PERLINDUNGAN KEASLIAN CITRA DENGAN TEKNIK WATERMARKING

Oleh :
Widiyanto Tri Handoko dan Dwi Agus Diartono

1. PENGANTAR

Konsep perlindungan keaslian dan hak cipta merupakan kepentingan utama dalam kerangka masyarakat informasi kita. Sebagai contoh, saluran tv biasanya menempatkan gambar logo kecil yang bisa dilihat di pojok sebagai salah satu bentuk perlindungan hak cipta. Dengan cara ini kesempatan adanya penggandaan yang tidak sah bisa diperkecil dan penerima dapat dengan mudah mengidentifikasi sumber tv tersebut. Uang kertas juga menggunakan watermark untuk tujuan perlindungan keaslian, yang mana sangat sulit untuk dihasilkan dengan teknik fotokopi konvensional. Logo-logo, pola-pola serta gambar-gambar yang disebutkan diatas merupakan contoh-contoh yang biasa ditemui pada *visible watermark* (watermark yang bisa dilihat).

Saat ini, teknologi digital yang berkembang cepat menggantikan teknik-teknik tradisional untuk transmisi, prosesing dan penyimpanan informasi. Sejumlah besar peralatan dan aplikasi komputer tersedia untuk menghasilkan dan memanipulasi produk-produk digital. Meskipun demikian, pada saat yang sama, metode pembajakan menjadi lebih kuat karena duplikasi, pemalsuan, dan retransmisi lebih mudah dari sebelumnya. *Visible watermark* juga dapat diterapkan untuk melindungi produk-produk digital dengan cara tradisional. Namun, kontribusi mereka untuk perlindungan hak cipta dan pembuktian keaslian kurang memadai. Teknik-teknik prosesing digital modern dapat digunakan dengan maksud jahat yakni untuk menghapuskan atau menggantikan visible watermark. Dalam usaha untuk mengatasi problem tersebut dikembangkan teknik yang disebut *invisible digital watermark* (watermark

digital yang tak terlihat) atau *invisible digital stamp.* Namun demikian, masalah penciptaan sistem *watermarking* yang efisien dan kuat masih tetap terbuka.

2. 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.

Perbedaan *stegranograpy* dengan *cryptography* terletak pada bagaimana proses penyembunyian data dan hasil akhir dari proses tersebut. *Cryptography* melakukan proses pengacakan data aslinya sehingga menghasilkan data terenkripsi yang benar-benar acak dan berbeda dengan aslinya, sedangkan *stegranography* menyembunyikan dalam data lain yang akan ditumpanginya tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hampir sama.

Watermarking atau tanda air dapat diartikan sebagai suatu teknik penyembunyian data atau informasi "rahasia" kedalam suatu data lainnya untuk "ditumpangi" (kadang disebut dengan *host* data), tetapi orang lain tidak menyadari kehadiran adanya data tambahan pada data *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 maupun tidak sengaja untuk menghilangkan data *watermark* yang terdapat didalamnya. *Watermark* juga harus tahan terhadap berbagai jenis pengolahan/proses digital yang tidak merusak kualitas data yang ter-*watermark*.

3. APLIKASI WATERMARKING

Beberapa aplikasi dari *watermarking* yang pernah dikerjakan dapat dilihat pada bagian bawah berikut ini :

Broadcast Monitoring

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.

Owner Identification

Keterangan hak cipta biasanya ditulis pada buku ataupun pada foto-foto dalam bentuk ©*waktu, pemilik*, tetapi keterangan ini ditulis secara eksplisit dan kelihatan. Demikian juga pada film biasanya diletakkan pada akhir film, sedangkan pada kaset atau CD audio diletakkan pada kotak pembungkusnya.

Kekurangan dari cara diatas adalah semua informasi mengenai hak cipta tersebut dapat dihilangkan baik dengan sengaja ataupun tidak disengaja seperti hilangnya kotak pembungkus kaset atau CD audio, film dipotong untuk diambil sebagian saja, gambar juga dapat dipotong (*cropping*), dan sebagainya.

Dengan demikian *watermarking* tampaknya dapat digunakan sebagai tool untuk *owner identification*, karena informasi hak cipta tersebut diletakan didalam data *host*-nya dan merupakan bagian dari data *host* tersebut, sehingga usaha untuk menghilangkan informasi hak cipta tersebut dapat menurunkan kualitas data *host*-nya.

