maka algoritma ini dapat menanamkan paling banyak 4 buah *watermark* yang berbeda tanpa mempengaruhi satu dengan yang lainnya. Pembagian ini menyediakan satu sub-band sebagai *public watermark* sisanya merupakan *secret watermark*.

Seperti yang dikatakan sebelumnya, setiap blok yang terpilih akan dikodekan *sebuah* bit *watermark* ke dalamnya, dengan algoritma sebagai berikut:

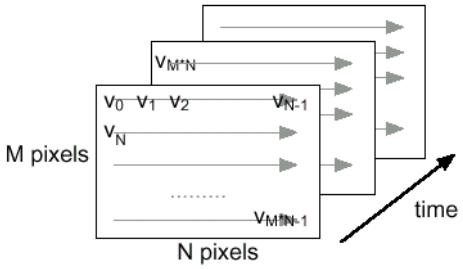
1. Nilai-nilai pixel dalam sebuah blok ditransformasi dengan DCT.
2. Mekanisme pendeteksian tepian (edge) diterapkan untuk menghindari distorsi pada host data yang di*watermark*.
3. Sepasang koefisien DCT (a,b) dipilih berdasarkan sub-band yang diinginkan.
4. Koefisien yang terpilih dilakukan kuantisasi.
5. Menggunakan koefisien tersebut untuk menentukan daerah-daerah yang cocok untuk penanaman *watermark*.
6. Tergantung pada nilai bit yang akan ditanamkan, bila ingin mengencode bit "1" maka a ≥ b + d, sebaliknya encoding bit "0" maka a + d ≤ b. Dimana d merupakan tingkat noise atau noise margin yang dapat diatur-atur untuk menghindari efek degradasi kualitas pada sinyal aslinya dan juga meningkatkan robustness.
7. koefisien yang telah diganti dikalikan dengan nilai kuantisasi sebelumnya, kemudian blok tersebut dilakuan inverse DCT. Demikian seterusnya sampai seluruh blok yang terpilih dilakukan hal yang serupa dari 1 – 7.

Perbedaan algoritma Koch-Zhao terutama terletak pada 2 dan 5 dalam menentukan apakah blok tersebut layak digunakan untuk *watermark* ataupun jika layak, maka berapa noise margin yang perlu untuk menghindari degradasi yang sangat kelihatan.

7.2. Algoritma Hartung-Girod

Prinsip komunikasi spread spectrum banyak digunakan dalam *watermarking*, termasuk algoritma algoritma yang akan kita bicarakan ini. Prinsip spread spectrum adalah mengirimkan sinyl dengan pita sempit melalui kanal yang berpita lebar dengan menggunakan penyebaran frekuensi. Demikian juga dengan *watermarking*, sinyal berpita sempit (dalam hal ini adalah *watermark* itu sendiri) akan ditransmisikan melalui kanal yang lebar bersama dengan data video atau citra.

Algoritma ini juga menggunakan prinsip private dan public key untuk embedding dan ekstracting bit *watermark*. Prinsip ini banyak digunakan dalam cryptography. Maksud penggunaan prinsip private dan public ini supaya masyarakat luas dapat juga mengekstrak informasi *watermark* yang ada tanpa menggunakan kunci private, tetapi tidak dapat menghapus informasi *watermark* yang ada hanya berdasarkan kunci public. Sering, video dianggap merupakan sinyal dengan 3 dimensi (spasial dan waktu), tetapi dalam algoritma ini sinyal akan dianggap sebagai 1 dimensi dengan prinsip line-scanning seperti berikut:



Prinsip line-scanning pada sinyal video

Misalkan serangkaian bit *watermark* yang akan ditanamkan dalam stream video sebagai berikut:

$$a_j,\ a_j \in \{-1,1\},\ j \in \mathbf{N}$$

Sinyal diskrit ini akan disebarkan dengan faktor penyebar cr, yang disebut chip-rate untuk mendapatkan rangkaian tersebar,

$$b_i = a_j,\ j \cdot cr \le i \le (j+1) \cdot cr,\ i \in \mathbf{N}$$

Maksud penyebaran adalah untuk meningkatkan redundansi dalam penanaman 1 bit informasi ke dalam *cr* pixel dari sinyal video. Kemudian b_j akan dikalikan dengan faktor penguat $\alpha_i > 0$, kemudian dimodulasikan dengan rentetan bipolar pseudo-noise,

$$p_i,\ p_i \in \{-1,1\},\ i \in \mathbf{N}$$

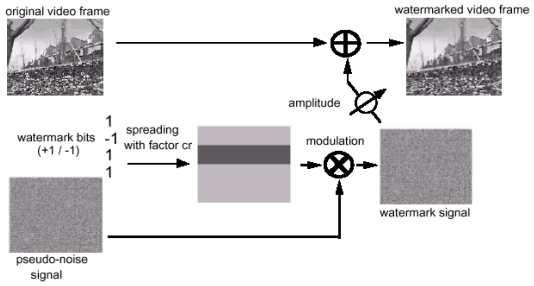
yang berfungsi sebagai penyebar frekuensi. Sinyal yang termodulasi tersebut merupakan spread spectrum *watermark*.

