Review Skema *Public-Key Watermarking* untuk Proteksi *Copyright* pada Distribusi Produk Multimedia

Rinaldi Munir[1], Bambang Riyanto[2], Sarwono Sutikno[3]

Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jl. Ganesha 10, Bandung

E-mail : rinaldi@informatika.org[1], briyanto@lskk.ee.itb.ac.id[2], ssarwono@ieee.org[3]

Abstrak

Kebanyakan skema *watermarking* pada produk multimedia digital bersifat simetri, yaitu menggunakan kunci yang sama untuk penyisipan dan pendeteksian *watermark*. Karena kunci ini rahasia dan hanya diketahui oleh pemilik *watermark*, maka skema *symmetric watermarking* tidak dapat digunakan jika pendeteksian *watermark* dilakukan oleh *decoder* yang tersebar di seluruh dunia, sebab publikasi kunci potensial menimbulkan serangan yang ditujukan untuk menghilangkan *watermark*. Di dalam makalah ini dipresentasikan konsep skema *public-key watermarking* (atau *asymmetric watermarking*) dan *review* dari sebuah metodenya yang dipublikasikan oleh [5]. Pada skema ini, penyisipan *watermark* menggunakan kunci privat sedangkan pendeteksian *watermark* dapat dilakukan oleh siapapun dengan menggunakan kunci publik. Metode *public-key watermarking* yang disajikan dianalisis ketahanannya terhadap serangan *malicious attack* dan *non-malicious attack*.

Kata kunci*: public-key watermarking, watermark, kunci privat, kunci publik, spread spectrum, serangan*

1. Pendahuluan

Representasi digital dari produk multimedia seperti data audio, citra, dan video menjadi populer karena data digital mudah dan murah untuk digandakan (*copy*) serta didistribusikan. Namun, penggandaan dan pendistribusian yang tidak berizin menimbulkan masalah terhadap hak kekayaaan intelektual (HAKI), karena pemilik data digital tidak memiliki suatu label yang mengidentifikasi pemilik (*ownership*) atau pemegang hak penggandaan (*copyright*) atas data digital tersebut.

Permasalahan di atas dapat diatasi dengan menggunakan *digital watermarking*. *Digital watermarking* adalah teknik untuk menyisipkan informasi yang menyatakan label kepemilikan ke dalam sebuah produk digital. Informasi yang disisipkan ke dalam produk digital dinamakan *watermark*. Penyisipan *watermark* dilakukan sedemikian rupa sehingga *watermark* tidak merusak produk digital yang dilindungi. Selain itu *watermark* yang telah disisipkan tidak dapat dipersepsi oleh indra manusia, namun ia dapat dideteksi oleh komputer dengan menggunakan kunci yang benar. *Watermark* yang telah disisipkan tidak dapat dihapus dari dalam data digital, sehingga bila produk multimedia ber-*watermark* disebar dan digandakan, maka otomatis *watermark* di dalamnya ikut terbawa.

Teknik *watermarking* pada citra secara umum terdiri dari 2 tahapan: 1) penyisipan *watermark* (*watermark embedding*), dan 2) pendeteksian *watermark* (*watermark detection/decoding*). Sejumlah skema *digital watermarking* sudah diusulkan dan dipresentasikan dalam beberapa tahun terakhir. Kebanyakan dari skema tersebut simetri, artinya pendeteksian *watermark* harus menggunakan kunci rahasia yang sama dengan kunci yang digunakan pada waktu penyisipan. Skema simetri ini jelas tidak cocok jika pendeteksian *watermark* dilakukan oleh peralatan yang tersebar di seluruh dunia, karena kunci hanya diketahui oleh pemegang *copyright* atas data digital. Jelas tidak mungkin mendistribusikan kunci rahasia kepada pihak lain sebab resiko keamanannya sangat besar: sekali kunci diketahui oleh pihak lawan, maka kunci tersebut dapat digunakan untuk menghilangkan *watermark* dari data digital tanpa menimbulkan kerusakan berarti. Hal ini dikarenakan pada kebanyakan skema simetri, kunci berasosiasi dengan lokasi penyisipan *watermark*.