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.

Authentication

Untuk membuktikan bahwa suatu data digital itu benar-benar asli dan tidak mengalami sedikit perubahan apapun juga dapat diterapkan dengan prinsip *watermarking*. Pembuktian bahwa data tersebut asli tanpa perubahan apapun meskipun perubahan kecil yang tidak dapat dipersepsi oleh mata atau telinga seperti penambahan pada citra diam beberapa garis halus pada tempat-tempat tertentu atau perubahan degradasi warna yang tidak disadari oleh mata sangat perlu untuk aplikasi-aplikasi tertentu seperti pada citra medis.

Sebelumnya pembuktian keaslian ini pernah dilalukan dengan metoda *cryptography*. Dimana *signature cryptography* yang berkaitan dengan data (dalam hal ini citra) tersebut diekstrak dan disertakan dengan data asli tersebut. Bila terjadi perubahan sedikit saja pada data aslinya maka *signature cryptography*-nya otomatis akan berbeda. Tapi sayangnya signature ini merupakan data tambahan yang dikirimkan bersamaan dengan data aslinya ataupun diletakkan pada header dari data tersebut. Dengan demikian signature tersebut dapat dengan mudah dihilangkan, sehingga pembuktian keaslian tidak dapat dilakukan lagi.

Dengan *watermarking*, dimana digabungkan dengan isi data tersebut, maka kemana pun data tersebut, baik di-*cropping*, diubah ke dalam format digital lain, dan sebagainya, *watermarknya* tetap akan ada bersama dengan *host* datanya.

Fingerprinting

Fingerprinting atau transactional *watermark* merupakan aplikasi *watermarking* dengan menyembunyikan informasi *watermark* yang berbeda-beda kepada tiap data digital yang didistribusikan. Biasanya untuk aplikasi pelabelan hak cipta, *broadcast monitoring*, semua data digital yang akan didistribusikan diisikan dengan informasi hak cipta yang sama.

Fingerprinting biasanya digunakan bila terjadi transaksi sebuah data digital antara pemilik dengan seorang konsumer, misalnya sebuah provider memberikan service *Video On Demand*, maka data yang akan didistribukan tersebut di*watermark* dengan informasi asal dan tujuan mungkin juga waktunya. Jadi bila terjadi perdagangan atau pembajakan terhadap data digital yang pernah ditransaksikan, maka dapat diketahui sumber kebocorannya atau pembajaknya. Penjelasan mengenai fingerprinting akan dibahas lebih lanjut pada bagian aplikasi video *watermarking* pada broadcasting dan streaming video.

Copy Control

Penggunaan *watermark* sebagai *copy control* hampir sama dengan copy protection yang digunakan pada disket-disket (*disk-protection*) beberapa tahun yang lampau. Penerapan *watermarking* sebagai *copy control* harus disertai dengan penanaman *watermarking detector* pada perangkat *hardware* untuk membaca data digital tersebut. Bila *detector* mendeteksi adanya *watermark* pada data digital yang akan dibacanya, maka beberapa proses yang dapat dilakukan hardware tersebut misalnya peng-*copy*-an akan di-*disable*-kan.

Aplikasi *copy control* juga sudah dikembangkan untuk diterapkan pada perangkat modern saat ini seperti pada *DVD player*. Tentunya penerapannya harus disepakati oleh seluruh pembuat perangkat player untuk menambahkan rangkaian detector *watermark* tersebut.

Covert Communication

Salah satu aplikasi *steganography* pada awalnya adalah untuk komunikasi rahasia terutama pada jaman perang. *Watermarking* sebagai perkembangan dari *steganography* juga dapat digunakan sebagai media untuk mengrimkan pesan-pesan rahasia kepada sekutu sehingga tidak diketahui musuh. Aplikasi *watermarking* sebagai media komunikasi rahasia lebih dikenal sebagai *data hiding*.

4. KARAKTERISTIK WATERMARKING

Ada beberapa karakteristik sistem *watermarking* seperti *robustness*, *tamper resistance*, *fidelity*, dan *computational cost*. Dimana setiap karakteristik tersebut terdapat *trade-off* diantaranya. Evaluasi terhadap karakteristik sistem *watermarking* tidak sama untuk semua aplikasi, sehingga pemilihan trade-off yang sesuai harus benar-benar dipertimbangkan berdasarkan aplikasi *watermarking*.

