PENERAPAN SISTEM KRIPTOGRAFI KUNCI-PUBLIK UNTUK MEMBENTUK SKEMA *PUBLIC-KEY WATERMARKING*, MUNGKINKAH?

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

Skema *public-key watermarking* mempunyai aplikasi riil untuk memverifikasi *watermark* di dalam dokumen multimedia yang tersebar di seluruh dunia. *Public-key watermarking* dapat dianggap sebagai teknologi *watermarking* generasi kedua. Konsep *public-key watermarking* banyak mengadopsi konsep di dalam sistem kriptografi kunci-publik. Sistem kriptografi kunci-publik dapat digunakan untuk membentuk *fragile public-key watermarking*, namun tidak cocok diterapkan untuk mendapatkan *robust public-key watermarking*. Sistem kriptografi kunci-publik dapat menjadi inspirasi untuk membentuk skema *public-key wateramrking.* Makalah ini mempresentasikan penggunaan kriptografi kunci publik untuk menghasilkan skema *public-key watermarking*.

Kata kunci: *watermark*, multimedia, *public-key watermarking, fragile, robust, public-key cryptography*.

1. PENDAHULUAN

Digital watermarking adalah teknik untuk menyisipkan informasi yang disebut *watermark* ke dalam dokumen multimedia (citra, audio, atau video). *Digital Watermarking* mempunyai banyak aplikasi, antara lain untuk bukti kepemilikan, otentikasi, perlindungan *copyright*, *fingerprinting*, dan *tamper proofing.*

Sejumlah skema *digital watermarking* sudah diusulkan dan dipresentasikan dalam beberapa tahun terakhir, tetapi kebanyakan dari skema tersebut simetri, artinya penyisipan dan pendeteksian *watermark* menggunakan kunci (rahasia) yang sama. Ini berarti proses penyisipan dan pendeteksian *watermark* hanya dapat dilakukan oleh pemilik multimedia, karena hanya ia yang mengetahui kunci. Skema *watermarking* simetri mempunyai aplikasi riil yang terbatas, karena produk multimedia saat ini sudah tersebar ke seluruh dunia (via internet), oleh karena itu pendeteksian *watermark* harus dapat dilakukan oleh siapapun tanpa harus memiliki kunci rahasia.

Skema *watermarking* simetri tidak cocok jika pendeteksian *watermark* dilakukan oleh peralatan yang tersebar di seluruh dunia, sebab sekali kunci diketahui oleh pihak lawan, maka kunci tersebut dapat digunakan untuk menghapus *watermark* dari data digital tanpa menimbulkan kerusakan yang berarti pada dokumen multimedia. Hal ini dikarenakan pada kebanyakan sistem simetri, kunci rahasia menspesifikasikan lokasi *watermark* di dalam dokumen multimedia, dan hanya orang yang mengetahui kunci yang dapat mendeteksi keberadaan *watermark*. Jika pihak penyerang berhasil mengetahui kunci ini, maka ia dapat menggunakan kunci tersebut untuk merusak atau menghapus *watermark*. Oleh karena itu, skema *watermarking* simetri tidak dapat melindungi data produk digital.

Masalah di atas dapat diselesaikan dengan menggunakan skema *asymmetric watermarking* atau lebih dikenal dengan nama *public-key watermarking*. Pada skema ini, pendeteksi *watermark* tidak membutuhkan kunci yang sama dengan kunci penyisipan. Penyisipan *watermark* (dilakukan oleh pemilik dokumen) menggunakan kunci (privat), tetapi pendeteksian *watermark* dapat dilakukan siapa saja asalkan ia memiliki kunci pendeteksian yang dibuat publik (tersedia untuk umum). Dengan skema ini, tidak ada kebutuhan mengirim kunci privat melalui saluran publik seperti halnya pada skema simetri.

Konsep *public-key watermarking* kebanyakan mengadopsi konsep di dalam sistem kriptografi kunci-publik (*public-key cryptography*), seperti konsep kunci privat dan kunci publik. Namun, tidak banyak teknik yang pernah diusulkan menggunakan kriptografi kunci-publik untuk menghasilkan skema *public-key watermarking*. Inilah yang menjadi pertanyaan: kenapa? Pertanyaan selanjutnya: apakah mungkin menggunakan algoritma kriptografi kunci publik untuk skema *public-key watermarking*?