$$w_i = \alpha_i \cdot b_i \cdot p_i, \; i \in \mathbf{N}$$

Spread spectrum *watermark* tersebut kemudian ditambahkan dengan line-scan sinyal video, sehingga dihasilkan sinyal video ter*watermark*:

$$\tilde{v}_i = v_i + \alpha_i \cdot b_i \cdot p_i, \;\; i \in \mathbf{N}$$

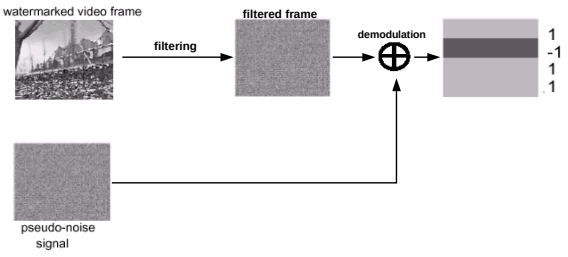
dimana harus diatur dalam bentuk matriks untuk ditampilkan kemudian sebagai sebuah sinyal video 3 dimensi. Gambar berikut akan memberikan gambaran proses *watermarking* dengan algoritma ini.



Proses embedding *watermark* dalam algoritma ini

Untuk kesederhanaan komputasi dan penjelasan, digunakan binary/bipolar pseudo-noise sequence seperti diatas, tetapi sebenarnya dapat digunakan bermacam-macam deretan pseudo-noise yang bukan data biner. Karena pseudo-noise tersebut merupakan kunci dari proses embedding dan extracting, maka deretan pseudo-noise tersebut, seharusnya tidak mudah didapat, sendangkan untuk kunci public diambil sebagian dari kunci private tersebut misalnya setiap bit ke 3 dari private key merupakan public key, selanjutnya bit-bit lain pada public key dihasilkan oleh generator yang lain.

Selanjutnya proses pembacaan bit *watermark* dapat dilakukan tanpa adanya data original asalkan kita memiliki kunci berupa pseudo-noise tersebut maka kita dapat membaca kembali *watermark* yang ditanamkan.



Proses pembacaan *watermark*

Karena algoritma ini memungkinkan pembacaan *watermark* dengan menggunakan public key dan private key, maka akan dibicarakan proses pembacaan dengan kedua key tersebut.

Proses Pembacaan Watermark dengan Private Key

Proses pembacaan *watermark* dengan menggunakan prinsip kolerasi, dimana sebelum proses kolerasi tersebut sinyal video ter*watermark* $\tilde{v}$ difilter dengan highpass filter. Penggunaan filter dimaksudkan supaya sinyal *watermark* terpisah dengan sinyal video asli, dimana setelah proses filter hanya sinyal *watermark* yang terlewatkan.

Proses berikutnya adalah demodulasi, dimana sinyal video yang telah di filter dikalikan dengan pseudo-noise p_i yang sama untuk proses embedding, seterusnya hasil perkalian dijumlahkan sehingga diperoleh:

$$s_j = \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} p_i \cdot \bar{\tilde{v}}_i = \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} p_i \cdot \bar{v}_i + \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} p_i \cdot \overline{p_i \cdot \alpha_i \cdot b_i}$$

dengan <u>*asumsi*</u> $\bar{v}_i$ telah difilter habis dengan highpass filter dengan demikian $\sum_1 = 0$, sehingga tinggal bagian $\sum_2$, dan $\overline{p_i \cdot \alpha_i \cdot b_i} \approx p_i \cdot \alpha_i \cdot b_i$, maka jumlah kolerasinya akan menjadi:

$$s_j = \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} {p_i}^2 \cdot \alpha_i \cdot b_i = a_j \cdot {\sigma_p}^2 \cdot cr \cdot mean(\alpha_i)$$

dimana ${\sigma_p}^2$ adalah varian dari deretan pseudo-noise. Dengan demikian tanda (sign) dari jumlah korelasi merupakan bit informasi yang ditanamkan.

$$sign(s_j) = sign(a_j \cdot {\sigma_p}^2 \cdot cr \cdot mean(\alpha_i)) = sign(a_j) = a_j$$

Proses Pembacaan Watermark dengan Public Key

Demikian juga dengan penggunaan public key dalam proses pembacaan *watermark* sama dengan proses pembacaan *watermark* dengan private key, bedanya hanya di p_i dengan ${p_i}^{public}$. Sebelumnya telah dikatakan bahwa public key diturunkan dari private key, misalnya ke mengambil bit ke-*n*, dimana *n* > *2*, dari private key dan bit-bit lainnya merupakan nilai acak dengan distribusi yang sama seperti private key.

