

Teknologi Watermarking yang Kuat pada Video MPEG

Fery Sinambela, Ranto Pramono, dan Krisna Adirama

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if11025@students.if.itb.ac.id, if11031@students.if.itb.ac.id,
if11078@students.if.itb.ac.id

Abstrak

Perkembangan dari layanan multimedia yang baru dan lingkungannya membutuhkan suatu konsep, baik untuk mendukung proses eksekusi yang baru pada komputer yang terdistribusi dan juga untuk melindungi data multimedia selama pembuatan dan pendistribusian dalam bentuk digital. *Paper* ini ditujukan dengan dasar bahwa perlindungan hak cipta sebagai permintaan tingkat keamanan yang paling tinggi dalam pemasaran barang-barang digital. Konsep utama dari *paper* ini adalah untuk menyediakan lingkungan dimana video digital dapat diberi tanda oleh pembuatnya atau produser sebagai properti intelektual untuk memastikan dan membuktikan hak kepemilikan dalam video produksinya baik selama produksi dan distribusi. Untuk mengembangkan tampilan ke perubahan bentuk dari frame watermarking kami mengembangkan suatu tampilan 3D-difference untuk mengukur perubahan yang dibuat selama proses watermarking dan atau disebabkan oleh beberapa serangan yang merusak.

Kata kunci: *Security and the media, digital watermarking for MPEG video, copyright protection*

1. Pendahuluan

Produk-produk video merupakan karya intelektual manusia. Produk ini mencakup film dan musik (video) atau yang disebut dengan multimedia. Berbagai masalah dapat terjadi dengan produk-produk tersebut, seperti penggandaan, pembacaan perubahan (manipulasi) yang semuanya dilakukan dengan cara yang tidak sah (*illegal*). Oleh karena permasalahan tersebut, perancang, produser dan *publisher* berusaha untuk mencari solusi agar produk-produk yang dihasilkan dapat aman dan memperoleh keuntungan yang lebih bagi mereka.

Konsep utama dalam *paper* ini adalah memberikan lingkungan di mana video digital dapat 'ditanda tangai' oleh pengarang

atau produser sebagai karya intelektual mereka untuk membuktikan bahwa karya tersebut adalah benar-benar karya sah mereka.

Teknologi watermarking yang ada pada umumnya diterapkan pada objek gambar, walaupun ada yang diterapkan pada objek video, teknologi watermarking tersebut kurang kuat atau kokoh (*robust*). *Paper* ini berupaya untuk mencari teknologi watermarking yang kuat pada video MPEG.

2. Ruang lingkup

Teknologi watermarking merupakan salah satu teknologi yang digunakan untuk memberikan 'tanda tangan' pada karya digital. Salah satu penerapannya adalah pada bidang multimedia, seperti musik dan film.

Paper ini akan membahas teknologi watermarking pada salah satu cakupan multimedia yaitu video MPEG.

3. Watermarking Dijital

Watermarking digital merupakan teknologi untuk memberikan dan membuktikan hak kepemilikan atas karya digital, mendeteksi *copy* yang sah, mengontrol penggunaan data yang sah dan menganalisis penyebaran data melalui jaringan dan *server*. Tujuan utama mengenai watermarking digital dalam *paper* ini adalah merancang sebuah algoritma yang bisa digunakan untuk semua jenis video dan dapat menyisipkan (*embed*) semua jenis kode informasi, terutama kode *binary*, dalam hal ini *words*

Pada watermarking, label atau kode yang disisipkan ke dalam data multimedia harus unik yang mengidentifikasi pemegang hak cipta dan label tersebut sulit untuk dihapus bahkan setelah beberapa kali transformasi data. Jadi keberadaan data (label) di dalam produk harus dijaga. Teknik pelabelan bertujuan untuk memberikan keamanan dan kekuatan (*robustness*) label yang disisipkan terhadap usaha-usaha sebagai berikut:

- a. Pendeteksian lokasi data yang disisipkan.
- b. Menemukan dan mengubah label yang disisipkan.
- c. *IMB attack*.
- d. Perusakan atau penghapusan label yang disisipkan.

