STUDI DAN IMPLEMENTASI ROBUST BLIND VIDEO WATERMARKING DENGAN MEKANISME ADAPTIVE EMBEDDING

Febrian Setiadi – NIM : 13503028

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if13028@students.if.itb.ac.id

Abstrak

Penyebaran data berbentuk video dijital melalui Internet menjadi semakin umum. Cuplikan film, video klip dan video yang berisi review dari produk yang berupa video games dan produk komersial lainnya, menjadi faktor penarik konsumen untuk membeli produk tersebut. Video yang di disebarluaskan ini perlu diproteksi untuk menghindari penyalahgunaan hak-cipta dan pelanggaran hukum.

Di makalah ini, akan dijelaskan pendekatan baru dari video watermarking di ranah spasial, pendekatan ini mengambil kelebihan dari informasi yang ada di kedua *intra-frame* dan *inter-frame* dari sebuah konten video untuk menjamin laten dan ketangguhan dari watermark. Sebuah *blok-classifier* secara sederhana dirancang berdasarkan informasi yang ada dalam pergerakan frame ke frame dan kompleksitas dari frame itu sendiri. Sementara itu ide dari penggantian bitplane diperkenalkan dalam prosedur pelekatan informasi ,keuntungan utama dari teknik bitplane ini adalah watermark dapat di ekstrak tanpa dibandingkan dengan konten video asal.

Strategi ekstraksi multi-frame memstikan bahwa sebuah watermark dapat secara tepat diungkap dari sebuah segmen video yang cukup singkat. Frame tunggal diekstrak dari video juga mengandung informasi watermark. Video yang telah di watermark hampir relatif sama dari konten video awal , maka teknik ini dipandang cukup tangguh dari serangan terhadap video watermarking.

Keywords: Perlindungan Hak-Cipta, *Digital watermarking, Video watermarking,* Teknik *Bit -Plane Adaptive algorithm.*

1. Pendahuluan

Perkembangan yang cepat dari teknologi multimedia dan jaringan komputer secara langsung memfasilitasi pembuatan dan pendistribusian dari konten dijital, tapi pada waktu yang sama hal itu menimbulkan isu baru yaitu penyalahgunaan hakcipta, dan Hak Atas Kekayaan Intelektual (HAKI). Sistem kriptografi biasa hanya mengijinkan pemegang kunci publik yang valid untuk mengenkripsi data, tetapi ketika sudah dalam bentuk cipher tidak bisa dilakukan runut balik pendistribusian dan penciptaan ulang. Untuk itulah digital watermarking, diperkenalkan seagai solusi dari masalah perlindungan hakcipta dari data multimedia.

Sebuah watermark dijital adalah sebuah tanda yang secara permanen dilekatkan dalam sebuah data dijital (citra tunggal atau potongan video atau audio), yang memungkinkan seseorang membuat pernyataan tentang kepemilikan atas konten dijital tersebut, misal, mengenali pembeli, ataupun menyediakan tambahan informasi tentang konten dijital yang telah dibuatnya.

Untuk kebanyakan aplikasi, sebuah tanda dijital biasanya harus memenuhi kebutuhan dasar seperti *transparency* (ketidaktampakan) dan *robustness* (ketangguhan), misalnya watermark yang dilekatkan dalam suatu konten dijital harus tak bisa dikenali dengan indra penglihatan dan juga harus susah dihilangkan,

kecuali kualitas penerimaan indera dari konten dijital secara signifikan berkurang.

Telah banyak teknik watermarking yang telah diperkenalkan untuk citra tunggal, baik itu berjalan di ranah *spatial* atau di ranah *transform*. Namun, Keunikan dari dimensi waktu dan ruang sebagai properti dari video dijital membedakan teknik video watermarking dari watermarking citra biasa. Unik disini maksudnya, untuk beberapa variabel tertentu citra yang ditampilkan pasti berbeda, hal ini menunjukkan ada dimensi lain dalam sebuah video secara umum.

Beberapa karakteristik yang benar-benar berbeda adalah, pada video watermarking, konten video dijital harus diperlakukan sebagai bagian yang utuh, diantaranya misalnya adanya aliran informasi inter-frame, penghitungan berdasar tahap encoding dan decoding memperhatikan serangan terhadap watermark misalnya, desinkronisasi bersama *temporal axis*.

Banyak teknik video watermark berbeda yang telah dikembangkan [6 dan 9], teknik2 ini secara garis besar dapat dibagi menjadi dua, yaitu teknik yang langsung menyisipkan watermark di konten video dijital yang telah di *compress* dengan metode tertentu (mislanya MPEG-2, 3GPP, WMV dan sebagainya), sedangkan teknik sisanya mengaplikasikan algoritma watermarking pada video yang belum ter-*compress* dengan format tertentu. Kedua teknik itu punya keunggulan dan kelemahan. apakah dari sisi kompleksitas proses nya atau kemudahan untuk diserang atau tidaknya sebuah watermark video tersebut.

Dalam melekatkan watermark ke dalam ranah video yang sudah ter-*compress*, perancangan dari MPEG encoder dan decoder harus disesuaikan agar bisa di impementasikan dengan skema video watermark tertentu yang sesuai.

Namun, teknik seperti ini mempunyai beberapa kendala-kendala utama seperti, watermark dapat dengan mudah dihilangkan oleh *attacker* dengan mengencode kembali data video dengan algoritma nya sendiri. Sedangkan untuk teknik uncompresed, teknik yang bisa digunakan adalah dengan memodifikasi contoh data spatial ataupun temporal. Hartung dan Girod [9] telah menggunakan ide "*direct sequence spread spectrum communication*" untuk video watermarking.

Ide dari *spread spectrum watermark* tersebut yaitu, *spread spectrum* watermark ditambahkan piksel demi piksel ke dalam sinyal dijital video dalam *scan line* nya. Jadi, menciptakan sebuah *yield* kedalam sinyal watermark.

Pendekatan lain untuk video watermarking dalam ranah spatial telah diperkenalkan di [8]. Di makalah tersebut dijelaskan pendekatan terhadap sebuah rangkaian keseluruha bit-plane yang digunakan sebagai unit dasar dari video yang akan dimodelkan dengan sebuah aliran bitplane. Kemudian Prosedur penyisipan watermark ditentukan dari 2 buah rangkaian m-frame. Rangkaian m-frame pertama membuat urutan yang acak semu dalam aliran bitplane. Watermark yang akan disisipkan, ditentukan sebagai frame sebanyak m (*m-frames*), untuk kemudian men-*supplant* rangkaian bitplane-bitplane yang telah diberi tanda.

Video yang telah di watermark harus cukup tangguh dari serangan noise dan dari upaya pengubahan konten video, seperti *subsampling* dan penggantian urutan frame.