Robustness

Watermark harus *robust* artinya *watermark* di dalam *host* data harus tahan terhadap beberapa operasi pemrosesan digital yang umum seperti konversi 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*.

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* :

- *Active attacks*. Merupakan serangan dimana seseorang berusaha untuk menghilangkan *watermark* yang terdapat didalam *host* data.
- *Passive attacks*. Berbeda dengan *active attacks*, dimana 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*)

Fidelity

Salah satu *trade-off* antara karakteristik *watermarking* yang sangat kelihatan adalah antara *robustness* dengan *fidelity*. Dalam beberapa literatur *fidelity* kadang disebut dengan *invisibility* untuk jenis data citra dan video atau *inaudible* untuk data jenis suara. 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.

Computational Cost

Ada beberapa aplikasi yang menuntut proses *watermarking* baik *embedding* maupun *extracting* bekerja secara *real time*, ada juga yang mengharapkan salah satu baik *extracting* atau *embedding* saja yang *real time* ataupun duanya boleh tidak *real time*. Contohnya untuk aplikasi *owner identification* atau *proof of ownership*, proses *watermarking* baik *embedding* maupun *extracting* tidak perlu *real time*, sedangkan untuk aplikasi *fingerprinting* pada service *video on demand*, maka proses *embedding watermark* harus dilakukan secara *real time*.

Setelah mengupas secara singkat aplikasi *watermarking* serta beberapa karakteristik sistem *watermarking*, maka sekarang akan lebih difokuskan pada aplikasi *watermarking* untuk tipe data video baik untuk video *broadcast monitoring* terhadap siaran acara televisi, periklanan maupun untuk *real time Video on Demand* serta aplikasi *watermarking* pada *copy control.*

5. WATERMARKING PADA TRANSFORMASI DOMAIN

Seperti diketahui bahwa perlindungan hak cipta membutuhkan *watermark* yang kuat terhadap berbagai serangan. Disamping pada *spatial domain*, *discrete cosine transform* (DCT) atau *discrete fourier transform* (DFT), ternyata juga menjadi domain citra yang baik dipakai untuk *watermarking*. Dalam hal ini, *watermark* dengan spektrum tersebar, yang dilekatkan pada frekuensi menengah yang sesuai, memberikan perlindungan invisibility (yang tak terlihat), dan kekuatan yang meningkat terhadap kehilangan kompresi dan modifikasi geometrikal tertentu.

Discrete Cosine Transform

Salah satu teknik *Watermarking* adalah transformasi matematik yang dikenal dengan nama *Discrete Cosine Transform* disingkat DCT. Transformasi adalah mekanisme pengubahan data yang ada ke bentuk data yang lain, baik kuantitas dan kualitasnya, sehingga mempermudah kita dalam melakukan analisis terhadap data tersebut. Hal penting lainnya tentang transformasi ini adalah sifatnya yang *reversible* (dapat dibalik). *Watermarking* dengan spektrum tersebar dalam citra domain DCT telah dikemukakan oleh Cox dkk. Skema mereka mempertahankan keaslian citra setelah dilakukan perubahan yang sesuai pada koefisien DCT. Prosedur deteksi melibatkan penggunaan citra asli dalam usaha untuk mengatasi masalah perubahan citra secara geometris.

Kita mengambil rangkaian satu-dimensional (1-D) dan koefisien DCT pada citra X yang dibentuk dengan susunan zigzag, yang dilambangkan oleh Z dari domain 2-D DCT :

$$\text{DCT}\ (X(n,m))\ o\ Z \rightarrow Y = \{y_1, y_2, y_3, \ldots.\}$$

Sinyal watermark ditentukan dengan rangkaian pseudo-random dari nomor M riil yang mengikuti distribusi normal dengan mean nol dan unit perbedaan :

$$W = \{w_1, w_2, \ldots..,w_M\}\ W_I \in (-d,d) \subset IR \qquad (1)$$

Pelekatan watermark terjadi dalam subset domain Y yang terletak pada frekuensi medium dalam interval (L,M+L). pelekatan tersebut multiplikatif :

$$Y_i^{(w)} = Y_i + \delta |Y_i| W_{i-L}, \quad L < i \leq M + L \qquad (2)$$

Citra watermark diperoleh dengan menerapkan transformasi invers :

$$X_W = Z^{-1}\ o\ \text{IDCT}\ (Y_W), \qquad Y_W = \{ Y_1^{(W)}, Y_2^{(W)}, \ldots..\} \qquad (3)$$

Karena perubahan (2) bisa menghasilkan distorsi signifikan dalam citra watermark, maka *visual masking* harus digunakan. Dengan cara ini, watermark casting diproses dengan tepat dalam usaha untuk menghasilkan perubahan kecil dalam bagian citra homogen dan dalam bagian yang sangat bertekstur.