Semua transformasi pada frames dapat menimbulkan kerusakan pada informasi yang disisipkan dan informasi tersebut tidak dapat ditemukan kembali oleh pemiliknya.

Kebutuhan untuk Watermarking pada Video MPEG

Algoritma kompresi MPWG menggunakan teknik pengkodean *Discrete Cosine Transform* (DCT) pada blok 8x8. Hasilnya berupa aliran (*stream*) yang berisi barisan I-, P-, dan B-*frame*.

Berikut ini hal-hal penting yang perlu diperhatikan dalam watermarking pada video MPEG:

- a. Kekuatan vs kompresi tinggi dengan kompresi DCT
- b. Kekuatan vs *scaling*.
- c. Pelabelan setiap *frame* video tunggal (I-, P-, dan B- *frame*) untuk memberikan watermarking yang berkelanjutan dan menghindarkan dari serangan pemotongan *frame* tunggal.
- d. Kebenaran pengkodean frame tanpa *visual artefact*. Perubahan pada I-*frame* mempengaruhi pengkodean B- dan P- *frame*.
- e. *Runtime*, performansi untuk *video streaming* atau penyimpanan video.

4. Algoritma Zhao Koch

Algoritma Zhao Koch menyisipkan label hak cipta ke dalam domain frekuensi. Algoritma ini secara *pseudo random* memilih tiga koefisien dari blok DCT yang di-*encode* dan mengubahnya untuk menyimpan informasi bit tunggal dari label hak cipta menggunakan kunci rahasia. Untuk menyisipkan bit 1 atau 0, Zhao dan Koch mendefinisikan pola yang berbeda, tinggi, sedang, dan rendah sebagai aturan perubahan. Penyimpanan sebuah bit yang mengandung informasi membutuhkan perubahan yang berarti di dalam blok, kemudian koefisien diubah ke dalam bentuk pola yang tidak valid untuk memberi tahu

bahwa tidak ada informasi yang disisipkan di dalam blok. Pada umumnya pola yang tidak valid membutuhkan perubahan yang lebih sedikit di dalam koefisien dari pada *encoding* sebuah bit 1 atau 0. Selama proses ekstraksi, koefisien yang sama secara *pseudo random* dipilih menggunakan kunci rahasia dan hubungan diantara koefisien dianalisis, bergantung pada sebuah bit 1 atau 0 yang diekstrak.

Algoritma ini tidak membutuhkan gambar asli untuk pelusuran. Keuntungan dari algoritma ini adalah informasi disisipkan di dalam domain yang dikompresi dan dengan mudah dapat diterapkan pada pengompresian video MPEG dengan operasi yang minimal.

Sebaliknya algoritma ini tidak kuat dalam melawan *scaling* atau rotasi karena dimensi gambar digunakan untuk membangkitkan barisan *pseudo random*. Tujuan *paper* dalam hal ini adalah untuk mengevaluasi kelakuan kompresi MPEG dan pengkodean di P- dan B-frame.

5. Algoritma Fridrich

Metode dari algoritma ini didasarkan pada pola *overlaying* dengan kekuatan yang terletak pada frekuensi yang rendah. Pola dibuat menggunakan *pseudo number random generator* dan *cellular automaton with voting value*. Metode ini juga menimbulkan kelemahan yang dapat diserang dengan menggunakan fakta bahwa area gambar hampir seragam atau mempunyai gradien kecerahan yang konstan mungkin memperlihatkan pola watermark. Untuk mengatasi kelemahan ini Fridrich menggunakan metode yang didasarkan pada pola *overlaying*. Jika pola dibentuk dalam bentuk yang sensitif, berdasarkan barisan watermark, bahkan jika pola watermark menunjukkan area yang seragam, hal ini tidak mungkin untuk melakukan

penyerangan. Barisan watermark bit digunakan untuk inisialisasi *pseudo random generator* untuk membuat pola hitam dan putih secara random dari gambar yang berukuran sama. Sebuah *cellular automaton with voting value* diterapkan sampai konvergensi dari *fixed point* didapat. Aturan *voting* menggabungkan *random patches* ke dalam area yang terhubung. Pola selanjutnya disaring menggunakan penyaring untuk mengubah porsi utama dari kekuatan ke dalam frekuensi yang rendah. *Level* abu-abu dari pola terakhir diubah ke dalam skala yang kecil dan pola kemudian ditambahkan ke dalam gambar. Gambar yang sudah diberi watermark menunjukkan tidak ada degradasi yang dapat dilihat dikarenakan pola yang terlapsi. Hal ini dimungkinkan untuk membuktikan keberadaan pola pada gambar setelah disaring. Watermark juga menjadi tahan terhadap *collusion attack*.

