SKEMA *ASYMMETRIC WATERMARKING* BERBASISKAN UJI KORELASI

Rinaldi Munir[1], Bambang Riyanto[2], Sarwono Sutikno[3], Wiseto P. Agung[4]
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], wiseto@telkom.co.id[4]

Abstract
Asymmetric watermarking is second generation watermarking scheme which uses different keys for embedding and detecting watermark. Key for embedding is private or secret, but key for detecting can be avalaible publicly and everyone which haves the key can detect watermark. Watermark detection need not original multimedia data. Detection of watermark is realized using correlation test between public key and multimedia data received. In most of schemes, private key is the watermark itself; public key is public watermark which correlates with the private watermark. This paper presents asymmetric watermarking scheme that based on correlation test and some schemes of asymmetric watermarking that have been proposed by researchers.

Keywords: *asymmetric watermarking, private key, public key, watermark, multimedia, correlation.*

1. PENDAHULUAN

Data multimedia seperti citra digital, audio, video, dan lain-lain mudah digandakan, diubah, dan didistribusikan. *Digital watermarking* merupakan teknik yang digunakan untuk melindungi *copyright* data multimedia tersebut. Persyaratan utama skema *digital watermarking* adalah *imperceptibility*, *robustness*, dan *security* [1]. Gambar 1 adalah contoh sebuah citra sebelum dan sesudah diberi *watermark* beserta *watermark* yang disisipan (berupa logo '@').

Citra asal Citra ber-*watermark*

watermark

Gambar 1. Citra sebelum dan sesudah di-*watermark*

Sejumlah skema *watermarking* sudah banyak dipublikasikan dalam beberapa tahun terakhir. *Review* beberapa metode dapat ditemukan dengan baik di dalam [2]. Satu masalah di dalam *state-of-the-art* skema *watermarking* tersebut adalah mereka umumnya simetri, artinya kunci untuk menyisipkan *watermark* sama dengan kunci untuk mendeteksi *watermark* dan kunci tersebut ini harus dijaga kerahasiaannya. Hal ini berarti penyisipan dan pendeteksian *watermark* hanya dapat dilakukan oleh pemilik data multimedia atau pihak lain yang sangat dipercaya. Skema *watermarking* simetri mempunyai aplikasi riil yang terbatas, karena data multimedia saat ini sudah tersebar ke seluruh dunia (via internet), oleh karena itu pendeteksian *watermark* juga harus dapat dilakukan oleh alat atau siapapun tanpa harus memiliki kunci rahasia.

Skema *watermarking* simetri jelas tidak cocok jika kunci untuk mendeteksi *watermark* diberikan kepada *detector*, sebab pada kebanyakan sistem simetri kunci adalah *watermark* itu sendiri atau kunci menspesifikasikan lokasi penyisipan *watermark* di dalam data multimedia. Dengan mengingat prinsip Kerckhoff [3] yang menyatakan bahwa suatu skema sekuriti seperti kriptografi dan *watermarking* harus mengasumsikan bahwa lawan mengetahui segala sesuatu mengenai algoritmanya, maka pihak lawan yang mengetahui algoritma *watermarking* dapat menggunakan kunci tersebut untuk menghapus *watermark* dari data multimedia tanpa menimbulkan kerusakan yang berarti pada data tersebut.

Masalah di atas dapat diselesaikan dengan menggunakan skema *asymmetric watermarking*. Pada skema ini, kunci untuk menyisipkan *watermark* berbeda dengan kunci untuk mendeteksi *watermark*. Cara ini dapat meningkatkan keamanan daripada skema simetri. Konsep *asymmetric watermarking* banyak diadposi dari *asymmetric*

cryptography. Sebagaimana kita ketahui, pada *asymmetric cryptography*, kunci untuk enkripsi berbeda dengan kunci untuk dekripsi.