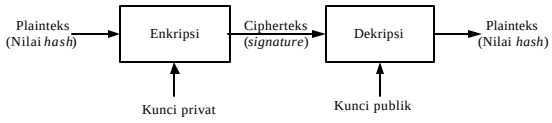
Makalah ini mempresentasikan *review* teknik yang tergolong ke dalam skema *public-key watermarking*. Kemudian dilanjutkan dengan

pembahasan mengenai penggunaan sistem kriptografi kunci-publik di dalam skema *public-key watermarking*.

2. SISTEM KRIPTOGRAFI KUNCI-PUBLIK

Pada sistem kriptografi kunci-publik, kunci kriptografi dibuat sepasang, satu kunci untuk enkripsi dan satu kunci untuk dekripsi. Kunci untuk enkripsi diumumkan kepada publik sehingga dinamakan kunci publik (*public-key*), sedangkan kunci untuk dekripsi bersifat rahasia sehingga dinamakan kunci privat (*private key*). Kunci privat diturunkan dari kunci publik, tetapi pengetahuan mengenai kunci publik tidak dapat digunakan untuk menemukan kunci privat.
Misalkan E adalah fungsi enkripsi dan D adalah fungsi dekripsi. Misalkan (e, d) adalah sepasang kunci publik dan kunci privat untuk enkripsi dan dekripsi. Pesan M dienkripsi dengan e menghasilkan cipherteks $C = E_e(M)$. Penerima pesan menggunakan d untuk mendekripsi cipherteks C menjadi plainteks $M = D_d(C) = D_d(E_e(M))$. Kedua persamaan ini menyiratkan bahwa dengan mengetahui e dan c, maka secara komputasi hampir tidak mungkin menemukan m. Asumsi lainnya adalah secara komputasi hampir tidak mungkin menurunkan d jika e diketahui. E_e digambarkan sebagai fungsi pintu-kolong (*trapdoor*) satu-arah dengan e adalah informasi *trapdoor* yang diperlukan untuk menghitung fungsi inversinya, D, yang selanjutnya membuat proses dekripsi dapat dilakukan. Salah satu algoritma kriptografi kunci-publik yang terkenal adalah algoritma *RSA*, pembahasan algoritma ini dapat ditemukan di dalam [2].

Salah satu kegunaan kriptografi kunci-publik yang penting adalah tanda-tangan digital (*digital signature*). Dalam hal ini, nilai *hash* dari pesan dienkripsi dengan menggunakan kunci privat pengirim (hasil enkripsinya disebut tanda-tangan digital), lalu tanda-tangan digital dilekatkan di dalam pesan (Gambar 1).



Gambar 1. Skema penandatangan pesan dengan sistem kriptografi kunci-publik

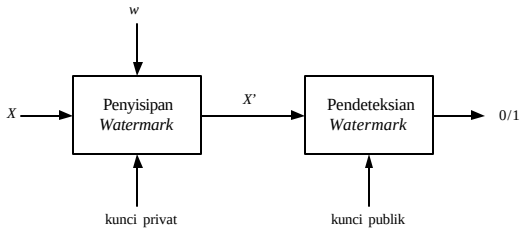
Di sisi penerima, verifikasi tanda tangan dilakukan dengan cara mendekripsinya menggunakan kunci publik pengirim, lalu hasilnya dibandingkan dengan nilai *hash* dari pesan. Beberapa agoritma kunci-publik seperti *RSA* dapat digunakan untuk menandatangani pesan dengan cara mengenkripsinya, asalkan algoritma tersebut memenuhi sifat: $D_{SK}(E_{PK}(M)) = M$ dan $D_{PK}(E_{SK}(M)) = M$, dengan PK = kunci publik dan SK = kunci privat (*secret key*).

Sayangnya, tanda-tangan digital tidak dapat digunakan sebagai *digital watermarking*, karena sekali tanda-tangan dilekatkan di dalam dokumen, ia dapat dihapus dengan mudah, yang menyebabkan verifikasi *watermark* tidak dapat dilakukan.