Ini berarti pendeteksian *watermark* harus dapat dilakukan secara publik, yaitu dapat dilakukan

oleh siapapun. Beberapa aplikasi mensyaratkan *watermark* dapat di-*decode* oleh *decoder* di manapun di seluruh dunia tanpa dapat menghilangkan *watermark* [5].

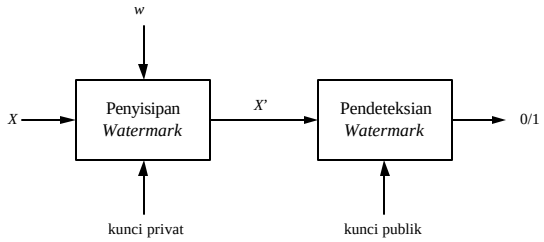
Masalah di atas dapat diselesaikan dengan *asymmetric watermarking* atau lebih dikenal dengan *public-key watermarking*, yang dalam hal ini penyisipan *watermark* (dilakukan oleh pemilik produk multimedia) menggunakan kunci privat yang dijaga rahasia, sedangkan pendeteksian *watermark* menggunakan kunci publik yang tersedia bagi siapa saja. Konsep *public-key watermarking* memang mengadopsi konsep yang terdapat di dalam *public-key cryptography*, yang mana enkripsi menggunakan kunci publik sedangkan dekripsi menggunakan kunci privat.

Konsep *public-key watermarking* menjadi penting karena perhatian terbesar yang diarahkan pada *watermarking* adalah masalah ketahanan (*robustness*) algoritma terhadap serangan yang dapat merusak atau menghancurkan *watermark* di dalam data digital. Sebaliknya persoalan keamanan (*security*) sering kali dilupakan dan perhatian untuk masalah tersebut saat ini relatif masih sedikit [2].

Makalah ini mempresentasikan konsep *public-key watermarking* dan persoalan keamanan yang berkaitan dengannya. Selain itu dibahas juga *review* sebuah skema *public-key watermarking* yang merupakan pengembangan dari teknik *watermarking spread spectrum* [5].

2. *Public-Key Watermarking*

Gambar 1 memperlihatkan skema umum *asymmetric watermarking* [1], yang dalam hal ini *X* adalah *host signal* berupa data digital yang akan diberi *watermark*, *w* adalah *watermark*, dan *X'* adalah data digital yang sudah ber-*watermark*. Pendeteksian *watermark* secara sederhana hanya menghasilkan keluaran apakah *watermark* ditemukan ("1") atau tidak ("0").



Gambar 1. Skema umum *public-key watermarking*

Skema *public-key watermarking* dilakukan dengan suatu cara sedemikian sehingga [2]:

1. Secara komputasi tidak mungkin menghitung kunci privat dari kunci publik.
2. Kunci publik tidak dapat digunakan untuk menghilangkan *watermark*.

Watermark yang bersifat *public-key* dapat dibaca oleh siapapun yang memiliki kunci publik, tetapi hanya orang yang memiliki kunci privat yang dapat menghilangkan *watermark* dari data digital dan memperoleh kembali data digital awal yang bersih (tanpa *watermark*) [6].

3. *Spread-Spectrum Watermarking*

Hartung dan Girod [3, 4, 5] mengembangkan teknik *symmetric watermarking* untuk video digital yang berbasis pada *spread spectrum*. Ide dasarnya adalah menjumlahkan sinyal semi-acak (yang berlaku sebagai *watermark*) dengan data video sehingga hasilnya tidak dapat dideteksi dan dihilangkan tanpa mengetahui parameter *watermarking* (yang berlaku sebagai kunci rahasia). Kita akan menggunakan contoh teknik *watermarking* ini untuk selanjutnya diperluas oleh Hartung dan Girod menjadi *asymmetric watermarking.*

