IMPLEMENTASI *WATERMARKING* UNTUK PENYEMBUNYIAN DATA PADA CITRA DALAM DOMAIN FREKUENSI MENGGUNAKAN *DISCRETE COSINE TRANSFORM*

Kartika Firdausy[1], Ikhwan Hawariyanta[2], Murinto[3]
[1] Program Studi Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan
[2,3] Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan
Kampus III, Jln. Prof Soepomo, Janturan, Yogyakarta, Telp. (0274) 379418
Fax. (0274) 381523, email: kartikaf@indosat.net.id

Abstrak

Saat ini banyak karya seni dalam format citra digital. Perkembangan teknologi informasi, terutama internet, memberi kemudahan dalam mengkopi file-file digital dari satu komputer ke komputer lain. Untuk itu diperlukan sebuah sistem keamanan untuk melindungi karya tersebut agar tidak bisa ditiru (dibajak) dengan mudah. Tujuan penelitian ini adalah menerapkan dan menganalisis teknik watermarking untuk melindungi Hak Atas Kekayaan Intelektual (HAKI) atau Intellectual Property Right dengan memberi tanda atau label pada citra digital. Penelitian diimplementasikan pada citra host (citra yang akan diberi label) dan citra watermark (label) dalam format grayscale dengan jenis citra statis yang berekstensi BMP. Citra hasil proses watermarking dinamakan citra watermarked. Proses penyisipan watermark ke dalam citra host dilakukan pada domain frekuensi dengan Discrete Cosine Transform (DCT). Hasil penelitian menunjukkan bahwa citra watermarked masih berkualitas baik, dengan nilai Peak Signal to Noise Ratio (PSNR) yang tinggi antara 46,9 dB sampai dengan 76,3 dB. Hasil ekstraksi watermark dari ctra watermarked menunjukkan bahwa watermark yang disisipkan pada citra host masih dapat diperlihatkan eksistensinya dengan melihat nilai Normalized Cross Correlation (NC) yang berada pada 0,965 sampai dengan 0,988. Hal ini membuktikan bahwa hasil uji terhadap penerapan watermarking memanfaatkan transformasi DCT memiliki ketahanan yang baik terhadap pemrosesan citra, khususnya kompresi lossy JPEG.

***Kata kunci** : HAKI, watermarking, Discrete Cosine Transform (DCT), PSNR*

1. PENDAHULUAN

Ada beberapa faktor yang membuat penggunaan data digital semakin marak dan disukai, yaitu [5] :

a. mudah diduplikasi dan hasilnya sangat mirip dan bahkan bisa sama dengan aslinya.
b. murah untuk penduplikasian dan penyimpanannya.
c. mudah disimpan untuk kemudian diproses atau diolah lebih lanjut.
d. mudah untuk didistribusikan baik melalui media fisik (*disk*) maupun media jaringan seperti *Internet*, dan lain-lain.

Segala kemudahan yang didapat di dunia digital tersebut mendorong pula munculnya ide-ide negatif, seperti adanya pembajakan terhadap hasil karya orang lain ataupun sabotase terhadap data-data rahasia yang seharusnya hanya bisa diketahui oleh pihak yang berhak saja. Banyak cara yang sudah ditempuh untuk melindungi data digital. Satu dekade terakhir ini mulai muncul *steganography*, yaitu suatu teknik yang digunakan untuk menyembunyikan sebuah pesan, di mana nantinya pesan tersebut dapat diambil kembali oleh pihak-pihak yang berhak saja. Salah satunya adalah dengan cara penandaan dokumen. Jika semua obyek ditandai dengan label yang sama, hal ini dikenal sebagai proses *watermarking* [1].

Herdiaman [3] melakukan penelitian dengan judul "Pengamanan Informasi dengan Menggunakan Teknik *Least Significant Bits* (LSB) pada Metode *Steganography* dengan Delphi". Penelitian tersebut membahas teknik penyembunyian data (label) teks dalam format *.txt, dan media penyembunyiannya (*host*) adalah citra dengan format *.bmp. Penelitian tersebut menitikberatkan pada bagaimana data itu disembunyikan ke dalam media yang lain untuk

meningkatkan keamanan data. Permasalahan yang belum dibahas dalam penelitian tersebut adalah bagaimana bila media yang digunakan untuk menyembunyikan data tersebut dikenai serangan atau pemrosesan citra, apakah data yang disembunyikan masih bisa ditemukan lagi atau tidak. Artinya, sejauh mana ketahanan citra *watermarked* (citra yang telah dikenai proses *watermarking*) dalam mempertahankan data yang dibawanya apabila dilakukan serangan terhadapnya sehingga data yang dibawa dapat dibuktikan kembali keberadaanya.