Skema *asymmetric watermarking* sering dirancukan dengan *public-key watermarking* padahal kedua terminologi ini sebenarnya berbeda. *Asymmetric watermarking* menjadi *public-key watermarking* jika kunci untuk mendeteksi *watermark* dipublikasikan sehingga siapapun dapat melakukan pendeteksian. Kunci untuk menyisipkan *watermark* disebut kunci privat (hanya pemilik data multimedia yang mengetahuinya), sedangkan kunci untuk mendeteksi *watermark* disebut kunci publik. (siapapun dapat mendeteksi *watermark* jika ia mengetahui kunci publik). Skema *public-key watermarking* ini dilakukan dengan suatu cara sedemikian sehingga: (a) secara komputasi tidak mungkin menghitung kunci privat dari kunci publik, dan (b) kunci publik tidak dapat digunakan oleh penyerang untuk menghilangkan *watermark*. *Asymmetric watermarking* mungkin dapat dipandang sebagai sebuah cara merealisasikan *public-key watermarking*. Beberapa skema *public-key watermarking* sudah dipublikasikan oleh [4]-[8] dan analisis keamanan skema tersebut dapat ditemukan di dalam [12] dan [15].

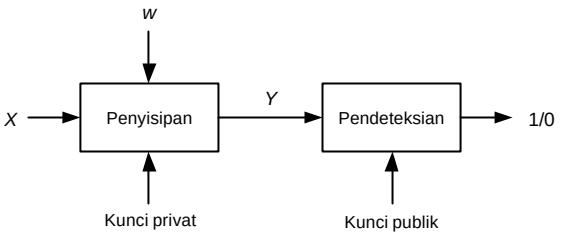
Secara umum, di dalam skema *asymmetric watermarking*, deteksi *watermark* biasanya direalisasikan dengan uji korelasi antara *watermark* publik dengan sejumlah koefisien data multimedia yang diterima. Hasil pendeteksian adalah keputusan biner yang mengindikasikan apakah data multimedia tersebut mengandung *watermark* atau tidak.

Makalah ini mempresentasikan konsep *asymmetric watermarking* berbasiskan uji korelasi dan *review* beberapa skema *asymmetric watermarking* yang berbasiskan prinsip ini.

3. *ASYMMETRIC WATERMARKING*

Mula-mula, kita perlu menjelaskan notasi yang digunakan untuk menggambarkan skema *asymmetric watermarking*. Misalkan X adalah *host signal* yaitu fitur yang diekstraksi dari data multimedia dan w adalah informasi *watermark*. Sinyal X yang berlaku sebagai pembawa informasi *watermark*. X dapat berupa *pixel-pixel* citra atau video, data audio, atau koefisien tansformasi (*DCT*, *FFT*, *DWT*, dan lain-lain). Di dalam makalah ini, kita menyatakan X sebagai *array* linier yang panjangnya N, yaitu $X = (x(1), x(2), \ldots, x(N))$, yang dalam hal ini $x(i)$ adalah data sinyal ke-i. Hal yang sama kita gunakan untuk informasi *watermark* w sebagai *array* linier $w = (w(1), w(2), \ldots, w(N))$.

Pendeteksian *watermark* menggunakan kunci publik dan secara sederhana hanya menghasilkan keluaran apakah *watermark* ada ("1") atau tidak ada ("0") di dalam sinyal yang diterima. Gambar 2 memperlihatkan skema umum *asymmetric watermarking*.



Gambar 2. Skema umum *asymmetric watermarking*

Penyisipan w ke dalam X menggunakan kunci privat dan menghasilkan sinyal ber-*watermark* Y. Pada kebanyakan sistem *asymmetric watermarking*, kunci privat adalah *watermark* itu sendiri (disebut juga *watermark* privat, disimbolkan dengan w_s); ini berarti informasi *watermark* bersifat rahasia. Biasanya penyisipan *watermark* diimplementasikan sebagai penjumlahan X dengan *watermark* privat w_s menggunakan kontrol parameter α, yang secara sederhana dinyatakan dengan rumus

$$Y = X + \alpha w_s \qquad (1)$$

Nilai α, dinamakan juga kekuatan *watermarking*, dipilih sedemikian rupa sedemikian sehingga menyeimbangkan antara *imperceptibility* dan kemampuan deteksi.

Pendeteksian *watermark* tidak membutuhkan kunci privat dan sinyal *host* (X), tetapi membutuhkan kunci publik. Pada kebanyakan sistem *asymmetric*, kunci publik adalah *watermark* yang dibuat publik (disebut juga *watermark* publik dan disimbolkan dengan w_p). *Watemark* publik dibuat sedemikian rupa sehingga berkorelasi dengan *watermark* privat. *Watermark* publik dapat dibangkitkan dengan banyak cara, antara lain dengan melakukan transformasi T terhadap *watermark* privat:

$$w_p = T(w_s) \qquad (3)$$

Transformasi T adalah transformasi yang bersifat satu-arah, sehingga secara komputasi hampir tidak mungkin mendedksi *watermark* privat (kunci privat) dari *watermark* publiknay (kunci publik).