3. *PUBLIC-KEY WATERMARKING*

Public-key watermarking mengadopsi konsep yang terdapat di dalam sistem kriptografi kunci-publik, karena *watermark* dapat dipandang sebagai *signature* dari sinyal digital. Gambar 2 memperlihatkan skema umum *public-key watermarking* [3] (ket: X adalah *host signal* berupa data multimedia, w adalah *watermark*, dan X' adalah data multimedia yang sudah ber-*watermark*). Pendeteksian *watermark* secara sederhana hanya menghasilkan keluaran apakah *watermark* ditemukan ("1") atau tidak ("0").

Teknik *public-key watermarking* ini dilakukan dengan suatu cara sedemikian sehingga [1]: (a) secara komputasi tidak mungkin menghitung kunci privat dari kunci publik, dan (b) kunci publik tidak dapat digunakan oleh penyerang untuk menghilangkan *watermark*. *Watermark* yang bersifat *public* 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*) [4].



Gambar 2. Skema umum *public-key watermarking*

Publikasi teknik *public-key watermarking* masih sedikit, berikut ini *review* beberapa teknik saja:

1. Sebagian kunci privat dijadikan publik

Publikasi pertama mengenai teknik *public-key watermarking* diperkenalkan oleh Hartung dan Girod [5]. Teknik ini pada dasarnya merupakan

perluasan dari skema *spread spectrum watermarking* simetri yang diterapkan pada video digital. Idenya adalah membuat sebagian dari kunci privat menjadi publik. Penerima hanya dapat mendeteksi bagian *watermark* yang publik. Kelemahan teknik ini, penerima juga dapat menghapus bagian *watermark* ini. Meskipun bagian *watermark* lainnya tidak berubah, *detector watermark* tidak dapat lagi mendeteksi keseluruhan *watermark*. Ini berarti pendeteksi *watermark* hanya dapat bekerja sekali dan sesudah itu kunci publik tidak bisa digunakan lagi.

2. *Legendre watermarking*

Schyndel dkk di dalam [6] mempresentasikan skema pertama mengenai penggunaan autokorelasi, yang didasarkan pada penyisipan barisan *Legendre*. Dalam hal ini, kunci privat yang sekaligus sebagai *watermark*, adalah barisan *Legendre* dan kunci publiknya adalah panjang barisan (p). Barisan *Legendre* ini disisipkan ke dalam data multimedia. Barisan *Legendre* invarian di dalam transformasi Fourier, karena itu barisan ini berkorelasi dengan transformasi *Fourier* konyugasinya. Sayangnya teknik ini dapat diserang dengan *exhaustive attack* [3], karena hanya terdapat $p - 2$ barisan *Legendre* berbeda. Kelemahan lainnya, barisan *Legendre* hanya ada untuk bilangan prima saja.

3. *Eigenvectos watermarking*

Teknik ini diusulkan oleh Eggers dkk di dalam [3], yang dalam hal ini *watermark* adalah vektor *eigen* dari sebuah matriks transformasi. Vektor *eigen* disisipkan ke dalam data multimedia. Vektor *eigen* berkorelasi dengan matriks transformasi tersebut. Kunci privat adalah vektor *eigen* dari matriks transformasi sedangkan kunci publiknya adalah matriks transformasi itu sendiri. Persoalan utama teknik ini adalah metode pembangkitan kunci privat dan kunci publik, karena terbukti tidak aman secara kriptografis [11]. Oleh karena itu, telah ditemukan cara untuk menghilangkan *watermark* seperti dilaporkan oleh [7].

4. KRIPTOGRAFI KUNCI-PUBLIK DAN *FRAGILE WATERMARKING*

Kriptografi dan *watermarking* jelas saling berkait, dan keduanya digunakan secara terpisah. Misalnya, *watermark* dienkripsi sebelum disisipkan ke dalam data multimedia.

Sistem kriptografi kunci-publik dapat digunakan untuk membentuk skema *fragile public-key watermarking*. Pada *fragile watermarking*, *watermark* dikatakan mudah rusak (*fragile*) jika ia berubah, rusak, atau malah hilang jika data multimedia dimodifikasi[1]. Aplikasi *fragile watermarking* misalnya untuk otentikasi data dan bukti kepemilikan (*ownership*), dimana *watermark* yang hilang atau berubah adalah pertanda bahwa data multimedia sudah dirusak (*tamper*), dan verifikasi *watermark* di dalam data dapat digunakan untuk menunjukkan kepemilikan data. Umumnya fungsi *hash* seperti *MD5* atau *SHA* diperlukan untuk mendukung proses otentikasi. Dua buah skema *fragile public-key watermarking* dijelaskan di bawah ini.

