PENURUNAN ALGORITMA *SYMMETRIC WATERMARKING* MENJADI ALGORITMA *ASYMMETRIC WATERMARKING* STUDI KASUS: ALGORITMA BARNI

Rinaldi Munir, Bambang Riyanto, Sarwono Sutikno, Wiseto P. Agung

Sekolah Teknik Elektro dan Informatika ITB

E-mail: rinaldi@informatika.org

Abstrak

Di dalam makalah ini disajikan metode asymmetric watermarking *yang diturunkan dari versi simetri Algoritma Barni. Perbedaan antara Algoritma Barni dan versi asimetrinya terletak pada watermark yang digunakan pada proses deteksi yang disebut watermark publik. Watermark publik berkorelasi dengan watermark privat yang disisipkan ke dalam watermark. Pendeteksian watermark di dalam citra dilakukan dengan uji korelasi antara watermark publik dengan citra yang diuji. Hasil eksperimen menunjukkan bahwa versi asimetri dari Algoritma Barni mempunyai kinerja (*imperceptibility *dan* robustness*) yang tidak berbeda jauh dengan versi simetrinya.*

Kata Kunci*: asymmetric watermarking, Algoritma Barni, simetri, asimetri, korelasi.*

1. PENDAHULUAN

Digital image watermarking merupakan teknik yang digunakan untuk mengontrol penggandaan dan distribusi citra digital dengan cara menyisipkan informasi pemilik *copyright* yang dinamakan *watermark* [1]. Penyisipan *watermark* dilakukan sedemikian rupa sehingga tidak dapat dipersepsi oleh mata manusia (*imperceptible*). *Watermark* juga harus kokoh (*robust*) terhadap serangan yang bertujuan merusak atau menghapus *watermark* dari citra digital.

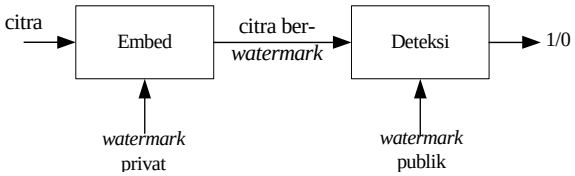
Dua proses utama di dalam skema *watermarking* adalah penyisipan *watermark* dan pendeteksian *watermark*. Skema *watermarking* yang sudah ada umumnya simetri, yakni kunci (atau *watermark*) yang digunakan pada proses dan penyisipan dan pendeteksian adalah sama dan hanya pemillik *copyright* yang dapat melakukan kedua proses tersebut. Pendeteksian *watermark* tidak bersifat publik, karena siapapun yang mengetahui kunci tersebut tidak hanya dapat mendeteksi *watermark* tetapi ia juga dapat menghapus *watermark* dari citra digital dengan cara pengurangan [2].

Di sisi lain, beberapa aplikasi mensyaratkan pendeteksian *watermark* dapat dilakukan oleh siapapun namun tanpa kemungkinan dapat menghapusnya.

Solusi masalah di atas adalah dengan menggunakan skema *asymmetric watermarking* (mirip dengan *asymmetric cryptography*). Pada skema ini, *watermark* yang digunakan pada proses penyisipan dan pendeteksian berbeda. *Asymmetric watermarking* sering disebut juga *public-key watermarking* karena *watermark* yang digunakan untuk pendeteksian dipublikasikan sehingga dinamakan *watermark* publik, sedangkan *watermark* yang disisipkan ke dalam citra hanya diketahui oleh pemilik *copyright* saja sehingga dinamakan *watermark* privat. Skema *asymmetric*

watermarking dilakukan dengan suatu cara sedemikian sehingga: (a) secara komputasi tidak mungkin menghitung *watermark* privat dari watermark publik, dan (b) kunci publik tidak dapat digunakan oleh penyerang untuk menghapus *watermark* [3].