Kelemahan dari algoritma ini adalah proses temu kembali (*retrieval*) memerlukan gambar aslinya. Untuk video hal ini tidak dapat diterapkan karena kita membutuhkan keseluruhan video untuk membuktikan watermark. Algoritma yang akan kita gunakan mengatasi masalah ini menggunakan teknik statistik untuk proses temu kembali label tanpa gambar aslinya.

Kelemahan kedua adalah algoritma watermarking menyisipkan hanya satu informasi. Tidak ada informasi lengkap tentang pengarang atau produser yang disisipkan. Proses temu kembali memberikan pola *true* atau *false* untuk menandakan keberhasilannya. Tujuan kita dari permasalahan ini yaitu algoritma dapat digunakan untuk menyisipkan lebih banyak informasi seperti nama atau alamat.

6. Uji Coba Watermarking pada Video MPEG dengan Pendekatan pada Domain DCT

Uji coba sistem mengambil kekuatan informasi yang disisipkan ke dalam properti HVS menggunakan dua parameter, yaitu *smoothness*, dan *edge character* dari blok. *Edge character* didasarkan pada analisis nilai DCT sehingga kita dapat mendeteksi vertikal dan horisontal *edge*. *Smoothnes* dan *edge character* adalah dua paramater utama. Sebelum watermarking dimulai, video MPEG di-*decode* sehingga menghasilkan *frame* tunggal. Informasi yang disisipkan dienkripsi dengan kunci rahasia dari pengguna dan kemudian disisipkan ke dalam gambar dengan kunci yang sama sebagai *seed* untuk pembangkitan *pseudo random number*.

6.1 Metode *Embedding*

Penyisipan label data dilakukan dalam tiga langkah. Dalam algoritma Zhao dan Koch, hal ini dilakukan dalam dua langkah, yaitu langkah pertama dan ketiga. Kita menggabungkan langkah kedua untuk meningkatkan kualitas visual dari *frame* yang disisipi dan menggabungkan sebuah *error correcting code*.

Langkah pertama, barisan posisi dibangkitkan dari kunci pengguna (sebagai *seed*) secara *secure random*. Hal ini penting untuk menyembunyikan watermark di dalam *frame*. Dengan tujuan untuk membangkitkan barisan posisi, setiap blok ditransformasikan ke dalam *discrete cosine*. Walaupun beberapa teknik telah dikembangkan untuk memeriksa karakteristik dari HVS, penghitungan *smoothnes* dan *edge character* blok dijaga agar tetap sederhana. Hal ini dikarenakan fakta bahwa di dalam versi yang akan datang,

penghitungan dilakukan dalam domain *stream* MPEG dan diharapkan dalam waktu nyata. Parameter *smooth* merupakan nomor koefisien DCT yang sederhana yang merupakan bilangan bukan nol setelah *quantization* dengan *quantization* matriks Q_m , yang dapat dilihat di dalam matriks berikut ini. *High value smooth* menandakan banyak komponen frekuensi.

low	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	High

Tetapi blok dengan *edge character* memiliki banyak komponen frekuensi juga, jadi parameter kedua (*edge*) ditambahkan untuk mengurangi *artefacts*.

Parameter *edge* dihitung sebagai *smooth* sederhana, *edge* merupakan penjumlahan dari nilai mutlak koefisien DCT 1, 2, 8, 9, 10, 16, 17 yang ditandai di matriks Q_m , yang merepresentasikan frekuensi DCT yang lebih rendah. Nilai yang tinggi di dalam komponen ini menandakan blok yang dapat memiliki *edge character*. Untuk menentukan level toleransi vs distorsi melalui watermark yang disebabkan oleh dua kombinasi dari parameter linear, dibuat hubungan $Level = smoothscales * smoth + edgescle * edge + offset$.