$${p_i}^{public} = \begin{cases} p_i, \; i = 1 + kn, k \in \mathbf{N} \\ rand\{-1,1\} \end{cases}$$

Dengan menggunakan public key tersebut maka perhitungan jumlah kolerasi publicnya menjadi :

$$s_j^{public} = \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} p_i^{public} \cdot \tilde{\tilde{v}}_i$$

$$\approx \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} p_i^{public} \cdot p_i \cdot \alpha_i \cdot b_i$$

$$\approx \frac{1}{n} \cdot cr \cdot \alpha_i \cdot a_j$$

maka seperti halnya dengan private key, tanda dari s_j^{public} merupakan bit informasi dari *watermark* tersebut.

$$a_j^{public} = sign(s_j^{public})$$

Meskipun prinsip public key sama dengan prinsip private key, tetapi robustness dari kedua cara tersebut berbeda, dimana robustness dari public key lebih rendah dibandingkan dengan private key. Faktor yang turut mendukung robustness dari metoda ini adalah chip-rate, *cr* dengan faktor penguat α tersebut. Hal ini dapat dilihat dari hasil estimasi BER dan hasil eksperimen berikut ini.

chip rate *cr*	amplification $mean(\alpha_i)$	PN variance σ_p^2	used filter	estimated BER	measured BER
1000	1	1	no filtering	0.415	0.412
10000	3	1	no filtering	0.021	0.018
50000	4	1	no filtering	7.2×10^{-10}	$\approx 0^{\dagger}$
1000	1	1	3×3 HP filter	0.146	4.8×10^{-2}
1000	2	1	3×3 HP filter	1.8×10^{-2}	8.1×10^{-3}
1000	3	1	3×3 HP filter	7.8×10^{-4}	5.5×10^{-4}
5000	1	1	3×3 HP filter	9.2×10^{-3}	5.1×10^{-3}
5000	2	1	3×3 HP filter	1.2×10^{-6}	$\approx 0^{\dagger}$
10000	3	1	3×3 HP filter	7.6×10^{-24}	$\approx 0^{\dagger}$
10000	4	1	3×3 HP filter	7.4×10^{-41}	$\approx 0^{\dagger}$
> 0	> 0	> 0	$\theta = 0$ (v removed)	0	$\approx 0^{\dagger}$

Pengaruh Chip-rate, Filter, dan α terhadap BER

Bagaimana menghitung pengaruh filter, chip-rate serta alpha tersebut dapat dilihat lebih jelas pada [6]. Tetapi dari tabel tersebut dapat dilihat bahwa penggunaan filter akan membantu mengurangi error yang terjadi, serta penggunaan *cr* dan α yang cukup besar akan mengecilkan BER. Tetapi dengan penggunaan α yang besar maka invisibility akan mengecil, sehingga akan kelihatan oleh indera persepsi manusia. Sedangkan penggunaan *cr* yang besar makan *payload* (banyaknya bit yang dapat ditanamkan) akan berkurang). Hasil percobaan dari algoritma ini dapat dilihat pada bagian berikut ini.

Atas: frame tanpa kompresi
Tengah: frame dengan kompresi MPEG-2
Bawah: frame dengan kompresi dan watermark

Daftar Pustaka

[1]. Benham D., Memon N., Yeo B.-L., Yeung M., *Fast Watermarking of DCT-based Compressed Images*, CISST '97 International Conference.

[2]. Cox, I.J., Miller, M.L., *A review of watermarking and the importance of perceptual modeling*, Proc. Of Electronic Imaging'97, 1997.

[3]. Ingemar J. Cox, Matt L. Miller and Jeffery A. Bloom, *"Watermarking applications and their properties"*, Int. Conf. On Information Technology'2000, Las Vegas, 2000.

[4]. Dittmann, J., Steinmetz, A., Nack, F., Steinmetz, R., *Interactive Watermarking Environments*, IEEE Multimedia 1998.

[5]. Fridrich, J., *Methods for data hiding*, Center for Intelligent Systems & Department of Systems Science and Industrial Engineering, 1997.

[6]. Hartung, F., Girod, B., *Copyright Protection in Video Delivery Networks by Watermarking of Pre-Compressed Video*, ECMAST 1997 Vol. 1242, pp.423-436, Springer, Heidelberg, 1997.

[7]. F. Hartung and B. Girod, "Copyright Protection in Video Delivery Networks by Watermarking of Pre-Compressed Video", Multimedia Applications, Services and Techniques – ECMAST'97, Springer, Heidelberg, 1997.

[8]. Koch, E. and Zhao, J., *Towards Robust and Hidden Image Copyright Labelling*, IEEE Workshop on Nonlinear Signal and Image Processing, 1995.