(i) Algoritma Wong

Contoh pertama teknik *fragile public-key watermarking* yang berdasarkan pada sistem kriptografi kunci-publik adalah algoritma Wong [10]. Garis besar algoritmanya sebegai berikut: mula-mula semua bit *LSB* (*Least Significat bit*) setiap *pixel* citra X dinolkan menjadi X_z, lalu nilai *hash* dari citra X_z plus ukuran citra ($N \times M$) di-*XOR*-kan dengan *watermark* w (yang dalam hal ini citra biner). Selanjutnya, hasil peng-*XOR*-an ini dienkripsi dengan kunci privat, lalu disisipkan ke dalam dokumen citra semula (disisipkan pada bit *LSB*) menghasilkan citra ber-*watermark*, X'.

Verifikasi *watermark* menggunakan kunci publik. Citra masukan Y (Y mungkin sama dengan X', atau Y tidak mengandung *watermark*, atau Y adalah X' yang telah mengalami perubahan) diekstraksi bit-bit *LSB*-nya, lalu rangkaian bit ini didekripsi dengan menggunakan kunci publik. Hasil dekripsi kemudian di-*XOR*-kan dengan nilai *hash* dari citra Y' (yang bit *LSB* nya telah dinolkan) plus ukuran citra ($N \times M$) untuk menghasilkan *watermak* yang terekstraksi, w. Perubahan yang dilakukan pada citra ber-*watermark* dapat dideteksi dengan melakukan pengamatan visual terhadap w yang diekstraksi. Jika citra ber-*watermark* telah diubah, maka *watermark* w hasil ekstraksi muncul sebagai gambar dengan pola acak (bukan *watermark* yang benar). Selain itu, karena verifikasi menggunakan kunci publik pemilik multimedia, maka kunci publik juga mengimplikasikan kepemilikan dokmen multimedia. Penggunaan kunci publik yang salah akan menghasilkan luaran yang berupa nilai-nilai acak (bukan *watermark*).

(ii) Algoritma Geruta

Geruta dkk [11] mempresentasikan teknik *public-key watermarking* untuk pembuktian keaslian dokumen citra (*tamper-proof*). Algoritma penyisipan dan pendeteksian dilakukan dalam domain *wavelet transform* (*DWT*). Infrastruktur kunci publik (*PKI*) seperti manajemen kunci publik di dalam *PGP* (*Pretty Good Privacy*) digunakan sebagai elemen untuk verifikasi identitas pengirim dan juga untuk menyimpan kunci pendeteksian *watermark*. Penggunaan *PKI* adalah untuk

menyediakan manajemen kunci yang kuat secara kriptografis, karena kebanyakan skema *public-key watermarking* menggunakan manajemen kunci yang baru atau independen secara kriptografis.

Watermark w adalah nilai *hash* dari transformasi *wavelet* citra masukan *X*. Nilai *hash* ini dienkripsi dengan menggunakan kunci privat pemilik citra, lalu disisipkan ke dalam *X* dalam domain *wavelet transform*. Penyisipan *watermark* berdasarkan rumus yang diusulkan oleh Cox [11]. Selanjutnya dilakukan transformasi *wavelet* inversi untuk mendapatkan citra ber-*watermark*, *X'*

Pendeteksian *watermark* dilakukan dengan mula-mula mengekstraksi *watermark* dari citra masukan. *Watermark* kemudian didekripsi dengan kunci publik. Selanjutnya verifikasi antara *watermark* hasil dekripsi dengan nilai hash dari citra ber-*watermark* dihitung untuk menentukan apakah citra ber-*watermark* mengalami perubahan atau tudak.

5. KRIPTOGRAFI KUNCI-PUBLIK DAN *ROBUST WATERMARKING*

Robust watermarking adalah jenis *watermarking* dimana *watermark* harus kokoh (*robust*) terhadap serangan yang bertujuan untuk merusak atau menghapus *watermark*. Aplikasi utama robust watermarking adalah *copyright protection* dan *fingerprinting* [1]. Namun, mengkombinasikan sistem kriptografi kunci-publik dengan *watermarking* untuk mendapatkan skema *robust public-key watermarking* tidak dilakukan orang karena dua alasan di bawah ini.

