Image Watermarking untuk Citra Berwarna dengan Metode Berbasis Korelasi dalam Ranah *DCT*

Rinaldi Munir
Program Studi Teknik Informatika ITB
Sekolah Teknik Elektro dan Informatika ITB, Jl. Ganesha 10 Bandung
E-mail: rinaldi@informatika.org

Abstract

This paper presents digital watermarking method for color images by using a method based on correlation in DCT (Discrete Cosine Transform) domain. At first, the color images in RGB model is transformed into YCbCr model. A watermark is embedded into Y component, then the result is transformed back into RGB model. The watermark is a sequence whose length is N and it has a normal distribution. The watermark is embedded into sub-band middle frequency of the selected DCT coefficients of Y component to get balance between robustness and imperceptibility. Watermark detection is established by computing correlation between the received image and original watermark, then its correlation value is compared by a specified threshold. Output of detection process is a binary decision that states that the received image contains the watermark or not. Experiment results show that quality of watermarked image is similar with the original image and this method is proved robust to non-malicious attacks like JPEG compression, histogram equalization, gamma correction, cropping, resizing, noising, sharpening.

***Keywords**: digital watermarking, color images, DCT, correlation, robust.*

Abstraksi

Makalah ini memaparkan metode *digital watermarking* pada citra berwarna dengan sebuah metode berbasis korelasi dalam ranah *Discrete Cosine Transform* (*DCT*). Citra berwarna dalam ruang warna *RGB* terlebih dahulu ditransformasikan ke dalam ruang warna YCbCr. *Watermark* disisipkan pada komponen *Y*, lalu hasilnya ditranformasikan kembali ke ruang warna *RGB*. *Watermark* adalah barisan riil sepanjang *N* elemen dan berdistribusi normal. *Watermark* disisipkan pada koefisien *DCT* yang dipilih dari *sub-band middle frequency* untuk mendapatkan keseimbangan antara *robustness* dan *imperceptibility*. Pendeteksian *watermark* dilakukan dengan menghitung korelasi antara citra yang diterima dengan *watermark* semula, kemudian membandingkannya dengan sebuah nilai-ambang. Hasil pengujian adalah keputusan biner yang menyatakan citra mengandung *watermark* atau tidak mengandung *watermark*. Hasil eksperimen menunjukkan bahwa kualitas citra ber-*watermark* tidak dapat dibedakan dengan citra aslinya dan metode ini terbukti *robust* terhadap beberapa serangan *non-malicious attack* seperti kompresi JPEG, *histogram equalization*, *gamma correction*, *cropping*, *resizing*, *noising*, *sharpening*.

***Kata Kunci**: digital watermarking, citra berwarna, DCT, korelasi, robust.*

A. PENDAHULUAN

Saat ini kebanyakan data multimedia disajikan dalam format digital, baik berupa data citra, audio, maupun video. Perkembangan teknologi kompresi seperti *JPEG*, *MP3*, dan *MPEG* memungkinkan penggunaan secara luas aplikasi multimedia. Citra digital adalah salah satu data digital yang paling paling banyak digunakan di dalam aplikasi multimedia. Citra digital, sebagaimana halnya dengan data digital lainnya, mempunyai beberapa karakteristik yang juga menjadi kelemahannya, antara lain: (1) Penggandaan (*copy*) terhadap citra digital mudah dilakukan dan hasilnya tepat sama dengan aslinya; (2) Citra digital mudah didistribusikan melalui *magnetic disk* maupun melalui internet; (3) Perubahan yang sedikit pada citra digital tidak mudah dipersepsi secara inderawi.