Kedua metode ini ([9] dan [8]) menyebarkan isi watermark ke semua piksel di dalam setiap frame dan tidak tergantung konten-video dijital yang akan disisipkan didalamnya.

Niu et al. [7]. juga telah memperkenalkan sebuah skema video watermarking yang baru. Skemanya yaitu dimana informasi watermark akan disisipkan kedalam piksel-piksel sepanjang *temporal-axis* didalam sebuah Segmen Watermark Minimum (SWM). Ketangguhan dari teknik yang diperkenalkan oleh Liu ini bisa dibilang bagus, tetapi Prosedur pengungkapan informasi watermark yang telah disisipkan sangat menguras waktu dan informasi watermark tidak dapat dikembalikan dari sebuah frame tunggal dari video asli.

Banyak algoritma lain memodifikasi koefisien transformasi untuk video watermarking. Beberapa diantaranya menggunakan DCT *(Discrete Cosine Ttransform)*. Beberapa menggunakan DWT *(Discrete Wavelet Ttransform)* sebagai proses transformasi utamanya karena ciri-khasnya yang menggunakan *multiresolution analysis.*

Algoritma Lain [5], memperkenalkan teknik video watermark yang berdasarkan DFT *(Discrete Fourier Ttransform)* untuk suatu

adegan video 3 dimensi. Sebuah watermark dan sebuah template yang sudah ditentukan di-encode menggunakan kunci pribadi untuk memastikan keamanan dari sistem dan disisipkan dalam nilai 3D DFT dari sebuah video yang besar.

Dibandingkan dengan Pendekatan ranah frekuensi tersebut (DFT) yang membutuhkan proses perhitungan yang lama dan sulit, *spatial watermarking* cenderung lebih mudah dan cepat di implementasikan dalam watermark dengan media video, maka dari itu, cocok untuk video dijital. Lagipula, diharapkan bahwa watermark akan disisipkan secara adaptif, dengan pertimbangan data watermark yang telah disisipkan bisa dikenali dan diungkap tanpa membandingkan dengan video aslinya. Tetapi kebutuhan tersebut menghadirkan masalah baru yang tak dapat dihindari khususnya untuk algoritma adaptif. Kebanyakan skema video watermarking tidak dapat menjawab permasalahan *blind* tersebut, yang mengharuskan tidak boleh ada pembanding video aslinya.

Di Makalah ini diperkenalkan pendekatan baru untuk video watermarking yang berdasarkan ranah spasial untuk video yang tidak ter-*compress* dengan format tertentu. Watermark akan disisipkan beberapa kali kedalam konten video dijital. Berdasarkan perancangan *blok-classifier* yang sederhana, blok-blok berbeda dari konten video asli dipisahkan menjadi kategori perseptual yang berbeda berdasarkan informasi gerakan dan kerumitan daerah dari frame yang terdapat dalam video tersebut. Jadi, lokalisasi dari watermark disesuaikan secara adaptif dengan pertimbangan sistem penglihatan manusia dan karakteristik dari sinyal video tersebut, yang membuatnya tidak tampak secara kasat-mata dan tidak mudah dilakukan penghapusan watermark.

Pendeteksian watermark dan pengungkapan watermark tidak membutuhkan video asli. Malahan, informasi tambahan tentang sinyal sinkronisasi yang biasanya ada dalam kebanyakan algoritma video watermarking tidak diperlukan untuk skema ini. Strategi pengungkapan watermark berdasarkan banyak frame memastikan bahwa watermark bisa diungkap dengan benar dari sebuah segmen video yang cukup kecil.

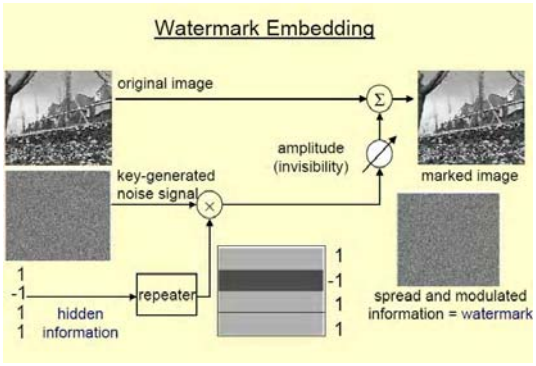
Sejumlah kecil frame yang diungkap dari video yang sudah diwatermark juga mengandung informasi watermark.Hasil percobaan menunjukkan bahwa waermark yang telah disisipkan tangguh dan tidak tampak oleh sistem penglihatan manusia.

2. Penjelasan Masalah

2.1. Video Watermarking Secara Umum

Video watermarking adalah upaya penyembunyikan informasi lewat konten video dijital, tujuan utamanya adalah mengendalikan penyebaran dari konten video dijital tersebut, dan membuat otorisasi dari pembuat video tersebut. Hal ini kerat kaitannya dengan Hak Atas Kekyaan Intelektual, dan Hak Atas karya Cipta.

Beberapa teknik yang bisa dilakukan dalam video watermarking adalah *Robust* dan *Blind* Video watermarking. yang akan dijelaskan dalam pada pembahasan selanjutnya.



2.2. Robust Watermarking

Robust watermarking adalah sebuah sistem waermark 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 dirubah isinya kecuali dengan merusak isi data aslinya juga,

sehingga waermark yang sudah disisipkan tidak dapat diungkap lagi..

2.3. 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 di watermark, sebagai acuan pembanding, hal ini dimungkin kan dan djielaskan dalam makalah ini.

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 dijital tersebut.

3. Teknik Watermarking Yang digunakan

3.1. Adaptive Embedding

Teknik *Adaptive Embedding* yang dilakukan yaitu menyisipkan informasi watermark ke dalam daerah di dalam frame bergantung kriteria tertentu yang sudah ditentukan, penyisipannya berdasarkan dua kriteria, kriteria berdasarkan detail dari daerah, dan pergerakan pada suatui daerah, hal ini aka dijelaskan lebih lanjut dalam Teknik penyisipan watermark

4. Aspek yang perlu diperhatikan

- Ketidaktampakan watermark dalam citra diam dalam video
- Ketidaktampakkan watermark dalam frame yang berhenti
- Penyisipan watermark yang sama dalam frame, mengakibatkan mudah diserang
- Penyisipan watermark yang benar-benar berbeda dalam frame yang berurutan sangat tidak aman.
- Penekanan kepada frame-frame yang berurutan dalam sebuah cuplikan video yang akan diberi watermark, *attacker* bisa mendapatkan informasi dai kedua frame yang bersesuaian.
- Kapasitas watermark dalam video, tentukan batas-batas kritisnya. dimana video tidak dapat menampung berkas berukuran tertentu.
- Sinkronisasi video dan audio setelah diwatermark tetap menjadi pertimbangan, seharusnya setelah disisipi watermark, tidak terjadi ketidaksesuaian antara video, audio juga subtitle (optional) pada video yang diwatermark.