Pertama, sistem kriptografi kunci-publik tidak dipakai untuk menghasilkan *watermarking* yang kokoh, karena perubahan kecil pada data multimedia (akibat suatu serangan) dapat menyebabkan dekripsi gagal. Sebagaimana disebutkan oleh Cox, Miller, dan Bloom di dalam [8], kriptografi memetakan plainteks dan cipherteks satu-ke-satu dan perubahan kecil pada plainteks menghasilkan perubahan acak pada cipherteks. Sebaliknya, pada *watermarking*, perubahan kecil pada data multimedia seharusnya tetap memungkinkan untuk mendeteksi *watermark*.

Kedua, tidak meningkatkan keamanan sistem. Misalnya pemilik data multimedia mengenkripsi *watermark* dengan algoritma *RSA* dan menggunakan kunci privat sebelum disisipkan ke dalam dokumen multimedia. Memang benar bahwa *watermark* dapat dideteksi oleh siapapun (termasuk pihak lawan) yang mempunyai kunci publik, tetapi karena algoritma deteksi tidak dirahasiakan, maka pihak lawan dapat menghapus *watermark* di dalam data multimedia dengan malakukan *hack* program *watermarking* atau mentransformasikan *watermark* dengan menggunakan serangan yang mangkus seperti *Stirmark* [9].

Meskipun tidak digunakan secara langsung, namun beberapa skema *robust public-key watermarking* diinspirasi oleh sistem kriptografi kunci- publik. Beberapa buah skema *robust public-key watermarking* dijelaskan di bawah ini.

(i) Algoritma Furon dan Duhamel.

Furon dan Duhamel mengusulkan teknik *watermarking* yang didasarkan pada pemrosesan sinyal satu-arah [7, 8]. Seperti kita ketahui, kriptografer menggunakan fungsi satu-arah dengan *trapdoor* (kunci rahasia) untuk mendapatkan kunci publik. Fungsi satu arah tidak mungkin dapat di-inversi tanpa mengetahui kunci rahasia. Furon dan Duhamel tidak benar-benar menggunakan fungsi satu-arah dengan *trapdoor*, mereka memakai prinsip ini. Mereka mengidentifikasi fungsi di dalam pemrosesan sinyal, yaitu *power density spectrum* (*PDS*), sebagai calon fungsi satu-arah. Hasil dari fungsi ini tidak memungkinkan rekonstruksi sempurna dari sinyal.

Mula-mula, sinyal *host* (yaitu data multimedia yang akan di-*watermark*) *X* dipermutasi menjadi X_p agar memperoleh *PDS* yang *flat* (tidak ada ketergantungan statistik antar sinyal yang bertetangga). Sinyal *watermark w* yang independen terhadap X_p dijumlahkan dengan X_p seperti pada *spread spectrum watermarking* menjadi sinyal publik $S = X_p + w$. Kunci privat adalah *w* sedangkan *PDS* dari *S* merupakan kunci publik. Selanjutnya, permutasi acak dikembalikan pada *S* dan menghasilkan sinyal ber-*watermark X'*.

Pendeteksian *watermark* dilakukan terhadap sinyal masukan *Y* (*Y* mungkin sama dengan *X'*, atau *Y* tidak mengandung *watermark*, atau *Y* adalah *X'* yang telah mengalami perubahan). Proses deteksi tidak membutuhkan pengetahuan mengenai *watermark w* (yang juga merupakan kunci privat), tetapi hanya membutuhkan *PDS* dari *S*. Mula-mula terhadap *Y* dilakukan permutasi secara acak, lalu *PDS* nya dihitung dan tes hipotesis dilakukan untuk memverifikasi kesamaannya dengan kunci publik.

Sayangnya, serangan yang dilakukan untuk menghapus *watermark* dari dalam data multimedia telah ditemukan seperti yang dilaporkan di dalam [7].