Parameter *offset* dibutuhkan untuk kekuatan dasar dari watermark. Kombinasi linear dapat dibayangkan sebagai kekuatan watermark yang ditandai oleh variasi *offset*

dan *slight* yang bergantung pada karakteristik blok dengan bobot *smoothscale* dan *edgescale*. Nilai *smoothscale* = -10, *edgescale* = 0,27 dan *offset* = 50 dievaluasi melalui uji coba.

Karena *level* dapat berupa nilai yang negatif, *level* dibatasi menjadi nilai diantara 0 dan 50. Sejauh ini *level-estimation* tidak bergantung pada algoritma watermarking.

Untuk menentukan kekuatan watermarking di dalam *level* yang bebas, *quantization-factor* Q_f digunakan di dalam algoritma Zhao Koch. Setiap perubahan nilai DCT didasarkan pada nilai DCT asli yang di-*quantized* dengan Q_m/Q_f . Oleh karena perubahan dibuat menjadi nilai DCT yang ter-*quantized*, dengan $Q_f = 1$, hal ini menyebabkan perubahan 4 kali lebih besar dari pada nilai $Q_f = 4$. Q_f dihitung dari *level* melalui tabel *look-up* karena nilai hubungan dan range Q_f yang kecil dianggap tidak penting.

Q_f	1	1	2	3	4	4
Level/10	0	1	2	3	4	>4

Sebelum proses penyisipan dimulai, sebuah *error code* dibuat dengan cara sebagai berikut. Setiap informasi watermarking dikode ke dalam 5 bit pertama. Aliran bit yang dihasilkan kemudian dikode dengan BCH. Untuk lebih meningkatkan redundansi, setiap 31 bit *word* disisipkan secara berulang-ulang. Redundansi parameter bit menentukan jumlah dari redundansi.

Di dalam langkah yang ketiga, informasi watermarking dengan *error correction* dan redundansi disisipkan seperti yang dijelaskan di dalam algoritma Zhao dan Koch. Dari setiap tiga lokasi blok DCT yang ter-*quantized* di dalam medium frekuensi dengan nilai mutlak Y1, Y2, dan Y3 yang dipilih, di situlah bit disisipkan. Untuk meng-*encode*

bit, tiga nilai yang diubah menjadi satu seperti pola berikut ini.

Bit	1	1	1	1	0	0	0	0
Y1	H	H	M	M	L	L	M	M
Y2	H	M	H	M	L	M	L	M
Y3	L	L	L	L	H	H	H	H

Jika perubahan pada bit yang disisipkan terlalu besar, Y1, Y2, dan Y3 diubah ke dalam pola yang tidak valid (H, L, M; L, H, M; M, M, M). Setelah perubahan dibuat, blok di-*quantized* dan DCT dibalik.

Keterangan:

H : *high* / tinggi.

M : *medium* / sedang.

L : *low* / rendah.

6.2 Metode Retrieval

Proses penemuan kembali (*retrieval*) dilakukan dengan langkah yang sama seperti pada algoritma Zhao dan Koch. Kita mendecode frame tunggal dari video dan melakukan langkah pembalikan (*inverse*) terhadap informasi yang disisipkan. Dua langkah pertama dilakukan di dalam proses penyisipan. Langkah kedua tidak begitu penting, tetapi informasi tentang kekuatan dari watermark di setiap blok berguna dalam penggunaan *error correcting* dan kode redundansi. Di langkah ketiga, tiga lokasi yang sama dari setiap blok diperiksa seperti pada proses penyisipan. Kemudian pola dapat diperiksa dan bit yang disisipkan dapat dibaca.

6.3 Hasil Uji Coba

Kita telah melakukan pengujian terhadap algoritma Zhao dan Koch yang diterapkan dengan video MPEG yang berbeda. Hasil

dari 15 frame pertama dapat dilihat di tabel. Tabel mengandung *error rate* setelah MPEG *reenconding*, konversi format ke dalam konversi QuickTime dan setelah informasi yang disisipkan dihapus dengan StirMark.