Masalah yang muncul dari distribusi dan penggandaan ilegal adalah pelanggaran hak kepemilikan (*ownership*). Masalah ini dapat diatasi dengan menggunakan *digital watermarking* [1-4]. *Digital watermarking* adalah teknik untuk menyisipkan informasi yang menyatakan label kepemilikan (yang disebut *watermark*) ke dalam citra. *Watermark* dapat berupa informasi apapun seperti teks yang menyatakan informasi *copyright*, gambar bermakna seperti logo, data biner, atau data acak. *Watermark* tersebut berlaku sebagai *signature* pemilik data multimedia yang memperingatkan kepada publik bahwa data multimedia tersebut adalah propertinya. Karena itu *watermarking* merupakan cara untuk menyediakan proteksi *copyright* atas produk multimedia.

Persyaratan utama *digital watermarking* adalah [2]: 1) *imperceptibility*: *watermark* yang disisipkan ke dalam citra tidak dapat dipersepsi oleh manusia; 2) *robustness*: *watermark* harus tahan terhadap berbagai serangani yang dilakukan pada citra ber-*watermark* yang mungkin dapat merusak atau menghapus *watermark*. Ini berarti manipulasi yang dilakukan terhadap citra ber-*watermark* masih

memungkinkan *watermark* dapat dideteksi. Manipulasi terhadap citra meliputi operasi seperti penambahan derau aditif (Gaussian atau *non-Gaussian*), kompresi (seperti *JPEG*), transformasi geometri (seperti rotasi, perbesaran, perkecilan), penapisan (baik penapisan lanjar maupun nirlanjar, konversi digital-ke-analog (*D*/*A*) atau *A*/*D*, seperti pemindaian citra; 3) *security*: *watermark* hanya dapat diakses oleh pihak yang mempunyai otoritas.

Dua proses utama di dalam skema *watermarking* adalah penyisipan *watermark* dan pendeteksian *watermark*, yang di dalam prosesnya menggunakan kunci rahasia agar persyaratan *security* dipenuhi. Sejumlah skema *watermarking* sudah banyak dipublikasikan dalam beberapa tahun terakhir. Kebanyakan riset *watermarking* diujicobakan pada citra *greyscale* dan relatif sedikit yang menerapkannya pada citra berwarna. Citra berwarna lebih banyak digunakan di dalam aplikasi multimedia daripada citra *greysacle*. Makalah ini mencoba menerapkan metode watermarking yang diusulkan oleh Barni dkk di dalam [5] yang selanjutnya dinamakan Algoritma Barni. Algoritma Barni adalah sebuah metode *image watermarking* yang berbasis korelasi dan penyisipan serta pendeteksian *watermark* dilakukan dalam ranah *discrete cosine transform* (*DCT*). Serangkaian eksperimen dilakukan untuk mengukur kualitas citra ber-*watermark* dan kekokohannya terhadap operasi pengolahan citra tipikal.

B. DASAR TEORI

Di dalam bagian ini dipaparkan konsep *digital watermarking*, transformasi *discrete cosine transform* (*DCT*), dan *watermarking* dalam ranah *transform*.

B.1 *Digital Watermarking*

Teknik *watermarking* pada citra secara umum terdiri dari 2 tahapan: 1) penyisipan *watermark* (*watermark embedding*), dan 2) deteksi atau ekstraksi *watermark* (*watermark detection/extraction*). Citra ber-*watermark* kemudian didstribusikan – misalnya dipublikasikan di dalam web atau dijual ke pelanggan. Selama transmisi dan distribusi, citra ber-*watermark* mengalami distorsi karena pemrosesan citra yang umum, seperti kompresi, perbaikan kontras, pengubahan ukuran, *re-sampling*, *gamma corection*, dan sebagainya. Semua distorsi yang dikenakan kepada citra ber-*watermark* dipandang sebagai serangan. Setiap serangan memberikan kontribusi *noise* (*n*) pada citra dan dapat mengganggu proses pendeteksian. Metode *watermarking* yang bagus harus kokoh (*robust*) terhadap serangan yang dapat merusak atau menghancurkan *watermark* di dalam citra.