Penyisipan watermark

Misalkan bit-bit *watermark* dikodekan sebagai *string* yang terdiri dari 1 dan –1. Misalkan

$$a_j, \qquad a_j \in \{-1, 1\} \qquad (1)$$

adalah *watermark* yang akan disembunyikan di dalam *video stream* linier v_i. Barisan a_j disebar (*spread*) dengan faktor *cr*, yang disebut *chip-rate*, untuk memperoleh barisan

$$b_i = a_j, \quad j \cdot cr \le i \le (j+1) \cdot c_r \qquad (2)$$

Barisan b_i dimodulasikan dengan barisan semi-acak biner (berlaku sebagai kunci) yang dikodekan sebagai

$$p_i, \qquad p_i \in \{-1, 1\} \qquad (3)$$

untuk menghasilkan sinyal *watermark* termodulasi

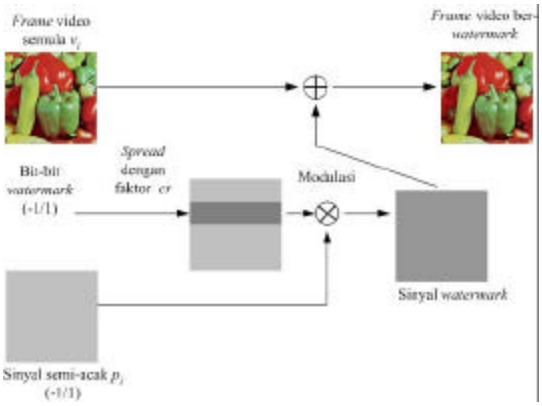
$$w_i = \alpha \cdot b_i \cdot p_i \qquad (4)$$

yang dalam hal ini kontanta α menentukan kekuatan sinyal *watermark* dan harus dipilih sedemikian sehingga *watermark* tidak dapat dipersepsi namun masih bisa dideteksi [4].

Selanjutya, w_i dijumlahkan dengan *video stream* linier v_i untuk menghasilkan video ber-*watermark*

$$\hat{v}_i = v_i + a \cdot b_i \cdot p_i \qquad (5)$$

Sinyal *watermark* termodulasi $a\,b_i p_i$ berlaku seperti derau (*noise*) yang sulit dideteksi dan dihilangkan. Gambar 2 memperlihatkan skema penyisipan *watermark*.



Gambar 2. Skema penyisipaan *watermark* dengan teknik *spread spectrum* [5]

Pendeteksian Watermark

Untuk mendeksi *watermark*, barisan sinyal semi-acak p_i yang digunakan pada waktu penyisipan harus diketahui. Sebelum dikalikan dengan p_i, video ber-*watermark* $\hat{v}_i$ disaring terlebih dahulu dengan penapis lolos-tinggi (*highpass filter*) menjadi $\overline{v_i}$. Penapisan dimaksudkan untuk menghilangkan komponen sinyal video dari superposisi *watermark* dengan video. Penapisan ini cukup membantu tahap korelasi. Selanjutnya, *frame* video $\overline{v_i}$ dikalikan dengan p_i lalu menjumlahkan seluruh hasil perkalian:

$$s_j = \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} p_i \overline{v_i} \approx \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} p_i^2 \cdot a \cdot b_i \qquad (6)$$

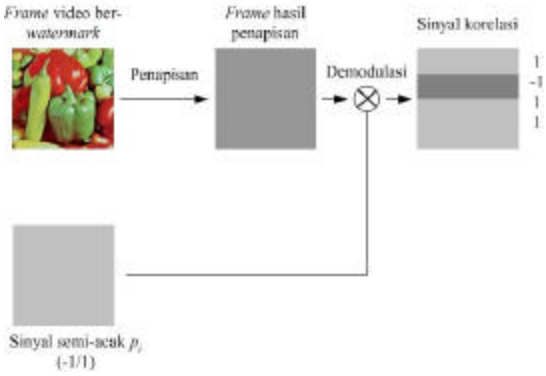
yang menghasilkan jumlah korelasi

$$s_j \approx cr \cdot a \cdot b_i \qquad (7)$$

Dengan mengasumsikan bahwa barisan sinyal semi-acak p_i dan *video stream* v_i tidak berkorelasi, persamaan (7) dihampiri menjadi $s_j = cr \cdot a \cdot a_j$. Bit *watermark* a_j diperoleh kembali dengan

$$a_j = sign(s_j) \qquad (8)$$

Proses pendeteksian *watermark* divisualisasikan pada Gambar 3.