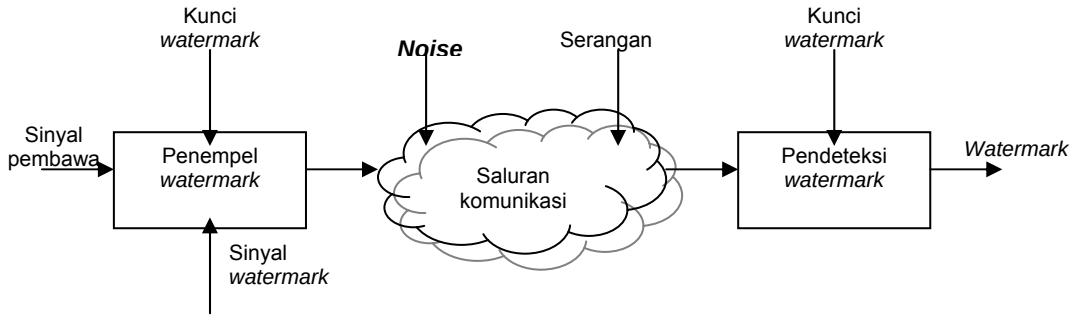
1.1. Watermarking

Watermarking adalah proses penempelan data (*watermark*/label) ke dalam sebuah obyek multimedia yang setipe (bertipe digital) di mana *watermark* tersebut dapat dideteksi dan diekstrak/dipisahkan pada suatu saat untuk mendapatkan sebuah pernyataan tentang obyek multimedia tersebut. Obyek tersebut dapat berupa gambar/citra atau audio ataupun video. Sebuah contoh sederhana dari digital *watermark* adalah sebuah segel/tanda yang terlihat di atas sebuah gambar untuk identifikasi hak cipta. Dengan memberikan tanda *watermark* yang berupa informasi pada barang yang diperjualbelikan akan diketahui bahwa barang tersebut asli atau hanya sebuah salinan saja.

Pada umumnya, dalam proses *watermarking* terdapat tiga komponen utama yaitu [5]:

a. label/*watermark*
b. proses penyembunyian label (penempelan).
c. menghasilkan kembali label *watermark* (verifikasi atau ekstraksi).

Pada sistem *watermarking* terdapat beberapa komponen utama yang harus diperhatikan. Gambar 1 memperlihatkan komponen-komponen tersebut [7].



Gambar 1. Sistem *Digital Watermarking*

Pada sistem *digital watermarking* terdiri dari dua bagian utama yaitu penempel *watermark* dan pendeteksi *watermark*. Penempel *watermark* menempelkan sinyal *watermark* ke dalam sinyal pembawa dan pendeteksi *watermark* mendeteksi kehadiran sinyal *watermark*. Terdapat sebuah entitas kunci *watermark*, kunci ini digunakan selama proses penempelan dan pendeteksian *watermark*. Saluran komunikasi pada umumnya berderau, yaitu cenderung terjadi serangan terhadap keamanan data, maka teknik *watermarking* harus tahan terhadap derau atau serangan.

Salah satu karakteristik *digital* w*atermarking* adalah *robust* artinya *watermark* di dalam *host* data harus tahan terhadap beberapa operasi pemrosesan digital yang umum seperti penkonversian dari digital ke analog dan sebaliknya, serta kompresi terutama kompresi *lossy*.

Penerapan metode *watermarking* pada domain frekuensi berarti data digital ditransformasikan dahulu ke dalam domain frekuensi, misalnya dengan menggunakan *Discrete Cosine Transform* (DCT). Citra hasil pemrosesan *watermarking* dengan memanfaatkan transformasi DCT diharapkan akan lebih tahan terhadap serangan/pengolahan citra.

DCT adalah transformasi yang sangat mirip dengan transformasi *Fourier* dan menghasilkan produk yang sejenis [8]. Transformasi ini akan mengolah titik-titik dari *domain spasial* dan mentransformasikannya ke bentuk sejenis dalam *domain frekuensi.* DCT mengolah sinyal tiga dimensi yang digambar pada sumbu-sumbu X, Y, dan Z.