Review beberapa metode *asymmetric watermarking* awal dapat ditemukan di dalam [4]. Metode yang lebih baru dapat ditemukan di dalam [6-10]. Secara umum, di dalam metode *asymmetric watermarking* tersebut pendeteksian direalisasikan dengan uji korelasi antara *watermark* publik dengan citra yang diuji [6]. Hasil pendeteksian adalah keputusan biner (1/0) yang mengindikasikan apakah citra tersebut mengandung *watermark* (1) atau tidak (0). Gambar 1 memperlihatkan skema umum *asymmetric watermarking.*



Gambar 1. Skema umum *asymmetric watermarking*

Di dalam skema *asymmetric watemmarking*, *watermark* publik memiliki korelasi dengan *watermark* privatnya. Hal ini penting agar proses pendeteksian dapat dilakukan dengan menggunakan *watermark* publik tersebut, karena yang disisipkan ke dalam citra adalah *watermark* privat. Makalah di dalam [6-10] menggambarkan kondisi ini. Misalnya di dalam [9], *watermark* publik diperoleh dengan melakukan permutasi terhadap *watermark* privat.

Mendesain sebuah metode *asymmetric watermarking* baru mungkin memerlukan usaha dan waktu yang lama. Karena itu, timbul ide untuk mentransformasikan sebuah metode *symmetric watermarking* menjadi versi *asymmetric*-nya. Metode simetri yang dipilih haruslah metode yang yang sudah terbukti memenuhi dua persyaratan dasar sistem *watermarking* yaitu *imperceptibility* dan *robustness*. Di dalam makalah ini metode simetri yang dipilih adalah algoritma *watermarking* yang terdapat di dalam [5], yang selanjutnya disebut Algoritma Barni. Algoritma Barni diturunkan menjadi versi *asymmetric*-nya, namun tetap memenuhi *imperceptibility* dan *robustness* yang tidak jauh berbeda dengan versi simetrinya. Serangkaian eksperimen dilakukan untuk mengukur *imperceptibility* dan *robustness* metode asimetri.

2. ALGORITMA BARNI

Watermark yang disisipkan ke dalam citra juga berlaku sekaligus sebagi kunci *watermarking*. *Watermark* ini harus dijaga kerahasiaannya. *Watermark* adalah barisan nilai riil yang berdistribusi normal $N(0, 1)$ (rata-rata = 0 dan variansi = 1) dengan panjang n:

$$\mathbf{w} = (w(1), w(2), ..., w(n))$$

Algoritma Barni melakukan penyisipan dan pendeteksian *watermark* dalam ranah *DCT* (*Discrete Cosine Transform*). Dalam hal ini, citra ditransformasikan ke dalam ranah *DCT*, lalu sejumlah koefisien yang dipilih pada bagian *middle frequency* diekstraksi sebanyak n buah. Misalkan koefisien *DCT* terpilih itu adalah:

$$\mathbf{f} = (f(1), f(2), ..., f(n))$$

Watermark **w** disisipkan pada **f** ini. Rincian algoritma penyisipan dan pendeteksian *watermark* adalah sebagai berikut:

2.1 Penyisipan *Watermark*

Langkah-langkah penyisipan *watermark* adalah sebagai berikut:

(i) Citra I yang berukuran N x M ditransformasi dengan *DCT*.

(ii) Semua koefisien *DCT* diurutkan secara *zig-zag.*

(iii) Pilih koefisien *DCT* pada bagian *middle frequency* dengan cara mengambil koefisien *DCT* hasil pengurutan zig-zag dari koefisien *L* + 1 sampai koefisien *L* + *n*. Misalkan koefisien-koefisien *DCT* yang terpilih ini disimpan di dalam larik **f**.

(iv) Sisipkan *watermark* **w** ke dalam **f** dengan menggunakan persamaan:

$$f_w(i) = f(i) + \alpha \mid f(i) \mid w(i) \quad (1)$$

yang dalam hal ini α adalah faktor kekuatan *watermark* ($0 < \alpha < 1$) yang dipilih sedemikian rupa sehingga *watermark* tidak dapat dipersepsi secara visual namun masih dapat dideteksi.