Karena sinyal *host* tidak dibutuhkan dalam proses deteksi, maka pendeteksian tidak dapat mengekstraksi kembali *watermark* dari sinyal yang diuji tetapi hanya mendeteksi keberadaannya, yaitu apakah *watermark* tersebut terdapat atau tidak di dalam sinyal uji. Pendeteksian dilakukan dengan

cara uji korelasi yaitu menghitung korelasi antara kunci publik dan sinyal yang diterima, lalu membandingkan hasil korelasi tadi dengan sebuah nilai ambang (*threshold*). Misalkan sinyal yang diuji adalah $Y^* = (y^*(1), y^*(2), \ldots, y^*(N))$ dan kunci publik adalah $w_p = (w_p(1), w_p(2), \ldots, w_p(N))$. Y^* mungkin sinyal ber-*watermark* atau tidak mengandung *watermark* w_s. Korelasi antara sinyal Y^* dan kunci publik w_p dihitung dengan persamaan

$$C = \frac{1}{N}\sum_{i=1}^{N} y^*(i) w_p(i) \qquad (4)$$

selanjutnya C dibandingkan dengan sebuah nilai ambang T untuk memutuskan apakah *watermark* w terdapat di dalam sinyal uji:

$$d = \begin{cases} 1 & , C \geq t \\ 0 & , C < t \end{cases} \qquad (5)$$

Watermark privat hanya dapat dideteksi keberadaannya bila *watermark* publik berkorelasi dengan sinyal uji. Karena *watermark* w_s dijumlahkan ke dalam X, maka jika $X^* = X'$, yaitu sinyal yang diterima adalah sinyal yang mengandung *watermark*, maka *watermark* publik juga akan berkorelasi dengan sinyal uji.

Nilai ambang t dapat ditemukan melalui eksperimen dengan cara mengamati korelasi antara beberapa barisan acak atau secara analitik. Secara analitik misalnya menggunakan rumus [9]:

$$t = \frac{a}{S.N}\sum_{N}|Y| \qquad (6)$$

yang dalam hal ini S adalah simpangan baku yang nilainya 2 atau 3. Tentu saja pemilihan nilai t mempengaruhi peluang deteksi-salah dan deteksi-benar. Banyak penelitian yang telah dilakukan untuk menemukan nilai ambang ini.

Skema *asymmetric watermarking* selain harus kokoh terhadap *non-malicious attack* seperti operasi pengolahan sinyal yang umum (kompresi, *cropping*, rotasi, dan sebagainya), juga harus kokoh terhadap *malicious attack*, yaitu serangan yang bertujuan untuk menghapus *watermark* dari dalam sinyal. Selain kedua jenis serangan tersebut, skema *asymmetric watermarking* juga harus kokoh terhadap serangan *subtraction attack*, yaitu penyerang mengurangkan sinyal ber-*watermark* dengan *watermark* publik tanpa menimbulkan kerusakan yang berarti. Serangan yang terakhir ini tidak dimaksudkan untuk menghapus *watermark*, tetapi untuk menghambat pendeteksian *watermark*.

4. BEBERAPA SKEMA *ASYMMETRIC*

Untuk memberikan gambaran mengenai skema *asymmteric watermarking* yang berbasikan pada uji korelasi, dibawah ini dipresentasikan secara ringkas beberapa proposal skema yang sudah dipublikasikan.

4.1 Proposal G.Gui (1)

Gui di dalam [10] memaparkan *skema asymmetric watermarking* berbasis matriks *non-full rank*. *Watermark* privat w_s yang panjangnya N dibangkitkan dari pembangkit bilangan semi-acak, dan elemen-elemen barisan adalah biner {1, –1}. *Watermark* publik dihasilkan dengan mengalikan sebuah matriks bujursangkar *non-full rank* , $T = \{t_{ij}, 1 \leq i, j \leq N\}$:

$$w_p = Tw_e \qquad (7)$$

Matriks T tidak perlu dirahasiakan. Penyisipan *watermark* dilakukan dalam ranah *transform* (*wavelet*) dengan menggunakan rumus (1). Pendeteksian *watermark* mula-mula didahului dengan mengalikan T dengan sinyal yang diuji, Y^*, menghasilkan $z = TY^*$, lalu menghitung korelasi

$$C = \frac{1}{N}\sum_{i=1}^{N} w_p(i) z(i) \qquad (8)$$

dan membandingkan C dengan nilai ambang yang dipilih untuk menentukan keberadaan *watermark*.