5. Skema Penyisipan Watermark

Dalam bagian ini akan dijelaskan skema penyisipan watermark lebih detail. Ada tiga isu utama dalam skema penyisipan watermark. yaitu *adaptive selection* dari wilayah yang akan dilekatkan berdasarkan DCT, pembagkitan watermark dan proses melekatkan watermark

5.1. Pemilihan bagian yang akan di watermark berdasar DCT

Untuk Watermark dengan citra, telah banyak algoritma adaptif yang telah diperkenalkan untuk memenuhi aspek terpenting dari watermarking, yaiut ketangguhan (*robustness*) dan ketidaktampakkan (*transpaency*). Namun metode-metode itu tidak bisa secara mudah diterapkan dalam data video. Di sisi lain dalam data video, masalah visibility dipandang lebih penting daripada watermarking dengan citra. Sebuah skema watermarking yang buruk dapat memunculkan masalah dalam visual, karena video tidak dapat dipandang sebagai citra tunggal, misalnya terjadi *flicker* dalam video

yang telah di watermark. Untuk itu dibutuhkan sebuah skema yang lebih mangkus dan sangkil, yang bisa menentukan lokasi di data video yang akan di watermark, disesuaikan dengan konten video, dan harus cocok dalam implementasi *real time* (seperti video streaming).

Dalam skema ini, Sebuah *block-classifier* dalam penyisipan watermark dirancang berdasarkan DCT (*Discrete Cosine Transform*) dan sistem pennglihatan manusia. Sebelum benar-benar menyisipkan informasi watrermark, akan digunakan kelebihan dari informasi yang ada di kedua frame, inter frame, dan intra frame yang ada dalam konten video dijital. Informasi yang ada dalam kedua frame itu kemudian akan menentukan wilayah mana saja yang akan disisipkan watermark, dan harus menjamin ketidaktampakan dari watermark .

Penelitian telah dilakukan [10], dalam model *psycho-visual*, dan fokus utama nya adalah model *spatial-masking* untuk citra tunggal (diam). Sudah diketahui bahwa kapasitas watermark kecil dalam wilayah citra yang aktifitas nya sedikit, maksudnya datar. dan besar dalam wilayah citra yang banyak aktifitasnya seperti wilayah bertekstur dan banyak sisinya.

Untuk watermarking dengan video. terlihat bahwa rangakaian video mempunyai kapasitas yang lebih besar untuk penyisipan watermark, dan mempuyai dimensi lebih banyak daripada watermark dengan citra.

Tapi dari banyak riset yang dilakukan, menunjukkan bahwa fitur yang paling harus diperhatikan dalam rangakaian video adalah peningkatan sensitivitas untuk merubah konten video lewat proses watermark. Jadi, kebutuhan untuk ketidaktampakkan dari watermark menjadi lebih penting.

Untuk alasan itulah. video stream harus diproses lebih cermat daripada citra. misalnya; penurunan kualitas video setelah di watermark harus benar-benar dihindari dan harus mempertimbangkan efek *temporal masking* juga.

Studi tentang psiko-visual mengindikasikan bahwa mata manusia memiliki tingkat kepekaanyang berbeda untuk beberapa keadaaan objek visual. Misalnya, mata manusia tidak sensitif terhadap distorsi dalam wilayah citra yang bertekstur tinggi, dan mata manusia tidak bisa melihat detail dari objek yang bergerak cepat.

Dalam skema watermark yang diajukan dalam makalah ini, berdasarkan heuristik yang telah disebutkan tentang psiko-visual, bahwa blok yang mengandung informasi detail dan berganti dengan cepat dalam sumbu temporal (pergerakan yang cepat), adalah cocok untuk disisipkan watermark.

Tujuan nya adalah memilih kandidat kandidat ini untuk penyisipan watermark selanjutnya. Untuk mencapai tujuan tersebut, ada dua kriteria yang diajukan disini. Pendeteksian gerakan, dan mekanisme pendeteksian tingkat ke-detail-an

Ada banyak algoritma pendeteksian gerakan dan pendeteksian sebuah detail, mulai dari yang cukup sederhana, seperti *Background substraction method* dan *sobel operator* sampai yang cukup rumit, seperti *wavelet-base schemes* [23].

Karena algoritma yang diajukan dalam makalah ini akan diaplikasikan pada data video, dan ditujukan untuk aplikasi waktu nyata. Kakas yang digunakan untuk pendeteksian tersebut harus bisa berjalan dengan cepat. Karena pertimbangan tersebut, akan dibuat sebuah algoritma untuk mekanisme pendeteksian dalam domain DCT.

Domain DCT adalah kakas yang cukup tangguh yang bisa dioptimalkan unyuk pemrosesan dan analisis sinyal

Juga karena mempunyai kompleksitas perhitungan yang rendah sehingga bisa diterapkan dalam sistem waktu nyata. Disamping itu, karena DCT biasanya digunakan dalam mode blok dari pada keseluruhan citra, seperti pendeteksian berdasarkan blok, dan pendekatan klasifikasi, memungkinkan untuk mengendalikan *local-spatial* dari ketangguhan watermark.

Untuk meminimalisasi kerumitan proses komputasi untuk pengklasifikasian blok. Skema ini mengimplementasikan kedua kriteria tadi berdasarkan nilai dari koefisien DCT untuk sebuah blok yang ditransformasikan. Term DC dari koefisien adalah *mean gray value* dari sebuah blok dan menandakan properti dasar dari konten dalam sebuah blok.

Jadi perbedaan antara koefisien DC yang bersesuaian dalam frame yang berdekatan

bisa dikatakan sebagai kriteria pendeteksian sebuah gerakan.

Sebaliknya. Dalam sebuah blok dengan perubahan cepat dalam piksel-piksel yang bertetangga. Energi sinyal cenderung terpusat di koefisien AC. Sehingga nilai dari koefisien DCT AC dari sebuah blok yang ditranformasikan bisa digunakan sebagai kriteria dasar dalam pendeteksian detail untuk menentukan blok mana yang mengandung informasi dengan detail tinggi.