Penyisipan dan pendeteksian/ekstraksi *watermark* melibatkan penggunaan kunci. Kunci bisa menyatakan lokasi yang menspesifikasikan penyisipan *watermark*, menyatakan barisan nilai yang dimodulasi dengan *watermark*, atau menyatakan kunci enkripsi sebab pada beberapa metode *watermarking*, *watermark* dienkripsi terlebih dahulu sebelum disisipkan ke dalam citra. Contoh kunci misalnya umpan (*seed*) yang digunakan di dalam pembangkit bilangan acak. Pada beberapa metode, *watermark* juga berlaku sebagai kunci itu sendiri [1, 5], yang mengimplikasikan *watermark* adalah informasi rahasia.

Watermark yang disisipkan ke dalam citra dapat dalam berbagai bentuk, misalnya teks, gambar hitam-putih atau logo, audio, data biner (+1/-1), barisan bilangan riil, dan sebagainya.

B.2. *Image Watermarking* dalam Ranah *DCT*

Menyisipkan dan mendeteksi *watermark* dalam ranah frekuensi, menghasilkan *robustness* yang lebih tinggi bila dibandingkan dengan ranah spasial. Selain itu *watermarking* dalam ranah frekuensi kompatibel dengan standard kompresi citra seperti *JPEG*. Kompatibalitas tersebut menjamin bahwa metode *watermarking* dalam ranah frekuensi memiliki kinerja yang baik bila citra ber-*watermark* mengalami kompresi *lossy*, yang merupakan operasi pengolahan citra yang paling umum.

Kakas transformasi dari ranah spasial ke ranah frekuensi yang umum digunakan misalnya *DFT* (*Discrete Fourier Transform*), *DCT* (*Discrete Cosine Transform*), dan *DWT* (*Discrete Wavelet Transform*), dan sebagainya. Makalah ini menggunakan *DCT* sebagai kakas transformasi.

Untuk sinyal dua dimensi seperti citra digital, *DCT* dua dimensi terhadap matriks I yang berukuran $M \times N$ didefinisikan sebagai berikut:

$$C(p,q) = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} I(m,n) \cos \frac{\pi 2(m+1)p}{2M} \cos \frac{\pi (2n+1)q}{2N} \quad \text{.....(1)}$$

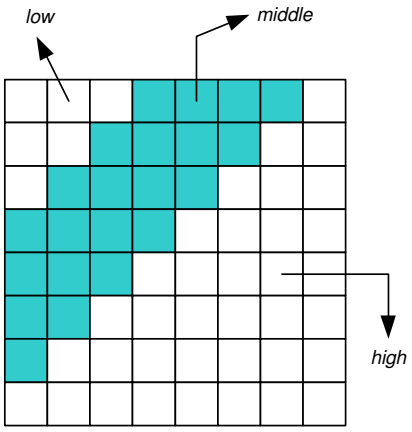
Nilai-nilai $C(p, q)$ dinamakan *koefisien DCT* dari citra ***I.*** Tranformasi *DCT* balikan dinyatakan dengan persamaan

$$I(m,n) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \alpha_p \alpha_q C(p,q) \cos \frac{\pi 2(m+1)p}{2M} \cos \frac{\pi (2n+1)q}{2N} \quad \text{.....(2)}$$

dimana

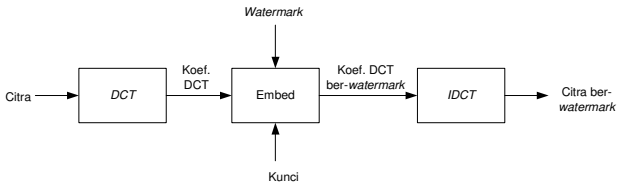
$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}} & , p = 0 \\ \sqrt{\frac{2}{M}} & , 1 \le p \le M-1 \end{cases} \qquad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}} & , q = 0 \\ \sqrt{\frac{2}{N}} & , 1 \le q \le N-1 \end{cases}$$