(v) Letakkan kembali semua koefisien DCT yang baru ($\mathbf{f_w}$) pada posisi semula, lalu terapkan transformasi *DCT* balikan (*IDCT*) untuk mendapatkan citra ber-*watermark*.

2.2 Pendeteksian *Watermark*

Pendeteksian *watermark* tidak membutuhkan citra asal, tetapi hanya membutuhkan *watermark* semula. Hasil pendeteksian ada dua kemungkinan: citra yang diuji mengandung *watermark* **w** atau citra tidak mengandung *watermark* **w**.

Langkah-langkah pendeteksian *watermark* adalah sebagai berikut:

(i) Transformasikan citra uji dengan *DCT*.

(ii) Semua koefisien *DCT* diurutkan secara *zig-zag.*

(iii) Pilih koefisien *DCT* pada bagian *middle frequency* dengan cara mengambil koefisien *DCT* hasil pengurutan zig-zag dari koefisien *L* + 1 sampai koefisien *L* + *n*. Misalkan koefisien-koefisien *DCT* yang terpilih ini disimpan di dalam larik **f***.

(iv) Hitung korelasi antara **f*** dan *watermak* **w** dengan persamaan:

$$c = \frac{1}{M} \sum_{i=i}^{M} f^*(i) \cdot w(i) \quad (2)$$

(iv) Bandingkan *c* dengan nilai-ambang *T* untuk menentukan apakah *watermark* **w** terdapat di dalam citra yang diuji.

Nilai-ambang *T* yang disarankan oleh Barni bergantung pada koefisien *DCT* citra yang diuji dan secara matemastis dihitung dengan persamaan berikut:

$$T = \frac{\alpha}{3n} \sum_{i=i}^{n} \left| f^*(i) \right| \quad (3)$$

Citra mengandung *watermark* jika $c \geq T$, sebaliknya jika $c < T$ maka citra tidak mengandung *watermark*.

3. VERSI *ASYMMETRIC* DARI ALGORITMA BARNI

Perbedaan versi simetri dan asimetri dari algoritma Barni terletak pada *watermark* yang digunakan pada proses pendeteksian. *Watermark* yang disisipkan adalah *watermark* privat, sedangkan *watermark* yang dikorelasikan pada saat pendeteksian adalah *watermark* publik. *Watermark* publik diperoleh dengan menjumlahkan *watermark* privat dengan sebuah barisan acak yang aman. Barisan acak aman yang digunakan di sini adalah barisan *chaos*. *Chaos* diterapkan karena ia mempunyai karakteristik penting untuk meningkatkan keamanan, yaitu sensitivitas pada kondisi awal. Karakteristik ini cocok untuk enkripsi dan *watermarking* [11].

Fungsi *chaos* yang digunakan adalah persamaan logistik (*logistic map*) yang berbentuk:

$$x_{i+1} = r\, x_i\, (1 - x_i) \quad (4)$$

dengan x_0 sebagai nilai awal iterasi ($0 \leq r \leq 4$). Dengan melakukan iterasi persamaan (4) dari nilai awal x_0 tertentu, kita memperoleh barisan nilai-nilai *chaos*. Nilai-nilai *chaos* tersebut teletak di antara 0 dan 1 dan tersebar secara merata serta tidak ada dua nilai yang sama.

3.1 Pembangkitan *Watermark* Privat dan Publik

Langkah-langkah pembangkitan *watermark* privat dan *watermark* publik adalah sebagai berikut:

(i) Bangkitkan *watermark* privat $\mathbf{w_s}$ berdasarkan distribusi *N*(0, 1):

$\mathbf{w_s} = (w_s(1), w_s(2), ..., w_s(n))$

(ii) Bangkitkan barisan *chaos* (rahasia) dengan nilai awal tertentu:

$\mathbf{k} = (k(1), k(2), ..., k(n))$

(iii) Jumlahkan barisan *chaos* dengan *watermark* privat untuk menghasilkan *watermark* publik $\mathbf{w_p}$:

$\mathbf{w_p} = (w_p(1), w_p(2), ..., w_p(n))$

yang dalam hal ini

$$w_p(i) = k(i) + \cdot\, w_s(i),\ i = 1, 2, ..., n \qquad (5)$$

3.2 Penyisipan *Watermark*

Tidak ada perubahan pada proses penyisipan *watermark*, hanya saja notasi *watermark* yang disisipkan adalah *watermark* privat $\mathbf{w_s}$:

$$f_w(i) = f(i) + \alpha \,|\, f(i) \,|\, w_s(i) \qquad (6)$$

3.3 Pendeteksian *Watermark*

Uji korelasi tidak membutuhkan *watermark* privat, tetapi mengunakan *watermark* publik yang berkorelasi dengan *watermark* privat yang disisipkan ke dalam citra.

Pendeteksian dilakukan dengan menghitung korelasi antara **f*** dan *watermak* publik $\mathbf{w_p}$:

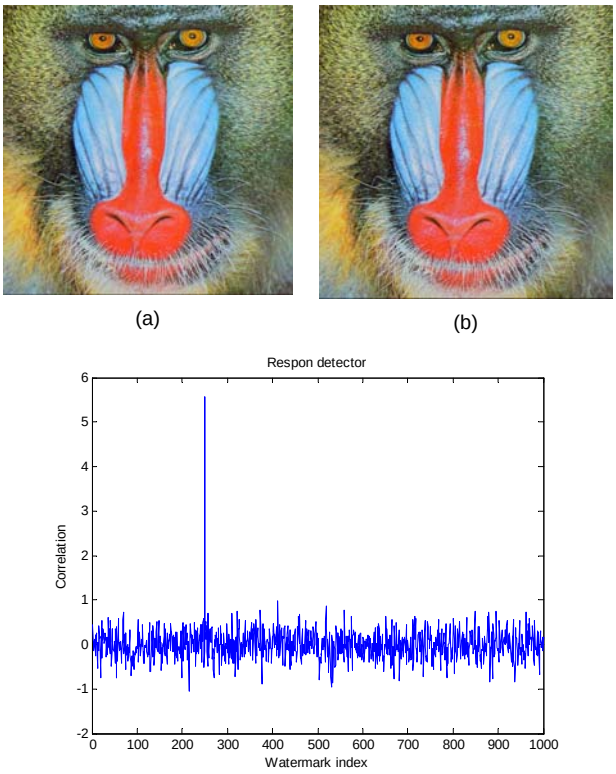
$$c = \frac{1}{M}\sum_{i=i}^{M} f^*(i)\cdot w_p(i) \qquad (7)$$

lalu membandingkan nilai *c* dengan nilai-ambang *T* untuk menentukan apakah citra mengandung watermark $\mathbf{w_s}$ atau tidak. Nilai *T* "dihampiri" dengan persamaan (3).

4. EKSPERIMEN DAN HASIL

Algoritma Barni versi simetri dan asimetri diimplementasikan dengan menggunakan kakas MATLAB 7. Citra yang diberi *watermark* adalah citra berwarna dengan kedalaman 24-bit. Sebelum disisipi *watermark*, citra berwarna dalam ruang *RGB* ditransformasikan terlebih dahulu ke ruang warna *YCrBr*. *Watermark* disisipkan pada komponen *luminance* (*Y*) saja, lalu hasilnya ditransformasikan kembali ke ruang warna *RGB*.

Citra yang diuji adalah '*baboon*' (512 x 512). *Watermark* privat berukuran *n* = 10000 dan berdistribusi normal N(0, 1). *Watermark* publik berukuran sama dengan *watermark* privat. Nilai *L* = 10000, α = 0.2., dan x_0 = 0.65 (x_0 harus rahasia).



Gambar 2. (a) Citra *baboon* asli, (b) citra *baboon* yang sudah ber-*watermark* (*PSNR* = 36.2736).