Beberapa metode pendeteksian juga dapat digunakan. Namun tes menunjukkan 2 kriteria yang digunakan tadi memenuhi aspek keakuratan dalam klasifikasi dan kompleksitas komputasi yang tidak terlalu *overload.*

Prosedur pemilihan blok secara lebih lengkap dirumuskan dalam gambar 1. Misalkan ada sebuah potongan rangkaian video yang mengandung frame sebanyak k. Ukuran setiap frame adalah $m \times n$ dan X_i menyatakan frame ke i dalam video aslinya. dimana $i = 0,1,2,3,...,k-1.$

Pertama-tama. Frame yang sedang diproses dipecah menjadi 8×8 blok yang terpisah, dinyatakan dengan $X_{i,i}$ berarti blok ke j dalam frame ke i. (disini dilakukan traversal keseluruhan frame dengan cara raster-scan), dimana $j = 0,1,2,3,...,\lfloor m \times n / 64 - 1 \rfloor.$

Untuk setiap blok $X_{i,i}$ tadi. Dilakukan transformasi DCT, lalu diadapat blok $\hat{X}_{i,j}$ yang sudah di transformasi. Koefisien DCT berkisar dari frekuensi terendah sampai frekuensi tertingginya. Misal $\hat{X}_{i,i,0}$ adalah sebuah koefisien DC. Lalu proses klasifikasi blok dilakukan dalam dua tingkat. dalam tingkat intra-frame, blok di klasifikasikan menjadi 2 kelas menurut energi dari koefisien AC dalam domain 2-D DCT transformasi yang disebut kriteria pendeteksian detail nya. Energi dari koefisien AC dalam blok $X_{i,i}$ dinyatakan dalam persamaan berikut :

$$E_{AC}(i,j) = \sum_{k=1}^{63} \left(\hat{X}_{i,j,k} \right)^2 \quad (1)$$

Untuk setiap blok $\hat{X}_{i,j}$. Jika nilai dari $E_{AC}(i,j)$ kurang dari nilai T_D yang sudah ditentukan sebelumnya, blok $X_{i,i}$ diklasifikasikan sebagai kelas dengan detail rendah.

Jika Tidak, $X_{i,i}$ diklasifikasikan sebagai kelas dengan detail tinggai yang dinyatakan sebagai himpunan S_1

$$S_1 : \{ X_{i,d_1}, X_{i,d_2}, ..., X_{i,d_p} \}$$

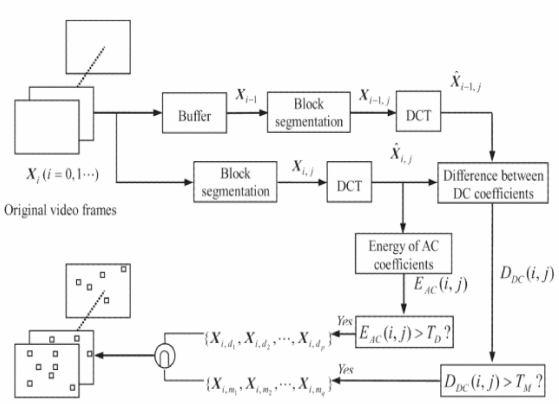
Dalam tingkatan inter-frame, blok $\hat{X}_{i,j}$ yang telah ditransformasikan di frame yang sedang diproses harus dibandingkan dengan frame-frame tetangganya.

Dalam kasus ini hanya dipertimbangkan frame sebelum frame ke $(i-1)$ untuk kemudahan.

Sebagaimana dihitung dalam rumus (1). koefisien DC dari blok yang bersesuaian dalam 2 frame yang berurutan dipilih dan kemudian di bandingkan.

Disini definisi dari $D_{DC}(i,j)$ diberikan dalam persamaan berikut. yang menunjukkan perbedaan nilai mutlak dari koefisien DC dari blok yang bersesuaian dan nilai ini disebut **kriteria pendeteksian gerakan**.

$$D_{DC}(i,j) = \left| \hat{X}_{i,j,0} - \hat{X}_{i-1,j,0} \right| \quad (2)$$



Gambar 1 Diagram dari prosedur seleksi adaptif

Dalam kasus ini jika $D_{DC}(i,j)$ kurang dari nilai T_M yang sudah ditentukan sebelumnya, blok $X_{i,i}$ dari frame yang sedang diproses diklasifikasikan sebagai kelas *slow motion*, jika tidak (lebih), $X_{i,i}$ diklasifikasikan menjadi kelas *fast motion*. Yang dinyatakan dalam himpunan S_2

$$S_2 : \{X_{i,m_1}, X_{i,m_2}, ..., X_{i,m_q}\}$$

Untuk setiap frame, hanya blok-blok yang berada dalam irisan himpunan S_1 dan S_2 yang akan dipilih sebagai tempat melekatkan watermark, yang dinyatakan dalam himpunan S_3

$$S_3 : \{X_{i,e_1}, X_{i,e_2}, ..., X_{i,e_n}\}$$

Yang akan dipilih sebagai tempat penyisipan frame.

Frame-frame selanjutnya kemudian mengikuti proses yang telah di sebutkan di atas. Disini Frame awal diwatermark sebagai citra tunggal. tanpa ada acuan frame sebelum dan sesudah nya. Nilai T_D dan T_M yang sudah didtentukan di awal dipilih berdasarkan keseuaian dari kualitas video dan redundansi dari watermark.

5.2. Pembangkitan Watermark

Bit-bit pesan yang dilekatkan dalam data-video biasanya didapat dengan fungsi hash satu arah. Bit-bit tersebut bisa menyatakan informasi tentang kepemilikan atau sidik dari informasi tersebut

Panjang dari bit-bit pesan b_i dimana $b_i \in \{0,1\}$ ditentukan sebesar 64. Angka tersebut tidak hanya memenuhi kebutuhan EBU [3], tetapi cocok dengan ukuran dari setiap blok.

Harus diperhatikan bahwa kapasittas watermark bisa melebihi jumlah yang normal jika dilakukan penyebaran informasi watermark melalui sebuah subset dari kandidat-kandidat blok dan misalnya dalam kasus, konsep *direct sequence spread spectrum* atau teknik *coding-correction* bisa digunakan.

Untuk meningkatkan keamanan sebuah sistem watermark, bit-bit pesan watermark dibangkitkan dengan cara permutasi oleh sebuah *key-controlled* rangkaian bilangan pseudo-random.

Tanpa kunci yang valid. Seorang Attacker akan susah untuk mendapatkan pesan watermark, bahkan dia mengetahui wilayah yang akan disisipkan (*embedding-regions*) dan mendapatkan rangkaian permutasi.