Ranah *DCT* membagi citra ke dalam tiga *sub-band* frekuensi (*low*, *middle*, dan *high*), lihat Gambar 1. Penyisipan pada bagian *low frequency* dapat merusak citra karena mata manusia lebih peka pada frekuensi yang lebih rendah daripada frekuensi lebih tinggi. Sebaliknya bila *watermark* disisipkan pada bagian *high frequency*, maka *watermark* tersebut dapat terhapus oleh operasi kuantisasi seperti pada kompresi *lossy* (misalnya *JPEG*). Oleh karena itu, untuk menyeimbangkan antara *robustness* dan *imperceptibility*, maka *watermark* disisipkan pada bagian *middle frequency* (bagian yang diarsir pada Gambar 1).



Gambar 1. Pembagian tiga kanal frekuensi pada ranah *DCT*

Gambar 2 memperlihatkan diagram penyisipan watermark dalam ranah *DCT*. Mula-mula citra ditransformasikan dengan *DCT*, hasilnya adalah koefisien-koefisien *DCT*. *Watermark* disisipkan pada koefisien *DCT* yang terpilih dengan menggunakan parameter kunci rahasia. Koefisien *DCT* yang sudah mengandung *watermark* ditempatkan pada posisi semula, lalu transfomasi balikan (*IDCT*) dilakukan pada keseluruhan koefisien DCT untuk memperoleh citra ber-*watermark* (dalam ranah spasial).



Gambar 2. Penyisipan *watermark* dalam ranah *DCT*

Watermark dapat diektsraksi atau hanya dideteksi keberadaanya di dalam citra bergantung pada natural algoritmanya (*blind* atau *non-blind*). Pada kasus *watermark* hanya dapat dideteksi keberadaannya (umumnya pada *blind-watermarking*), deteksi *watermark* dilakukan dengan uji korelasi antara koefisien *DCT* citra yang diterima dengan *watermark*. Misalkan **w** adalah *watermark* dan **v*** adalah koefisien *DCT* yang diterima, keduanya sepanjang *N*. Korelasi antara **w** dan **v*** dapat dihitung dengan *linear correlation*. *Linear correlation* biasa dipraktekkan di dalam komunikasi untuk menguji keberadaan sinyal transmisi **w** di dalam sinyal yang diterima, **v***, dengan menghitung korelasi keduanya melalui persamaan.

$$c = \frac{1}{N}\mathbf{w}\cdot\mathbf{v}^* = \frac{1}{N}\sum_{i=1}^{N} w_i\, v'_i \qquad \text{.....(3)}$$

Selanjutnya, c dibandingkan dengan sebuah nilai ambang T. Jika $c \geq T$, maka disimpulkan *watermark* **w** terdapat di dalam citra, sebaliknya **w** tidak terdapat di dalam citra.

C. Algoritma Barni

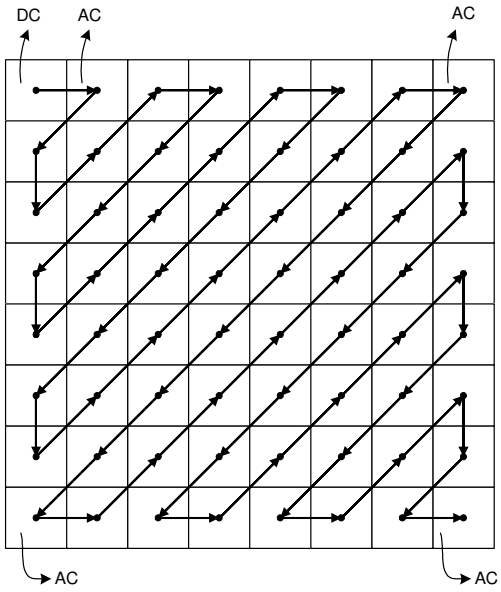
Salah satu metode *watermarking* yang mempunyai kinerja bagus adalah algoritma yang diusulkan oleh Mauro Barni, F. Bartolini, V. Cappellini, A.Piva, di dalam makalahnya yang berjudul "*A DCT-Domain System for Robust Image Watermarking*" [5]. Algoritma ini akan dijadikan dasar untuk pengembangan algoritma *asymmetric watermarking* yang merupakan tujuan penelitian ini.