Deteksi didasarkan pada korelasi antara watermark W dan tes citra X^* dengan koefisien DCT $Y^* = \{Y_1^A, Y_2^A, \ldots.\}$:

$$R = \frac{1}{M} \sum_{i=1}^{M} y^*_{L+i} W_i \qquad (4)$$

Dengan cara yang sama korelasi R mengikuti distribusi normal. Dengan kehadiran *visual masking*, distribusi mempunyai nilai dan perbedaan :

$$\mu_R = \begin{cases} \delta\mu_{|Y^*|}, & if\ Y^* = Y_W \\ 0, & \text{otherwise} \end{cases}, \quad \sigma_R^2 \approx \frac{\sigma_{Y^*}^2}{M} \qquad (5)$$

Keputusan akhir tentang keberadaan watermark diperlukan untuk menentukan nilai threshold R_{thres}. Total kesalahan diperkecil untuk $R_{thres} = \delta\mu|Y^*|/2$. Spektrum watermark tersebar dalam domain DCT menunjukkan daya tahan

tinggi terhadap modifikasi. Seperti kompresi JPEG, filtering, histogram equalization (penyamaan histogram) dan besar/kecil ukuran citra juga internal cropping atau penggantian sebagian obyek. Meskipun demikian, kekuatan watermark seperti itu merupakan suatu kerugian bila yang dikehendaki adalah verifikasi isi. Kita harus mencatat bahwa domain DCT tidak invarian di bawah rotasi c itra, w atermark a kan t idak t erdeteksi s etelah t erjaadi se rangan. Bagian citra yang dilakukan *cropping* dan *resize* berisi formasi watermark tetapi sinkronisasi watermark memerlukan pengetahuan ukuran citra asli yang sudah tersedia.

6. KESIMPULAN

Digital Watermarking merupakan topik penelitian yang baru. Kemajuan yang penting telah terjadi akhir-akhir ini dan banyak teknik baru telah ditampilkan dalam literatur. Penelitian *watermarking* terutama sekali difokuskan pada masalah kekuatan atau daya tahan *watermark* untuk perlindungan hak cipta. Dapatkah suatu *watermark* tahan terhadap semua pemrosesan teknik serangan citra dalam mempertahankan kualitas produk yang diciptakan? Jawabnya mungkin bisa "ya" untuk serangan-serangan yang telah dikenal saat ini. Namun, apa y ang akan terjadi dengan serangan pemrosesan citra di masa mendatang atau metode penghilangan kompresi? *Watermarking* dan kompresi merupakan teknik-teknik yang terus berkembang. *Watermark* mungkin bisa menjadi kuat dibawah kompresi JPEG, tapi hal ini bisa menjadi sesuatu y ang tidak benar untuk teknik yang lebih kuat, yang mana mungkin akan terjadi di tahun-tahun mendatang. Sekali produk watermark keluar dalam distribusi publik, maka menjadi rentan terhadap serangan apapun di masa datang. Teknik anti-*watermarking* telah dikembangkan berdasarkan berbagai macam kebutuhan pemrosesan citra.

DAFTAR PUSTAKA

1. A. Piva, M. Barni, F. Bartolini, V.Cappellini, "*A DCT-Domain System for Robust Image Watermarking*", Firenze, Dipartimento di Ingegneria Elettronica, Universita di Firenze,1998

2. A. Piva, M. Barni, F. Bartolini, V.Cappellini, "Threshold Selection for Correlation-Based Watermark Detection", Dipartimento di Ingegneria Elettronica, Universita di Firenze

3. A. Piva, M. Barni, F. Bartolini, V. Cappellini, "*Image Watermarking for Secure Transmission over Public Network* ", Firenze, Dipartimento di Ingegneria Elettronica, Universita di Firenze, 1982

4. J. Zhao and E. Koch, Proceeding of the Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technology, "*Embedding robust labels into images for copyright protection* ", Vienna, August 1995, 242-252.