Lebih lanjut, rangkaian dari 1-Dimensi dibentuk ulang dalam 2-Dimensi, sehingga teknik bitplane masih bisa diterapkan. Kita mengacu ke pola 2-Dimensi ini, pola W_k, sebagai watermark yang akan disisipkan.Proses pembangkitan watermark ditunjukkan di gambar 2

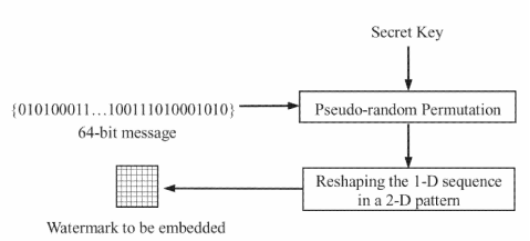
5.3. Penyisipan watermark

Skema pelekatan informasi watermark yang dijelaskan dalam makalah ini berada dalam spatial domain, bukan dalam ranah transform ataupun ranah video yang ter-*compress* dengan format tertentu.

Pemilihan spatial domain ini dapat dengan jauh mengurangi kompleksitas komputasi. Tidak

seperti metode watermarking yang dilakukan dalam domain spatial lainnya, seperti penggantian LSB, penambahan piksel demi piksel, metode ini menggunakan Teknik Penggantian Bit Plane untuk melakukan prosedur penyisipan watermark.

Selain itu, untuk meningkatkan ketangguhan watermark dari kompresi MPEG-2 yang kutang baik. dan penambahan *noise*. watermark dilekatkan dengan redundansi (dilakukan leih dari satu kali).



Gambar 2 Diagram prosedur pembangkitan watermark

Disini kita akan menyispkan watermark kedalam komponen "yang bersinar" dari sebuah video yang tidak terkompres dengan format tertentu dan mengambil satu frame tunggal sebagai contoh. Sebagaimana ditunjukkan di gambar 3.

untuk daerah yang telah dipilih untuk menyisipkan watermark. Setiap Blok X_{i,e_j} bisa di dekomposisi menjadi 8 bitplane (bitplane terendah ditandai dengan nomor 0 dan yang tertinggi ditandai dengan 7).

Dengan beroperasi di level bit plane. kandidat-kandidat dari bitplane untuk watermarking dipilih berdasarkan dari pengaruh penggantian terhadap kualitas citra. dan ketangguhan terhadap serangan.

Di sisi lain, hasil percobaan yang dilakukan menunjukkan bahwa, watermark praktis menjadi tak-tampak jika dilekatkan pada bit ke tiga atau bit sebelumnya. (0,1,2).

Sebaliknya, bit yang lebih rendah adalah lebih mudah terpengaruh noise dan kompresi, ketika bitplane yang lebih tinggi diharapkan relatif tahan dari gangguan-gangguan tersebut.

Jadi bitplane yang lebih tinggi dari pada bit LSB bisa dipilih menjadi kandidat untuk pelekatan watermark. Dalam makalah ini, karena daerah yang dipilih lebih mempunyai karakteristik *masking* (cenderung tak terlihat), watermark bisa diletakkan pada bit plane pertengahan. Hal ini menjamin bahwa, watermark yang dilekatkan tidak tampak selagi tetap memperhatikan kemungkinan robustness tertinggi.

Untuk meningkatkan keamanan sistem lebih lanjut. Ada sebuah pengendali posisi bitplane dalam proses pelekatan watermark. Pengendali ini membangkitkan sebuah *pseudorandom pointer* yang mencegah bitplane-bitplane individual ke daerah yang telah dipilih dan menggantinya dengan pola watermark yang akan disisipkan

.

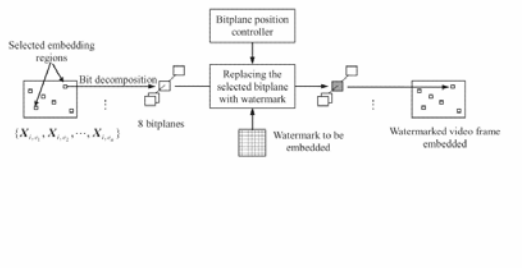
Pointer ini mempunyai banyak pilihan dan bergerak diantara bitplane- bitplane pertengahan, biasanya ke-2 ke-3 dan bitplane ke-4.

Dalam kasus ini. Untuk meningkatkan *robustness* dalam mempertahankan sifat tak bisa di indera dengan mata, Akan dispesifikasikan penyebaran dari lokasi watermark mendekati distribusi Gaussian.

Dengan kata lain. bitplane ke-3 dipilih dengan kemungkinan terbesar (0.6), sementara bit ke-2 dan ke-4 dengan kemungkinan lebih kecil (masing- masing 0.2).

Mekanisme pengendalian ini cukup sederhana dan mudah di implementasikan, tetapi menyediakan sebuah perlindungan yang efektif dari penghapusan watermark.

Misalnya, watermark susah dihapuskan jika tidak mengakibatkan penurunan kualitas video secara signifikan.



Gambar 3 Diagram prosedur penyisipan watermark

6. Pendeteksian Watermark dan Algoritma Ekstraksi

Dua metode telah dikembangkan untuk mengekstrak watermark potensial dari sebuah rangkaian video uji atau frame video uji. Kedua metode tersebut bisa dibagi menjadi 2 langkah : pendeteksian watermark dan pengekstraksian.

Perbedaan utamanya adalah dalam pendeteksian watermark menggunakan video asli sebagai sebuah acuan pembanding selama pendeteksian, dimana yang ke dua tidak membutuhkan video asli dalam proses pendeteksian (*blind watermarking*).

6.1. Pendeteksian Watermark

6.1.1. Dengan akses video asli

Pendeteksian otorisasi dari informasi yang telah disembunyikan bisa didapatkan dengan mudah menggunakan data video yang asli.

Dengan melakukan kriteria seleksi yang terlah disebutkan diatas dengan nilai T_D dan T_M yang telah ditentukan.

Daerah Pelekatan dari video yang telah di watermark $\{X'_{i,e_1}, X'_{i,e_2},..., X'_{i,e_n}\}$

Bisa didapatkan. yang pada dasarnya identik dengan daerah-daerah itu selama dilakukan proses penyisipan.

Selanjutnya untuk setiap frame yang diwatermark, dekomposisi masing masing masing blok $X'_{i,e_j}\ j \in \{1,2,3,...,n\}$ menjadi 8 bitplane.

$$X'_{i,e,_j} = \sum_{l=0}^{7} X'_{i,e_j}(l) \quad (3)$$

Dan hitung nilai keterhubungan antara pola watermark W_k dan yang ke- 2 (3 dan 4 seterusnya)

$$r_l = X'_{i,e_j}(l) \otimes W_k, l = 2,3,4 \quad (4)$$

Disini operator $\otimes$ adalah korelasi di posisi (0,0) pada 2-Dimensi. dan korelator akan membangkitkan respons maksimum dari 64. tanpa adanya gangguan pada video.