Karena T, w_p, dan algoritma *watermarking* tersedia secara publik, maka pihak lawan mungkin menggunakan informasi ini untuk mendeduksi *watermark* privat dan menghapusnya melalui persamaan:

$$Tv = w_p \qquad (9)$$

Jika *watermark* privat $v = w_s$ dapat dihitung dari persamaan (9), maka pihak lawan akan menggunakannya untuk menghapus w_s dari sinyal ber-*watermark* dan mendapatkan sinyal *host* (X) tanpa kerusakan berarti berdasarkan persamaan (1):

$$X = Y - \alpha w_s \qquad (10)$$

Tetapi, karena T adalah matriks *non-full rank*, maka persamaan (9) tidak dapat diselesaikan. Jika *rank* T cukup kecil, maka secara komputasi juga tidak mungkin menurunkan *watermark* privat $v = w_s$ dari persamaan (9).

4.2 Proposal G. Gui (2)

Gui di dalam [11] mengusulkan skema *asymmetric watermarking* yang menggunakan banyak *watermark* publik. *Watermark* privat diturunkan dari sejumlah *watermark* publik. Tujuan yang hendak dicapai adalah mendapatkan skema deteksi publik dengan kekokohan yang sama dengan deteksi secara privat. Idenya didasarkan pada fakta bahwa pada kebanyakan skema *asymmetric watermark* publik hanya sebagian berkorelasi dengan *watermark* privat, artinya hanya sebagian informasi *watermark* privat terdapat di dalam *watermark* publik. Jika semua informasi *watermark* publik tersembunyi di dalam *watermark* privat, maka deteksi secara publik akan sekokoh deteksi secara privat.

Misalkan terdapat M ($M \geq 2$) buah *watermark* publik, w_{p1}, w_{p2}, …, w_{pM}, yang dibangkitkan dari pembangkit bilangan semi-acak dan elemen-elemen barisan adalah biner {1, –1}. Setiap *watermark* publik mempunyai rerata 0 (*zero mean*) dan satu sama lain saling ortogonal (yaitu $w_{pk} \cdot w_{pl} \cong 0$ untuk $k \neq l$). Kemudian terdapat M buah vektor rahasia biner t_1, t_2, …, $t_M \in \{0, 1\}$ yang masing-masing panjangnya N dan $\sum_{k=1}^{M} t_k(i) = 1$ untuk sembarang i. *Watermark* privat dibangkitkan dari persamaan:

$$w_s(i) = \sum_{k=1}^{M} t_k(i) w_{pk}(i), \text{ i} = 1, 2, \ldots, N \qquad (11)$$

yang dalam hal ini $w_s(i)$ adalah elemen ke-i dari *watermark* privat w_s. Semua *watermark* publik berkorelasi dengan *watermark* privat ini dan koefisien korelasinya ditentukan oleh vektor rahasia t_k.

Penyisipan *watermark* privat w_s ke dalam sinyal *host* X dilakukan dalam ranah *transform* dengan menggunakan rumus (1). Pendeteksian *watermark* dilakukan dengan menghitung korelasi antara *watermark* publik w_{pk} dengan sinyal uji yang diterima, Y^* (diasumsikan $Y^* = Y + n$, yang dalam hal ini n adalah derau) dengan menggunakan persamaan

$$C_p = \frac{1}{N} \sum_{k=1}^{M} Y^* w_{pk} \qquad (12)$$

Karena *watermark* publik mempunyai rerata nol dan independen dari sinyal *host* dan derau, persamaan (12) jika diselesaikan akan menghasilkan $C_p \cong \alpha$. Dengan membandingkan C dengan nilai ambang yang telah ditetapkan, maka *watermark* dapat dideteksi keberadaannya.

Pendeteksian secara privat juga dapat dilakukan dengan menghitung korelasi antara *watermark* privat w_s dengan sinyal uji yang diterima, Y^* (diasumsikan $Y^* = Y + n$, yang dalam hal ini n adalah derau) dengan menggunakan persamaan

$$C_s = \frac{1}{N} \sum_{i=1}^{N} Y^*(i) w_s(i) \qquad (13)$$

yang menghasilkan $C_s \cong \alpha$. Karena nilai C_s sama dengan C_p.maka dapat disimpulkan bahwa deteksi secra publik memiliki kekokohan dengan deteksi secara privat [11].