(2) Penggunaan Protokol Pengetahuan-Nol

Craver menggunakan protokol pengetahuan nol (*zero knowledge protocol*) untuk membuktikan

keberadaan *watermark* di dalam sinyal [8, 11, 12]. Primitif kriptografi yang digunakan adalah pembuktian pengetahuan-nol yang didasarkan pada isomorfisma graf. Kunci privat adalah permutasi *P* pada grup berhingga yang beranggotakan *n* elemen. Kunci publik adalah graf *G* dan dan permutasinya, *P*(*G*).

Sinyal *host X* diperlakukan sebagai *array n* elemen. *Watermark w* disisipkan ke dalam *X* sehingga dihasilkan sinyal ber-*watermark X'*. Tanda-tangan dari *X'* adalah *tupple* <*P*(*X'*), *P*(*w*)>. Protokol membutuhkan berkali-kali putaran antara pengirim (Alice) dan penerima sinyal (Bob) untuk memperoleh keyakinan bahwa *w* disisipkan ke daalm *X*. Skema ini sebenarnya tidak memecahkan persoalan industri yang menggunakan *public-key watermarking*, sebab ia membutuhkan banyak data untuk membuktikan keberadaan *watermark*, membutuhkan banyak komputasi, dan membutuhkan banyak pertukaran antara data antara pengirim dan penerima [8].

Pembuktian interaktif dengan protokol pengetahuan- nol dapat ditansformasikan menjadi skema tanda-tangan [8]. Bila transformasi itu diterapkan, kita dapat melakukan verifikasi tanda-tangan secara *off-line*, tetapi kita kehilangan sifat pengetahuan-nol. Pada sisi lain, jika tanda-tangan dihapus, *watermark* tidak dapat diverifikasi keberadaannya.

6. KESIMPULAN

Public-key watermarking mengadopsi konsep di dalam sistem kriptogtrafi kunci-publik. Makalah ini sudah menunjukkan bahwa kita dapat menggunakan sistem kriptografi kunci-publik untuk memperoleh skema *fragile public-key watermarking*, tetapi ia tidak dapat (atau belum dapat) diterapkan untuk memperoleh *robust public-key watermarking*. Skema *public-key watermarking* yang *robust* dapat diperoleh dengan meniru perilaku sistem kriptografi kunci-publik, seperti penggunaan fungsi satu-arah dan protokol keriptografi.

Penelitian mengenai *public-key watermarking* masih sedikit. Masih terbuka peluang untuk menemukan skema *robust public-key watermarking* yang elegan, sederhana, mudah diimplementasikan, namun tetap aman.

REFERENSI

1. Mauro Barni dan Franco Bartolini, *Watermarking Systems Engineering*, Marcel Dekker Publishing, 2004.
2. Bruce Schneier, *Aplied Cryptography 2nd*, John Wiley & Sons, 1996
3. Joachim J Eggers, Jonathan K.Su, dan Bernd Girod, *Public Key Watermarking by Eigenvectors of Linear Transform*, EUSIPCO 2000.
4. Joshua R. Smith and Chris Dodge, *Developments in Steganography*, Proceeding of the Third International Information Hidng Wokshop, 1999.
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. R. G. van Schyndel, A. Z. Tirkel, I. D. Svalbe, *Key Independent Watermark Detection*, in Proceeding of the IEEE Intl. Conference on Multimedia Computing and Systems, volume 1, Florence, Italy, June 1999.
7. Joachim J. Eggers, Jonathan K. Su, and Bernd Girod, *Asymmetric Watermarking Schemes*, GMD Jahrestagung, Proceddings, Springer-Verlag, 2000.
8. Gael Hachez and Jean-Jacques Quisquater, *Which Directions for Asymmetric Watermarking?*
9. Tedy Furon and Pierre Duhanel, *An Asymmetric Public Detection Watermarking Technique*, Proceeding of 3rd Int. Work. On Information Hiding, Dresden, Sept. 1999.
10. Ping Wah Wong, *A Public Key Watermark for Image Verification and Authentication*, IEEE Transaction on Image Processing, 198.
11. Geruta Kazakeviciute, *Tamper-Proof Image Watermarking, Based on Existing Public Key Infrastructure*, Informatica 2005, Vol. 16, No. 1, 1- 18.
12. Scott Craver dan Stefan Katzenbeisser, *Security Analysis of Public-Key Watermarking Schemes*, 2000.