Kemudian nilai r_l yang bersesuaian dibandingkan dengan nilai T_C yang telah ditentukan berdasarkan kondisi

$$\begin{cases} r_l \geq T_C \\ r_l \leq T_C \end{cases} \quad r_l \geq T_C \text{ ada watermark}$$

Jika pendeteksi *response* melebihi nilai T_C yang telah ditentukan. kita menduga bahwa ada watermark yang terdeteksi dan menyimpan bitplane yang bersesuaian $X'_{i,e_j}(l)$ dalam himpunan S_4 yang didefinisikan.

$$S_4 : \{X'_{i,e_1}(l), X'_{i,e_2}(l),..., X'_{i,e_r}(l)\}, l \in \{2,3,4\}$$

untuk proses selanjutnya akan di ekstraksi dari video yang diwatermark, jika kurang maka ditolak, dan diperlakukan sebagai video rusak atau tak ada watermark nya. Proses seperti ini terus berlanjut hingga akhir video.

Pada kenyataannya, menggunakan sinyal video yang asli untuk mendeteksi ada atau tidak adanya watermark, Beberapa distorsi yang umum dapat ditangani seperti *crop*, *scaling*, *frame drop*, dan *frame swap.*

Tetapi untuk aplikasi seperti transmisi TV digital dan distribusi *video on demand*. Adalah hampir tidak mungkin untuk menyimpan keseluruhan data video yang ukurannya cukup besar. untuk kemudian dibandingkan. Sehingga harus dilakukan metode pendeteksian yang lain, yaitu *blind detection.*

Dalam makalah ini juga jelaskan skema kedua tanpa menggunakan data video asli sebagai pembanding.

Pada khususnya. Tidak ada informasi mengenai *temporal axis* yang diperlukan. misalnya. kita tidak perlu menentukan titik awal atau urutan urutan sebenarnya dari frame-frame video.

6.1.2. Tanpa akses video asli

Sedikit modifikasi dari teknik yang pertama (pendeteksian tanpa menggunakan video asli sebagai pembanding), hanya kriteria pendeteksian detail yang akan diterapkan pada video yang telah di watermark selama proses pendeteksian watermark.

Dengan menerapkan kriteria konten-dependen menggunakan rumus

$$E'_{AC} = \sum_{k=1}^{63} \left(X'_{i,j,k} \right)^2 \qquad (6)$$

dan kemudian dibandingkan hasilnya dengan nilai T_D yang telah ditentukan sebelumnya. Dari penghitungan tersebut, didapat himpunan kandidat S_5

$$S_5 : \left\{ X'_{i,e_i}, X'_{i,e_2}, ..., X'_{i,e_8} \right\}$$

Perhatikan bahwa selama pendeteksian nilai treshold T_D yang telah ditentukan sebelumnya dinyatakan dengan T'_D untuk menekankan bahwa nilai T'_D disini sebenarnya kurang dari nilai T_D yang digunakan sebelumnya.

Dengan cara ini dapat dipastikan bahwa sebagian besar dari daerah penyisipan mungkin ada didalam himpunan kandidat S_5.

Kemudian untuk setiap blok di S_5, pendeteksian korelasi yang sama dilakukan pada bitplane- bitplane pertengahan sebagaimana telah disebutkan pada metode pertama. dan nilai yang berkorelasi lebih besar dari T_C mengindikasikan adanya keberadaan watermark.

Serupa dengan hal itu, bitplane yang berkorelasi juga disimpan dalam S_4 untuk selanjutnya digunakan dalam langkah kedua.

Perhatikan bahwa, dalam banyak kasus. *attacker* mungkin ingin membuat video rusak, dengan cara mengubah ukuran video, caranya. mengurangi frame atau menginterpolasi sebuah frame. Dengan demikian video menjadi tidak normal lagi. Malahan, dalam serangan lain si pembajak mengubah urutan frame, hal ini akan dijelaskan lebih lanjut dalam bagian serangan.

Skenario tersebut memunculkan suatu tantangan untuk *blind detection.* Pelekatan dari sebuah sinyal sinkronisasi akan sangat membantu, tetapi hal itu juga meningkatkan kemungkinan diserang.

Karena kriteria pendeteksian detail lebih tergantung dari konten daripada struktur video yang merupakan 3-Dimensi itu sendiri, metode ini tidak sensitif terhadap serangan desinkronisasi pada sumbu temporal. Dengan kata lain Jika dilakukan penyerangan berupa

pengacakan frame, pengambilan frame, atau interpolasi frame yang tidak mengakibatkan penurunan kualitas video secara signifikan. Akan selalu mungkin dilakukan proses pengungkapan watermark.

6.2. Ekstraksi Watermark

Setelah lokasi dari watermark ditentukan, strategi pengekstraksian watemark yang mudah bisa diterapkan. Hal ini sama untuk kedua metode.

Perhatikan posisi pelekatan dari sebuah pola watermark, Semua sisa bitplane2 dalam S_4 di beri bobot dan dikombinasikan. Hal ini berguna tidak hanya untuk membebaskan efek dari kompresi atau penambahan noise, tetapi juga mengeksploit keberagaman dari watermark secara menyeluruh.

Kita menyatakan deskripsi prosedur pengekstraksian dalam persamaan berikut

$$W* = \sum_{\mathbf{S_4}} \frac{w_{i,\ e_j}(l)}{\sum_j w_{i,\ e_j}(l)} X'_{i,\ e_j}(l) \tag{7}$$

dimana $w_{i,e_j}(l)$ menyatakan nilai bobot dari setiap bitplane $X'_{i,e_j}(l)$ dan bisa dinyatakan dalam

$$w_{i,\ e_j}(l) = 2^l,\ l \in \{2,\ 3,\ 4\}$$

Lebih lanjut, watermark dapat diungkap dari sebuah segmen video yang sangat pendek, dan bisa dimulai dari lokasi yang acak.

$$W** = \sum_i \sum_{\mathbf{S_4}} \frac{w_{i,\ e_j}(l)}{\sum_i \sum_j w_{i,\ e_j}(l)} X'_{i,\ e_j}(l)$$

Disini hasil kombinasi di konversi kedalam bentuk binari. Akhirnya, permutasi pseudorandom dibalik dengan nilai kunci yang telah ditentukan dan bit pesan yang akan dilekatkan bisa didapatkan dari $W*$ atau $W**$

7. Hasil Pengujian

Untuk Membuktikan kemangkusan dari skema watermarking yang dibahas dalam makalah ini, dilakukan sebuah simulasi pengujian terhadap 2 video beresolusi rendah CIF (*Common Intermediate Format)*), rangakaian video "Kalender dan mobil" dan "Tenis meja". Gambar CIF terdiri dari tiga komponen : satu komponen Y yang berpendar, dan 2 komponen *chrominance* Cb dan Cr.