4.3 Proposal Y. Fu

Yong-Gang Fu dkk di dalam [13] mengusulkan skema *asymmetric watermarking* yang menyisipkan *watermark* privat dan *watermark* publik sekaligus ke dalan sinyal *host*. Kedua *watermark* ini tidak berkorelasi satu sama lain. Deteksi *watermark* dapat dilakukan baik secara privat maupun publik.

Pemilik data multimedia memilih pasangan kunci rahasia (k_1, k_2), yang dalam hal ini k_1 adalah bilangan bulat sembarang dan k_2 adalah bilangan bulat di dalam selang [N/2, 2N/3]. Dua buah bilangan bulat ini digunakan untuk membangun fungsi satu-ke-satu:

$$f(i) = ((k_1 + k_2 i) \bmod N) + 1 \qquad (14)$$

untuk $i = 1, 2, \ldots, N$.

Watermark privat w_s mempunyai rerata 0 dan variansi σ serta independen dari sinyal *host*. *Watermark* publik w_p adalah versi terenkripsi dari w_s dengan menggunakan fungsi f:

$$\begin{aligned} w_p &= (w_p(1), w_p(2), \ldots, w_p(N)) \\ &= (w_s(f(1)), w_s(f(2)), \ldots, w_s(f(N)) \end{aligned} \qquad (15)$$

Kedua *watermark* ini disisipkan ke dalam sinyal *host* (dalam ranah *transform*) dengan persamaan:

$$Y = X + (1 - \alpha) w_s + \alpha w_p \qquad (16)$$

Nilai α, yang berada di dalam selang [0, 1], bertujuan untuk mengontrol kompromi antara *watermark* privat dan *watermark* publik.

Pendeteksian dapat dilakukan secara priivat maupun secara prublik. Pendeteksian secara publik dilakukan dengan menhitung korelasi antara *watermark* publik w_p dan sinyal yang diuji, Y^*, dengan persamaan (4). Nilai ambang yang digunakan adalah $t = \alpha\sigma^2/2$, yaitu jika nilai $abs(C) > t$ maka disimpulkan sinyal uji mengandung *watermark*. Pendeteksian secara privat dilakukan

dengan menghitung korelasi antara sinyal yang diuji *Y** dan *watermark* privat w_s dengan persamaan

$$C_s = \frac{1}{N}\sum_{i=1}^{N} Y^*(i)w_s(i) \qquad (17)$$

Jika pihak lawan mencoba melakukan *subtraction attack*, yaitu mengurangkan sinyal ber-*watermark Y* dengan *watermark* publik, $Y' = Y - w_p$, maka *watermark* masih bisa dideteksi keberadaannya jika syarat $1 - \alpha > \alpha$, yaitu $\alpha < 1/2$, terpenuhi [13].

4.4 Proposal Choi

Choi dkk [16] mengusulkan skema *public-key watermarking* berdasarkan *transformed-key*, yang dinamakan *transformed-key watemarking* (*TKW*). Matriks transformasi *G* yang berukuran $N \times N$ dan tidak dapat diinversikan dikalikan dengan himpunan *u* yang panjangnya *N*. Untuk penyederhanaan, *u* haruslah himpunan yang ortonormal, yaitu $u^t u = 1$.

Penyisipan watermark

Kunci privat adalah *Gu* dan *watermark* privat yang bersesuaian dibangkitkan dengan persamaan

$$w_s = g_s Gu \qquad (18)$$

Kunci publik adalah $G^{-t}u$ dan *watermark* publik yang bersesuaian dibangkitkan dengan persamaan

$$w_p = g_p G^{-t} u \qquad (19)$$

yang dalam hal ini $g_s = \|Gu\|^{-1}$ dan $g_p = \|G^{-t}u\|^{-1}$, yang dalam hal ini G^{-t} menyatakan *invers* transpose dari *G*. Perhatikan bahwa $\|w_p\| = \|w_s\| = 1$. Koefisien γ_s dan γ_p dimaksudkan untuk menormalkan kunci privat dan kunci publik dan agar mempunyai kekuatan yang sama seperti *u*. *Gu* ijaga rahasia, sedangkan $G^{-t}u$ dipublikasikan.