Di dalam algoritma Barni, *watermark* yang disisipkan ke dalam citra juga berlaku sekaligus sebagi kunci *watermarking*. *Watermark* ini harus terjaga kerahasiaannya. *Watermark* adalah berupa barisan nilai riil yang berdistribusi normal $N(0, 1)$ (rata-rata = 0 dan variansi = 1) dengan panjang N, misalkan watermark dinyatakan sebagai **w** = ($w(1)$,$w(2)$, ..., $w(N)$).

Algoritma Barni melakukan penyisipan dan pendeteksian *watermark* dalam ranah *DCT* (*Discrete Cosine Transform*). Dalam hal ini, mula-mula citra ditransformasikan ke dalam ranah *DCT*, lalu *N* buah koefisien yang dipilih pada bagian *middle frequency* diekstraksi. Untuk mengekstraksi koefisien *DCT* pada bagian *middle frequency* ini, diperlukan pengurutan zig-zag sebagaimana pada algoritma kompresi *JPEG*. Pengurutan zig-zag menghasilkan sebuah vektor (*array* linier) yang menyatakan urutan koefisen *DCT* mulai dari *low* hingga *high frequency*.

Gambar 3 memperlihatkan alur pengurutan zig-zag pada matriks *DCT* berukuran 8×8, dimulai dari elemen pada sudut kiri atas matriks (disebut komponen *DC*), lalu bergerak searah panah menyusuri komponen-komponen *AC*, dan berakhir pada ujung kanan bawah matriks. Hasil pengurutan disimpan sebagai sebuah vektor linier. Untuk mengambil koefisien *DCT* pada bagian *middle frequency* dilakukan lompatan (*skip*) pada vektor linier sejauh *L* elemen, kemudian elemen dari $L + 1$ hingga $L + N$ diambil.

Misalkan koefisien *DCT* yang terpilih itu adalah **v** = ($v(1)$, $v(2)$, ..., $v(N)$). *Watermark W* sepanjang *N* disisipkan pada elemen-elemen **v** ini. Algoritma penyisipan dan pendeteksian *watermark* dijelaskan sesudah ini.



Gambar 3. Skema pengurutan secara zig-zag

C.1 Penyisipan *Watermark*

Langkah-langkah penyisipan *watermark* adalah sebagai berikut:

(i) Citra *I* 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 **v**.
(iv) Sisipkan *watermark* **w** ke dalam **v** dengan menggunakan persamaan:

$$v'(i) = v(i) + \alpha |v(i)| w(i) \qquad .....(4)$$

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 (**v'**) pada posisi semula, lalu terapkan transformasi *DCT* balikan (*IDCT*) untuk mendapatkan citra ber-*watermark*.

C.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 **v***.
(iv) Hitung korelasi antara **v*** dan *watermak* **w** dengan persamaan:

$$c = \frac{1}{N}\sum_{i=i}^{N} v^*(i) \cdot w(i) \qquad .....(5)$$

(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 analitis dihitung dengan persamaan berikut:

$$T = \frac{\alpha}{3N}\sum_{i=i}^{N} |v^*(i)| \qquad .....(6)$$

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

D. Pengujian *Robustness*

Untuk menguji *robustness* metode terhadap *non-malicious attack*, maka dilakukan pengujian pada dua buah citra. Citra yang diberi *watermark* adalah citra berwarna. Sebelum disisipkan *watermark*, warna dalam ruang *RGB* ditransformasikan ke dalam ruang warna *YCbCr*. *DCT* diterapkan pada komponen *luminance* (*Y*) saja, lalu setelah dilakukan penyisipan *watermark*, hasilnya ditransformasikan kembali ke ruang warna *RGB*.