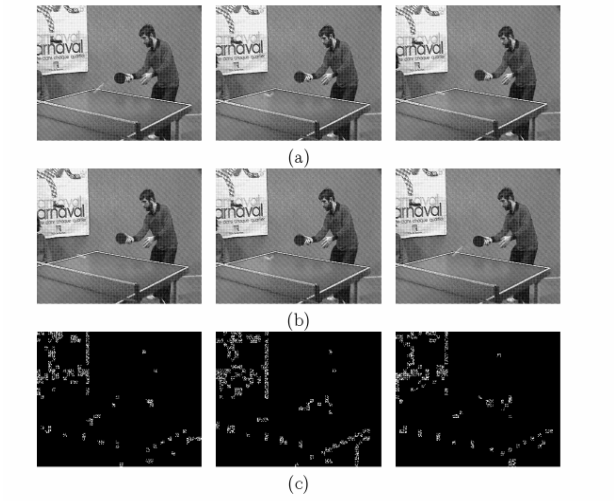
Ukuran gambar nya 352x 288 piksel dimana untuk Cb dan Ce di sesuaikan menjadi 176 x 144 piksel. Hanya elemen yang bercahaaya yang diperhatikan dalam proseur pengujian, dalam percobaan nilai T_D = 1200 T_M = 80, T_C = 40, dan T'_D =1000.

Gambar 4 menunjukkan contoh frame untuk evaluasi subjektif dari kualitas video. Baris teratas terdiri dari tiga frame yang berurutan dari video tenis meja. Baris tengah terdiri dari frame yang sudah diwatermark dari frame sebelumnya. Bagian bawah menggambarkan perbedaan frame absolut berdasarkan frame yang asli dan yang sudah diwatermark. (dikuatkan untuk agar bisa dilihat dengan indera penglihatan), dan daerah yang cerah menggambarkan nilai yang besar.

Tabel 1 menunjukkan nilai PSNR dari 30 frame dari video tenis meja yang sudah diberi waermark. Dapat kita lihat bahwa distorsi akibat penyisipan watermark tidak bisa di indera dengan mata. Nilai-nilai maksimum, minimum dan rata-rata untuk semua frame yang telah

diwatermark berturut-turut 44.4 dB, 42.6 dB, dan 43.5 dB.

Dari percobaan yang dilakukan, dengan mem-*playback* di pemutar video semua frame yang sudah di watermark, secara keseluruhan tidak bisa dilihat oleh mata. Tidak ada kerlip dalam video, karena dilakukan penyisipan informasi di daerah dengan pergerakan kompleks yang cepat.



Gambar 4 Tiga Frame dari video tenis meja, (a) videoa asli, (b) video yang sudah di watermark, (c) dengan perbedaan frame absolut

Karena video dijital biasanya dalm format terkompresi dengan MPEG-2 dan disimpan dan disebarluaskan dalam format terkompresi, dilakukan juga pengujian terhadap ketangguhan watermark pada MPEG-2.

Ada dua sampel video dalam format terkompresi MPEG-2 yang diuji, pengujiannya menggunakan *source-code* dari *codec (coding and decoding)*, hasilnya dapat dilihat pada tabel 2. Dapat dilihat bahwa informasi waermark bisa diungkap dengan baik dari GOP (Group Of Pictures) dan frame-frame terpisah.

Ditemukan juga sedikit kesalahan bityang terjadi dalam bit rate 4Mbps *coding*, hal ini bisa dieksplor lebih lanjut, teknik *error correction coding*, untuk meningkatkan robistness dari algoritma video watermarking ini.

Dilakukan juga pengujian ketangguhan watermark terhadap serangan video yang umum. Sebuah sinyla video biasanya mengalami serangan *indexing*. Proses perekaman dan ketidaknormalan yang lain mungkin pada kenyataannya acak, apakah itu reguler ataupun *frame-dropping* pada frame yang berurutan.

Frame number	PSNR (dB)									
Frame 0 – Frame 9	43.23	44.07	44.39	43.63	43.24	43.66	43.52	43.55	43.22	42.90
Frame 10 – Frame 19	42.63	43.74	43.17	43.95	43.03	42.57	42.86	43.97	43.63	43.57
Frame 20 – Frame 29	43.88	43.10	44.32	43.30	43.07	43.57	43.63	43.64	44.03	43.14
Average	43.47									

Gambar 5 Nilai-nilai dari 30 frame yang diwatermark dari video "tenis meja"

Proposed method	Sample video	MPEG-2 coding bit rate	Percentage of bits correctly recovered			
			Extracted from GOP	Extracted from individual frames		
				Min	Max	Average
Non-blind detection and extraction	Mobile & Calendar	6M bits/s	100%	100%	100%	100%
		4M bits/s	100%	96.9%	100%	98.8%
	Table Tennis	6M bits/s	100%	100%	100%	100%
		4M bits/s	100%	98.4%	100%	99.5%
Blind detection and extraction	Mobile & Calendar	6M bits/s	100%	100%	100%	100%
		4M bits/s	100%	95.3%	100%	98.1%
	Table Tennis	6M bits/s	100%	100%	100%	100%
		4M bits/s	100%	96.9%	100%	99.2%

Gambar 6 Hasil dari pengungkapan dari frame yang diwatermark terhadap serangan MPEG-2

Sample video	Recovery of watermark information				
	Frame dropping	Frame interpolation	Frame shuffling	Color space conversion	Gaussian noise addition
Mobile & Calendar	OK	OK	OK	OK	OK
Table Tennis	OK	OK	OK	OK	OK

Gambar 7 Hasil dari pengungkapan dari frame yang diwatermark terhadap serangan video yang umum

Sebuah upaya penghilangan watermark bisa melibatkan pengacakan keterkaitan dalam aspek waktu diantara frame-frame.

Untuk skema yang djelaskan dalam makalah ini, serangan desinkronisasi tersebut sepanjang sumbu waktu tidak terlalu berpengaruh terhadap pemulihan dan pengungkapan watermark. Lebih lanjut watermark membuktikan lebih tahan terhadap serangan noise hanya untuk redundansi penyisipan.

Karena watermark disisipkan dalam komponen video yang bercahaya cerah *(luminance)*, konversi dari YCbCr dan RGB atau diantara warna dan hitam-putih-abu-abu berpengaruh besar terhadap pengungkapan watermark.

Tabel 3 menunjukkan hasil dari pengungkapan watermark dari sebuah video yang sudah diwatermark dengan adanya serangan terhadap video tersebut, di tabel 3 dapat dilihat bahwa algoritma yang dijelaskan di makalah ini tangguh terhadap serangan yang berupa *frame-dropping, frame-shuffling, color-*

space conversion dan penambahan *noise* Gaussian.