Penyisipan *watemark* ke dalam sinyal *host X* dilakukan dengan operasi penjumlahan,

$$Y = X + aw_s = x + ag_s Gu \qquad (20)$$

Koefisien α adalah konstanta yang membuat *watermark* tidak dapat dipersepsi.

Pendeteksian Watermark

Misalkan sinyal yang diterima adalah *Y**, yaitu sinyal *Y* yang telah mengandung derau *n*,

$$Y^* = Y + n = (X + ag_s Gu + n) \qquad (21)$$

Pendeteksian *watermark* dilakukan dengan menghitung korelasi antara *watermark* publik w_p dengan sinyal yang diterima, *Y**, dan membandingkan nilai korelasi tersebut dengan nilai ambang *t* untuk menentukan apakah *watermark* terdapat di dalam sinyal yang diterima. Pendeteksian juga dapat dilakukan secara *watermark* publik w_s dengan sinyal yang diterima, *Y**.

Keamanan sistem TKW berdasarkan pada apakah *Gu* dapat dihitung dari $G^{-t}u$ (yang tidak dirahasiakan). Jika *Gu* berhasil dihitung, maka *watermark* privat dapat ditentukan dengan persamaan (18), yang pada akhirnya *watermark* dapat dihapus dari sinyal ber-*watermark*. Perhatikanlah bahwa $Gu = GG^t (G^{-t}u)$, tetapi faktanya tidak mungkin menemukan GG^t hanya dari $G^t u$ saja.

5. KESIMPULAN

Makalah ini sudah mempresentasikan konsep *asymmetric watermarking* berbasiskan uji korelasi. Kunci privat adalah *watermark* rahasia, sedangkan kunci publik adalah *watermark* yang berkorelasi dengan *watermark* privat. Secara komputasi, pengetahuan mengenai kunci publik tidak memungkinkan pihak lawan menurunkan *watermark* privat. Berdasarkan paparan yang sudah diuraikan di atas, maka kita dapat membangun skema *asymmetric watermarking* dengan tingkat keamanan yang lebih baik.

REFERENSI

[1] I. Wiseto P. Agung, *Watermarking and Content Protection for Digital Images and Video*, thesis of PhD in University of Surrey, 2002.

[2] Saraju P. Mohanty, "*Digital Watermarking: A Tutorial Review*", Dept. of Computer Scieence and Engineering, University of South Florida.

[3] Bruce Schneier, *Aplied Cryptography 2nd*, John Wiley & Sons, 1996.

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

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

[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] Tedy Furon and Pierre Duhanel, *An Asymmetric Public Detection Watermarking Technique*, Proceeding of 3rd Int. Work. On Information Hiding, Dresden, Sept. 1999.

[8] Tedy Furon and Pierre Duhanel, *An Asymmetric Watermarking Method*, IEEE Trans. Signal Processing, Vol. 51, no.4, pp.981-995, April 2003.
[9] Peter Meerwald, *Digital Image Watermarking in the Wavelet Transform Domain*, thesis diploma in University of Salzburg, 2001.
[10] Guo-fu Gui, Liang-ge Jiang, *A New Asymmetric Watermarking Scheme for Copyright Protection*, IEICE Trans. Fundamentals, Vol. E89-A, No. 2 February 2006.
[11] Guo-fu Gui, Liang-ge Jiang, *A Robust Asymmetric Watermarking Schme Using Multiple Public Watermarks*, IEICE Trans. Fundamentals, Vol. E88-A, No. 7 Juli 2005.
[12] Joachim J. Eggers, Jonathan K. Su, and Bernd Girod, *Asymmetric Watermarking Schemes*, GMD Jahrestagung, Proceddings, Springer-Verlag, 2000.
[13] Yong-gang Fu, Rui –Min Shen, Li-Ping Shen, *A Novel Asymmetric Watermarking Scheme*, Proc. Of 3rd Int. Conf. on Machine Learning and Cybernetics, 2004.
[14] H. Choi, K. Lee, dan T. Kim, *Transformed-Key Asymmetric Watermarking System*, IEEE Signal Processing Letters, Vol. 11. No. 2, February 2004.
[15] Scott Craver dan Stefan Katzenbeisser, *Security Analysis of Public-Key Watermarking Schemes*, 2000.