Gambar 3. Skema pendeteksian *watermark* dengan teknik *spread spectrum* [5]

4. *Review* Metode *Public-Key Watermarking*

Hartung dan Girod [3,5] mempresentasikan modifikasi skema *symmetric watermarking* di atas menjadi skema *public-key watermarking*, yang dalam hal ini *watermark* disisipkan dengan menggunakan kunci privat sedangkan pendeteksian *watermark* menggunakan kunci publik. Kunci privat tetap terdiri dari barisan semi-acak p_i, sedangkan kunci publik diperoleh dengan membuat sebagian dari barisan p_i menjadi publik dan mengganti bit-bit lainnya dengan barisan acak lain.

Agar lebih jelas, pada kunci publik p_i^{publik} setiap koefisien ke-n ($n > 2$) diambil dari barisan sinyal semi-acak semula p_i, sedangkan koefisien lainnya adalah nilai acak sembarang dengan distribusi yang sama seperti pada barisan p_i:

$$p_i^{\text{publik}} = \begin{cases} p_i, & \text{acak dengan peluang } 1/n \\ rand\{-1,+1\}, & \text{lainnya} \end{cases} \qquad (9)$$

Jadi, setiap penerima video ber-*watermark* memiliki p_i^{publik} yang sebagian elemennya bersesuaian dengan p_i sedangkan sisanya dibangkitkan secara acak.

Dengan menggunakan kunci publik, *watermark* dapat dideteksi dengan cara yang sama seperti yang dijelaskan sebelumnya

(yaitu dengan mengganti p_i dengan p_i^{publik}), yaitu:

$$s_j^{\text{publik}} = \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} p_i^{\text{publik}} \overline{v_i} \approx \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} p_i^{\text{publik}} \cdot p_i \cdot a \cdot b_i \qquad (10)$$

yang menghasilkan jumlah korelasi

$$s_j^{\text{publik}} \approx \frac{1}{n} \cdot cr \cdot a \cdot a_j \qquad (11)$$

karena secara rata-rata hanya setiap koefisen ke-n dari p_i^{publik} dan p_i yang bersesuaian. Semua koefisien lainnya tidak berkorelasi sehingga dapat dibuang dari penjumlahan. Bit *watermark* a_j diperoleh kembali dengan

$$a_j^{\text{publik}} = sign(s_j^{\text{publik}}) \qquad (12)$$

5. *Robustness Public-key Watermarking*

Salah satu kriteria skema *watermarking* yang bagus adalah tahan (*robust*) terhadap serangan yang dilakukan terhadap data digital ber-*watermark*. Serangan yang tipikal misalnya kompresi *lossy*, operasi penapisan lolos-rendah, operasi geometri dan *cropping*. Serangan semacam ini digolongkan sebagai *non malicious attack* yaitu serangan yang normal terjadi selama penggunaan data digital ber-*watermark* [2]. Serangan tersebut dapat merusak atau menghancurkan *watermark* di dalam data digital. Jika akibat serangan tersebut *watermark* masih dapat diekstraksi, maka skema *watermarking* yang digunakan dikatakan *robust*.

Sayangnya, *skema public-key watermarking* yang dipresentasikan oleh Hartung dan Girod memiliki ketahanan yang lebih rendah daripada ketahanan skema simetrinya [5]. Untuk meningkatkan ketahanannya, parameter *cr* dan α harus dipilih sedmikian rupa sehingga dapat menjamin *watermark* cukup *robust* [5].