Transformasi dari *RGB* ke *YCbCr* dihitung dengan rumus berikut:

$$Y = 0.299R + 0.587G + 0.114\,B \qquad .....(7)$$
$$Cb = -0.1687R - 0.3313G + 0.5B + 128 \qquad ....(8)$$
$$Cr = 0.5R - 0.4187G - 0.0813B + 128 \qquad .....(9)$$

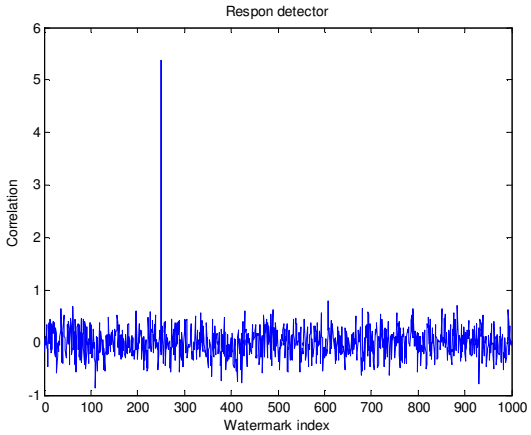
Sedangkan transformasi balikan dari *YCbCr* ke *RGB* dihitung dengan rumus berikut:

$$R = Y + 1.402\,(Cr - 128) \qquad ....(10)$$
$$G = Y - 0.34414(Cb - 128) - 0.71414(Cr - 128) \qquad ..(11)$$
$$B = Y + 1.772\,(Cb - 128) \qquad ...(12)$$

Citra uji yang digunakan adalah adalah citra 'fajar' yang berukuran 512 x 512 (Gambar 4a). *Watermark* berukuran *N* = 16000 dan berdistribusi normal N(0, 1). Nilai *L* = 16000. Gambar 4b memperlihatkan citra ber-*watermark* dengan PSNR = 37.1347. Secara visual citra ber-*watermark* tidak dapat dibedakan dengan citra aslinya. Gambar 4c memperlihatkan respon detektor terhadap 1000 *watermark* acak yang dikaji, tetapi hanya satu *watermark* yang berkorelasi dengan citra masukan. Pada kasus tidak ada serangan, detektor memberikan nilai *c* = 5.3745. Nilai ini jauh lebih lebih tinggi dari nilai-ambang *T* yang dihitung dengan persamaan (6) yaitu *T* = 1.7622, sehingga dapat disimpulkan citra yang diuji mengandung *watermark*.

(a) Citra asli

(b) Citra ber-*watermark*



(c) Respon detektor

Gambar 4 (a) Citra 'fajar' asli, (b) citra ber-*watermark*, (c) respon detektor

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*.

a. Kompresi *JPEG* (kompresi ekstrim hingga kualitas 5%)

Citra ber-*watermark* dikompresi ke format *JPEG* dengan kualitas kompresi ekstrim 5%. Hasil pengujian memberikan c = 1.9577 dan T = 1.6930. Karena $c > T$, maka disimpulkan *watermark* tetap berhasil dapat dideteksi (Gambar 5a).

b. *Cropping*

Citra ber-*watermark* dipotong dengan mengambil bagian tertentu saja, sementara bagian yang ditinggalkan diisi dengan *pixel-pixel* hitam. Hasil pengujian memberikan c = 2.9220 dan T = 1.3197. Karena $c > T$, maka disimpulkan *watermark* berhasil dideteksi (Gambar 5b).

c. *Histogram Equalization*

Citra ber-*watermark* diperbaiki sebaran warnanya sehingga terdistribusi secara merata dengan perataan histogram. Hasil pengujian memberikan c = 7.8483 dan T = 2.6606. Karena $c > T$, maka disimpulkan *watermark* tetap dapat dideteksi (Gambar 5c).

d. *Gamma Correction*

Citra ber-*watermark* diperbaiki kontrasnya dengan metode *gamma correction*. Hasill pengujian memberikan c = 4.5338 dan T = 1.3177. Karena $c > T$, maka disimpulkan *watermark* tetap dapat dideteksi (Gambar 5d).