Gambar 2(a) memperlihatkan citra *baboon* semula dan Gambar 2(b) memperlihatkan citra *baboon* yang sudah ber-*watermark*. Gambar 2(c) memperlihatkan respon detektor terhadap 1000 *watermark* publik acak yang dikaji, tetapi hanya satu *watermark* publik yang berkorelasi dengan *watermark* privat yang secara signifikan memiliki

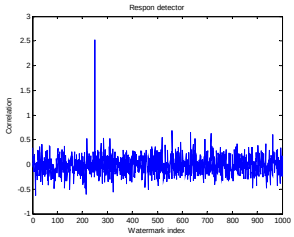
korelasi lebih tinggi dari yang lain. Nilai ambang *T* yang dihitung dari persamaan (3) adalah 1.9361 Pada kasus tidak ada serangan, detektor memberikan nilai *c* = 5.8747. Nilai *c* ini lebih besar dari *T* yang artinya citra yang diuji mengandung *watermark* privat.

Eksperimen selanjutnya dilakukan untuk melihat kekokohan *watermark* terhadap berbagai serangan *non-malicious attack*, yaitu operasi tipikal yang umum dilakukan pada pengolahan citra (*cropping*, kompresi, dll). Program pengolahan citra yang digunakan adalah *Jasc Paintshop Pro*.

Eksperimen 1: Pemotongan (*cropping*)

Citra ber-*watermark* dipotong dengan mengambil bagian tertentu saja, sementara bagian yang ditinggalkan diisi dengan *pixel-pixel* hitam. Percobaan menunjukkan *watermark* masih dapat dideteksi dari citra ber-*watermark* (*c* > *T*). Lihat Gambar 3.

(a) *Cropping*



c = 2.8045, *T* = 1.2422

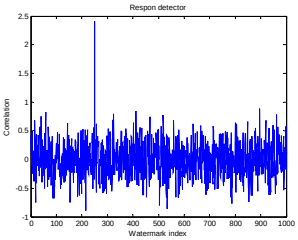
(b)

Gambar 3. (a) Citra baboon yang sudah dipotong (b) Respon detektor. Hasil: *c* > *T*

Eksperimen 2: Kompresi JPEG

Citra ber-*watermark* dikompresi ke format *JPEG* dengan kualitas kompresi ekstrim 5%. Hasil pengujian menunjukkan bahwa *watermark* tetap dapat dideteksi dari citra hasil kompresi (Gambar 4).

(a) Kualitas kompresi 5%



c = 2.7915, *T* = 1.9444

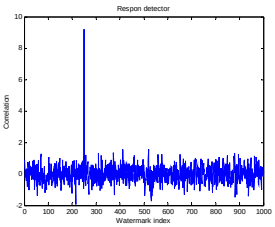
(b)

Gambar 4. (a) Kompresi ke format JPEG dengan kualitas 5%. (b) *Watermark* masih dapat dideteksi.

Eksperimen 3: Perataan Histogram

Citra ber-*watermark* diperbaiki sebaran warnanya sehingga terdistribusi secara merata dengan perataan histogram. Hasil percobaan menunjukkan *watermark* dapat dideteksi, bahkan nilai korelasi *c* jauh lebih besar dari nilai-ambang *T* (Gambar 5).

(a) Perataan histogram



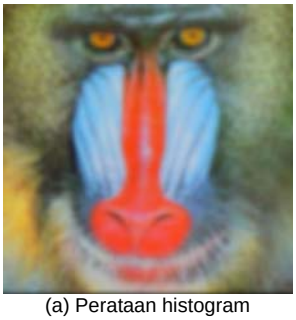
c = 9.6541, *T* = 3.3589

(b)

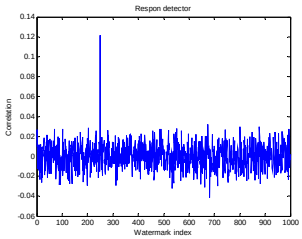
Gambar 5. (a) Perataan histogram. (b) *Watermark* dapat dideteksi.

Eksperimen 4: *Gaussian Blur*

Citra ber-*watermark* dibuat menjadi kabur (*blur*) dengan efek *Gaussian blur*. *Watermark* tetap masih dapat dideteksi (Gambar 6).