6. Keamanan *Public-key Watermarking*

Meskipun kunci publik tidak bersifat rahasia, namun pengetahuan mengenai kunci publik tidak memberi informasi yang berarti untuk menurunkan kunci privat (kunci privat digunakan penyerang untuk menghilangkan *watermark* dari media digital). Hal ini dikarenakan secara rata-rata hanya setiap koefisen ke-n dari p_i^{publik} dan p_i yang bersesuaian, sedangkan semua koefisien lainnya tidak berkorelasi.

Serangan yang mungkin dapat dilakukan kepada video ber-*watermark* adalah menggunakan kunci publik untuk menghancurkan atau memanipulasi *watermark*, namun hanya bagian publik dari *watermark* yang dapat dihilangkan atau dimanipulasi. Caranya adalah dengan mengurangkan $\alpha b_i p_i^{\text{publik}}$ (lihat persamaan 5) dengan asumsi b_i berhasil diketahui:

$$v_i = \hat{v}_i - a \cdot b_i \cdot p_i^{\text{publik}} \qquad (13)$$

Persamaan (13) menyatakan bahwa bagian *watermark* yang publik dapat dihancurkan tetapi bagian yang privat tetap bertahan. Serangan semacam ini digolongkan sebagai *malicious attack*, yaitu serangan yang tujuan utamanya adalah menghilangkan atau membuat *watermark* tidak dapat dideteksi [2].

Pemilik *watermark* dapat saja membentuk barisan publik yang baru dengan menggunakan elemen-elemen p_i yang belum dipakai, tetapi penyerang juga dapat menghilangkan kembali bagian *watermark* yang publik yang bersesuaian. Semakin sering kunci publik baru dibentuk, semakin banyak bagian *watermark* yang dihancurkan, akibatnya data *watermark* pun habis [3].

Skema ini juga hanya membatasi penggunaan beberapa buah kunci publik saja, sebab semakin banyak kunci publik didistribusikan ke pengguna, semakin besar peluang untuk merekonstruksi kunci privat dengan merata-ratakan kunci kunci publik [5]. Jadi, skema ini tidak cocok untuk perlindungan *copyright* yang lebih banyak.

5. Skema *Public-key Watermarking* Lainnya

Skema *public-key watermarking* lain yang pernah diusulkan adalah penggunaan barisan Legendre, vektor *eigen* dari transfromasi linier, dan operasi pemrosesan sinyal satu-arah. Namun, tidak satupun dari skema tersebut yang tahan terhadap serangan *malicious attack*. Lihat [4] untuk analisis lebih rinci.

6. Kesimpulan

Makalah ini sudah menyajikan konsep skema *public-key watermarking*. Pada skema tersebut, penyisipan *watermark* menggunakan kunci

privat pemilik media digital, sedangkan pendeteksian *watermark* dapat dilakukan siapapun atau alat *decoder* dengan menggunakan kunci publik.

Contoh metode *public-key watermarking* yang di-*review* adalah perluasan teknik *spread spectrum* pada video digital. Idenya adalah membuat sebagian dari barisan nilai pada kunci privat menjadi kunci publik, sedangkan sebagian lain dari kunci publik dibangkitkan secara acak. Sayangnya skema tersebut tidak tahan terhadap serangan *malicious attack*.

Referensi

[1] Joachim J Eggers, Jonathan K.Su, dan Bernd Girod, *Publik Key Watermarking by Eigenvectors of Linear Transform*, EUSIPCO 2000.

[2] Mauro Barni dan Franco Bartolini, *Watermarking Systems Engineering*, Marcel Dekker Publishing, 2004.

[3] Scott Craver dan Stefan Katzenbeisser, *Security Analysis of Public-Key Watermarking Schemes*, 2000.

[4] Joachim J. Eggers, Jonathan K. Su, and Bernd Girod, *Asymmetric Watermarking Schemes*, GMD Jahrestagung, Proceddings, Springer-Verlag, 2000.

[5] Frank Hartung dan Bernd Girod, *Fast Public-Key Watermarking of Compressed Video*, Proceeding of the 1997 International Conference on Image Processing (ICIP ’97), 1997

[6] Joshua R. Smith and Chris Dodge, *Developments in Steganography*, Proceeding of the Third International Information Hidng Wokshop, 1999