(a) Kualitas kompresi 5%
c = 1.9577, T = 1.6930

(b) *Cropping* hingga 50%
c = 2.9220, T = 1.3197

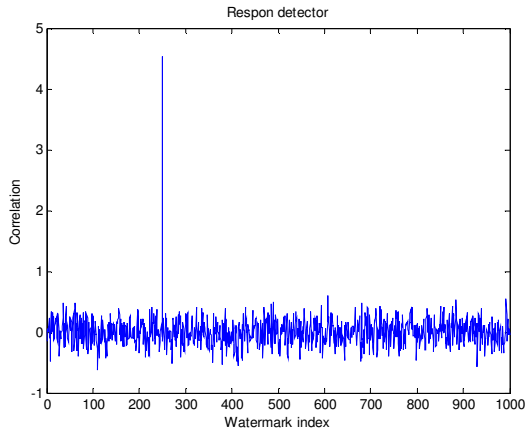
(c) *Histogram equalization*
c = 7.8483, T = 2.6606

(d) Gamma correction
c = 4.5338, T = 1.3177

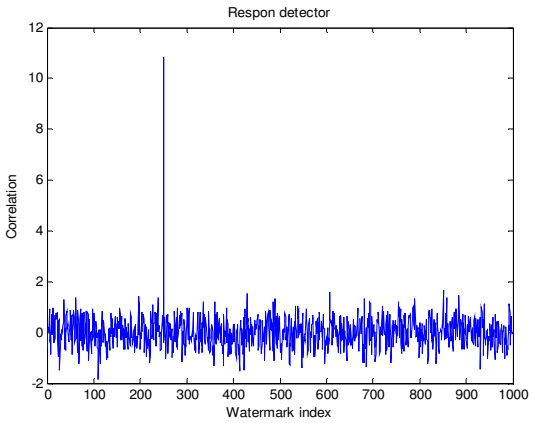
Gambar 5. Pengujian *robustness* dengan kompresi, *cropping*, *histogram equalization*, dan *gamma correction*

e. *Resize* 50% dan 200%

Citra ber-*watermark* diperkecil ukurannya hingga 50%. Percobaan menunjukkan bahwa *watermark* masih dapat dideteksi (Gambar 6a). Untuk perbesaran hingga 2 kali ukuran semula, *watermark* juga *masih* dapat dideteksi (Gambar 6b).



(a) *Resize* 50% ukuran semula
(c = 2.2249, T = 0.7898)



(b) *Resize* 200% ukuran semula
(c = 10.8523, T = 3.6839

Gambar 6. (a) Pengecilan 50%, (b) Perbesaran 200%. *Watermark* masih dapat dideteksi.

Hasil pengujian untuk operasi pengolahan citra yang lain seperti pengubahan kontras dan tingkat kecerahan, *sharpening*, penambahan derau *salt and peppers*, dan lain-lain juga menunjukkan bahwa *watermark* tetap berhasil dideteksi keberadaannya.

5. Penutup

Di dalam makalah ini telah dipresentasikan metode *image watermarking* untuk citra berwarna. Metode yang digunakan adalah Algoritma Barni yang dimodifikasi untuk kasus citra berwarna. Eksperimen menunjukkan bahwa untuk citra berwarna metode ini tetap memiliki *imperceptibility* yang bagus dan kokoh terhadap operasi pengolahan citra seperti kompresi, *cropping*, *histogram equalization*, *gamma correction*, dan *resizing*.

DAFTAR PUSTAKA

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

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

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

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

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