(a) Perataan histogram



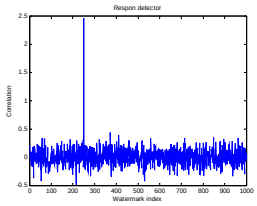
c = 0.1491, *T* = 0.0555

(b)

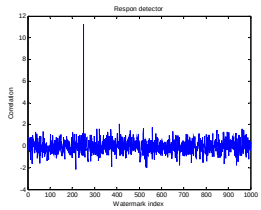
Gambar 6. (a) *Gaussian blur* (b) *Watermark* tetap dapat dideteksi.

Eksperimen 5: Pengubahan ukuran gambar

Citra ber-*watermark* diperkecil ukurannya hingga 50%. Percobaan menunjukkan bahwa *watermark* masih dapat dideteksi. Untuk perbesaran hingga 2 kali ukuran semula, *watermark* juga masih dapat dideteksi (Gambar 7).



c = 2.5944, *T* = 0.8722
(a) Pengecilan 50%



c = 11.7525, *T* = 4.0361
(b) Perbesaran 200%

Gambar 7. (a) Pengecilan 50%, (b) Perbesaran 200%. *Watermark* masih dapat dideteksi.

5. KESIMPULAN

Di dalam makalah ini telah dipresentasikan metode *asymmetric watermarking* yang diturunkan dari Algoritma Barni (simetri). *Watermark* publik berkorelasi dengan *watermark* privat yang disisipkan ke dalam *watermark*. *Watermark* publik diperoleh dengan menjumlahkan *watermark* privat dengan barisan *chaos*. Dibandingkan dengan hasil-hasil yang dicapai di dalam [5], hasil eksperimen menunjukkan bahwa metode ini memiliki *imperceptibility* dan *robustness* yang tidak jauh berbeda dengan versi simetrinya.

6. DAFTAR PUSTAKA

[1] Ingemar J. Cox, dkk, "*Secure Spread Spectrum Watermarking for Multimedia*", IEEE Trans. On Image Processing, Vol. 6, No. 12, Dec 1997, pp.1673-1687.

[2] Frank Hartung, Bernd Girod, "*Fast Public-Key Watermarking of Compressed Video*", Proceedings of the 1997 International. Conference on Image Processing (ICIP), 1997.

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

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

[5] Mauro Barni, F. Bartolini, V. Cappellini, A.Piva, "*A DCT-Domain System for Robust Image Watermarking*", Signal Processing 66, pp 357-372, 1998.

[6] G.F Gui, L.G Jiang, C He, "*A Robust Asymmetric Watermarking Scheme Using Multiple Public Watermarks*" IECE Trans, Fundamentals Vol. E88-A, No 7 July 2005.

[7] G.F Gui, L.G Jiang, C He, *General Construction of Asymmetric Watermarking Based on Permutation*, Proc. IEEE Int. Workshop VLSI Design & Video Tech., May 28, 2005.

[8] G.F Gui, L.G Jiang, C He, "*A New Asymmetric Watermarking Scheme for Copyright Protection*" IECE Trans, Fundamentals Vol. E89-A, No 2 February 2006.

[9] Y.G Fu, R.M, Shen, L.P Shen, "*A Novel Asymmetric Watermarking Scheme*", Proc. Of the 3rd Int. Conf. on Machone Learning and Cybernetics, Shanghai, 26-29 August 2004.

[10] H. Choi, K. Lee, dan T. Kim, *Transformed-Key Asymmetric Watermarking System*, IEEE Signal Processing Letters, Vol. 11. No. 2, February 2004.

[11] Zhao Dawei, dkk, "*A Chaos-Based Robust Wavelet-Dmain Watermarking Algorithm*", Jurnal Chaos Solitons and Fractals 22 (2004) 47-54.

[11] Hongxia Wang, dkk, "*Public Watermarking Based on Chaotic Map*", IEICE Trans. Fundamentals, Vol. E87-A, No. August 2004.

[12] Sangoh Jeong dan Kihyun Hong, *Dual Detection of A Watermark Embedded in the DCT Domain*, EE368A Project Report, 2001.