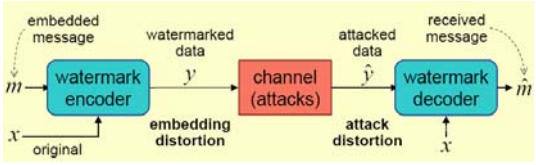
8. Serangan Terhadap Watermarking

Pada bagian ini akan dijelaskan serangan-serangan yang biasa dilakukan terhadap video watermarking, teknik-teknik nya, dan bagaimana penanganan dari serangan tersebut.

Serangan terhadap video watermark adalah suatu proses untuk mendapatkan data yang telah disisipkan secar illegal, untuk kemudian akan dilakukan pengubahan isi dari watermark yang telah disisipkan.

Serangan juga bisa berarti upaya penghilangan data yang disisipkan dalam video dengan cara merusak video asli nya, dengan harapan tidak bisa diungkap informasi yang sudah disembunyikan.

Secara umum diagram penyerangan terhadap video watermarking sebagai berikut



pesan m yang akan disampaikan seharusnya identik dengan $\hat{m}$.

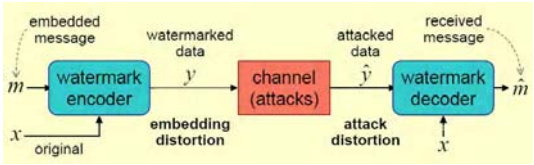
Ukuran ketangguhan dari suatu watermark adalah sejauh mana pesan m itu tidak berubah dalam mengalami serangan-serangan sebelum pengungkapannya.

Ketangguhan dari suatu sistem watermark mudah ditentukan tetapi sulit dievaluasi, karena pesan yang sudah disisipkan tidak bisa dihapus atau dirusak isinya dengan tidak membuat data aslinya rusak juga.

Sebuah sistem video watermark dikatakan tangguh apabila Komunikasi yang terjadi (pesan yang disisipkan) tidak bisa dirusak kecuali membuat data yang diserang menjadi tidak bermakna. Dan hendaknya asumsi awal terhadap suatu penyerangan adalah, pihak lawan mengetahui strategi kita (algoritma dan implementasi sistem watermark kita) tetapi tidak mengetahui kunci untuk mengungkap watermark tersebut.

Distorsi yang terjadi selama proses penyerangan watermark bisa diukur. Data asli bisa dianggap rusak atau tidak tergantung seberapa besar distorsi yang terjadi.

Proses distorsi dapat terjadi pada 2 tahap, pada tahap penyisipan dan tahap penyerangan, bisa dilihat di gambar berikut



Secara umum ada 4 jenis serangan terhadap watermarking

a) Simple waveform processing

Jenis ini bekerja dengan pendekatan *brute-force*, biasanya merusak watermark dan data aslinya, yang dilakukan adalah : kompresi, *linear-filtering*, penambahan *noise*, dan *quantization*

b) Advanced removal

Prosesnya bertujuan merusak dan secara khusus mengalahkan watermark, tujuan utamanya mengapuskan watermark. membuat watermark tiruan didalam konten asli, sehingga terjadi *collision* dan watermark sebenarnya tidak dapat diungkap

c) Detection-disabling methods

Membuat kekacauan dalam *synchronization* seperti keterkaitan frame dengan waktu tertentu, dengan melakukan transformasi geometri, pemotongan video, ataupun pengacakan frame.

d) Ambiguity / deadlock issues

Hampir sama dengan *advanced removal* tetapi, penciptaan watermark palsu bertujuan

untuk mengungkap watermark sebenarnya dari sinyal watermark yang didapat

9. Kesimpulan

Di makalah ini telah diperkenalkan sebuah algoritma watermarking yang adaptif. Video Watermarking ini diperuntukkan bagi perlindungan Hak-cipta dalam komunikasi yang menggunakan media video.

Ketimbang menyisipkan informasi watermark kedalam domain transformasi atau dalam ranah video yang ter-*compress*. Sebuah pendekatan baru untuk watermark berbasis ranah spasial untuk video yang tidak ter-*compress*.

Digunakan dalam skema yang dijelaskan dalam makalah ini mengurangi kompleksitas perhitungan. Algoritma watermarking yang dijelaskan adalah content-adaptive, malahan tidak perlu menggunakan video asli untuk pendeteksian sebuah watermark.

Di sisi lain. di makalah ini digunakan strategi pengungkapan berbasis multi-frame, sehingga pengaruh dari kompresi MPEG-2 bisa dikurangi dengan baik. Hasil pengujian menyatakan keefektifan dari teknik penyisipan watermark yang dijelaskan.

10. Daftar Pustaka

[1] M. Kucukgoz, O. Harmanci, M. K. Mıhc¸ak, and R. Venkatesan, "Robust Video Watermarking via Optimization Algorithm for Quantization of Pseudo-Random Semi-Global Statistics," Proc. SPIE 2005, San Jose, CA, 2005.

[2] Kim Dug-Ryung , Park Sung-Han "A Robust Video Watermarking Method" School of Electronics and Computer Engineering, Hanyang University GyungGi Do, Korea, 2004.

[3] Wang Hao-Xian, Lu Zhe-Ming, Pan Jeng-Shyang, Sun Sheng-He "Robust Video Watermarking With Adaptive Embedding Mechanism" Department of Electronic Engineering Harbin Institute of Technology Harbin 150001, P. R. China. 2004

[4] Munir, Rinaldi. Diktat Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung. 2006

[5] Deguillaume, F., G. Csurka, J. J. K. O Ruanaidh and T. Pun, Robust 3D DFT video watermarking, Proc.ofSPIE3657,Security and Watermarking of Multimedia Contents, pp.113-124, 1999

[6] Lin, E. T. and E. J. Delp, Temporal synchronization in video watermarking, Proc. of the SPIE 4675, Security and Watermarking of Multimedia Contents IV, pp.478-490, 2002

[7] Niu, X. M., M. Schmucker and C. Busch, Video watermarking resisting to rotation, scaling and translation, Proc. of SPIE 4675, Security and Watermarking of Multimedia Contents IV, pp.512-519, 2002.

[8] Mobasseri, G., Direct sequence watermarking of digital video using m-frames, Proc. of IEEE International Conference on Image Processing, vol.2, pp.399-403, 1998

[9] Hartung, F. and B. Girod, Watermarking of uncompressed and compressed video, Signal Processing, vol.66, no.3, pp.283-301, 1998

[10] Wolfgang, R. B., C. I. Podilchuk and E. J. Delp, Perceptual watermarks for digital images and video, Proceedings of the IEEE, vol.87, no.7, pp.1108-1126, 1999.