Video characteristics:	Museum.mpg
No. of 8x8 blocks	1320
Compression I-Frame	3.42 %
Compression P-Frame	2.65 %
Compression B-Frame	1.22 %
IPB-order	IBBPBB

Compression-rate dihitung dari 24 bit gambar yang tidak dikompres dan kemudian digunakan parameter berikut ini: *smoothscale* = -10, *edgescale* = 0,43, *offset* = 40 kekuatan watermark = 2 dan bit redundansi = 4. Tabel konversi dari *level* ke *quantization factor* Q_f dapat dilihat di bawah ini.

Q_f	1	1	2	3	4	4
Level/10	0	1	2	3	4	>4

Hasil pengujian kekuatan (*robust*) yang dilakukan dapat dilihat di dalam tabel berikut ini. Kita menyisipkan 60 bit informasi. Kita melakukan MPEG-*encoding*, transformasi QuickTime dan serangan StirMark dengan algoritma Zhao dan Koch yang ditingkatkan sehingga mendapatkan nilai sebagai berikut. Tabel mengukur bit *error* setelah dilakukan transformasi dengan *error correcting code*. Nomor menunjukkan jumlah bit *error* yang muncul di dalam 13 frame pertama setelah dilakukan kompresi tinggi MPEG, konversi QuickTime, dan serangan StirMark.

Frame No.	0	1	2	3	4	5	6
F-Type	I	B	B	P	B	B	I
MPEG BCH	0	0	0	0	0	0	0
QuickTime BCH	0	1	9	1	0	0	0
StirMark BCH	22	29	29	16	17	19	24

Frame No.	7	8	9	10	11	12	13
F-Type	B	B	P	B	B	I	B
MPEG BCH	0	0	0	0	0	0	0
QuickTime BCH	0	0	0	1	0	0	5
StirMark BCH	22	29	29	16	17	19	24

Bit *error rate* berikut ini dapat diukur melalui uji coba yang dilakukan.

museum.mpg:

MPEG:

I-Frames <1% P-Frames 1-2% B-Frames 5%

QuickTime:

I-Frame 1-2% P-Frames 5% B-Frames 7%

StirMark:

15%

Algoritma yang digunakan menunjukkan hasil yang bagus di dalam kompresi MPEG dan QuickTime. *Error rate* dari informasi yang disisipkan menunjukkan hasil yang baik di I-frame. B-frame masih memiliki beberapa masalah. StirMark menghapus informasi yang disisipkan sampai 30%. Tanpa *error correcting code* watermark akan rusak semuanya. StirMark menghapus watermark di dalam algoritma asli Zhao Koch. *Visual artefact* dapat dihindari.

7. Kesimpulan

Dalam *paper* ini, kita telah membahas teknik-teknik watermarking, keunggulan dan kelemahannya untuk memungkinkan keamanan dari hak cipta yang disisipkan. Tes kekuatan yang diadakan terutama didasarkan pada kompresi, kompresi bentuk dan transformasi geometrik. Kita tekankan bahwa pendekatan yang diambil dari Zao Koch dengan *error corecting code* cocok

untuk video MPEG dan kualitas frame di mana informasi disisipkan dapat ditingkatkan. Pendekatan Fridrich juga dapat digunakan dan berhasil meningkatkan keberhasilan kode *binary* yang disisipkan dan dapat digunakan untuk proses temu kembali tanpa gambar aslinya. Keuntungan algoritma Firdrich adalah kemungkinan untuk menyisipkan lebih banyak bit-bit informasi (>250) per frame dan untuk menganani serangan *StirMark*.

- [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] Digimarc, *Watermarking Technology*, PictureMarcTM 1996, http://www.digimarc.com/wt_page.html diakses tanggal 7 Januari pukul 09:30.
- [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] Koch, E. and Zhao, J., *Towards Robust and Hidden Image Copyright Labelling*, IEEE Workshop on Nonlinear Signal and Image Processing, 1995.
- [8] Kuhn, M.G., *Stirmark*, <http://www.cl.cam.ac.uk/mgk25/stirmark/>, diakses tanggal 7 Januari 2005 pukul 09:45.
- [9] AlpVision, *Digital Vidoe Watermarking*, http://www.alpvision.com/Video/video_wm_rd.html, diakses tanggal 7 January 2005 pukul 10:05.