Pada kasus ini sinyal adalah gambar grafik. Sumbu-sumbu X dan Y menunjukkan frekuensi dari sinyal dalam dua dimensi yang berbeda. Amplitudo dari sinyal pada kasus ini adalah nilai dari piksel pada titik di layar. Sebagai contoh adalah nilai yang digunakan untuk menyajikan gambar dalam derajat keabuan (*grayscale*). Gambar grafik yang ditampilkan di layar dapat dianggap sebagai sinyal tiga dimensi yang kompleks dengan nilai sumbu Z ditunjukkan oleh warna pada layar pada titik yang bersangkutan. Ini adalah sinyal yang direpresentasikan pada *domain spasial*. DCT dapat digunakan untuk mengubah informasi spasial ke bentuk frekuensi atau spektral. Terdapat fungsi *invers* DCT (IDCT) yang dapat membalikkan representasi spektral ke bentuk spasial mula-mula.

Rumus DCT dua dimensi dapat ditunjukkan pada persamaan (1) dan rumus untuk Invers DCT ditunjukkan pada persamaan (2) sebagai berikut [2]:

$$DCT\ (i,j) = \frac{2}{N} C(i) C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} pixel\ (x,y)\ Cos\ \left[\frac{(2x+1)i\pi}{2N}\right] Cos\ \left[\frac{(2y+1)j\pi}{2N}\right] \quad (1)$$

$$C(i), C(j) = \begin{cases} \frac{1}{\sqrt{2}} & \text{untuk} \quad \text{i, j} = 0 \\ 1 & \text{untuk} \quad i, j > 0 \end{cases}$$

i = posisi baris untuk koefisien DCT x = posisi baris untuk piksel N = banyaknya baris atau kolom
j = posisi kolom untuk koefisien DCT y = posisi kolom untuk piksel

DCT dikenakan pada sebuah matriks bujur sangkar $N \times N$ dari nilai-nilai piksel, dan akan menghasilkan sebuah matrik bujur sangkar $N \times N$ dari koefisien frekuensi.

$$Pixel\ (x,y) = \frac{2}{N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} C(i) C(j)\ DCT\ (i,j)\ Cos\ \left[\frac{(2x+1)i\pi}{2N}\right] Cos\ \left[\frac{(2y+1)j\pi}{2N}\right] \quad (2)$$

$$C(i), C(j) = \begin{cases} \frac{1}{\sqrt{2}} & \text{untuk} \quad i, j = 0 \\ 1 & \text{untuk} \quad \text{i, j} > 0 \end{cases}$$

Transformasi ini berbasiskan vektor. DCT membagi citra ke dalam 8 × 8 blok citra. Setiap blok akan dihitung koefisiennya masing-masing. DCT 2 dimensi menghasilkan citra hasil transformasi ke dalam matriks 2 dimensi.

1.2. Peak Signal to Noise Ratio (PSNR) dan Normalized Cross Correlation (NC)

PSNR digunakan untuk menentukan kualitas citra *watermarked* setelah disisipi *watermark*. Citra *watermarked* dibandingkan dengan citra asli (citra *host*) untuk menentukan kualitas citra *watermarked*. Semakin besar nilai PSNR berarti penyisipan pesan (*watermark*) ke dalam citra asli tidak menyebabkan penurunan kualitas citra *watermarked*. Sebaliknya jika nilai PSNR semakin kecil maka pada citra *watermarked* akan terjadi penurunan kualitas citra. Nilai PSNR biasanya mempunyai rentang nilai antara 20 dB sampai dengan 60 dB. Tabel 1 memperlihatkan nilai PSNR beserta penjelasannya [9].

Tabel 1. Nilai PSNR

Rasio (dB)	Kualitas Citra
60 dB	*Excellent*, tanpa derau
50 dB	*Good*, terdapat banyak derau tapi kualitas citra masih bagus
40 dB	*Reasonable*, terdapat butiran halus seperti salju dan beberapa detail citra hilang
30 dB	*Poor*, terdapat banyak derau pada citra
20 dB	*Unusable*

Rumus untuk menghitung PSNR dapat dilihat pada persamaan (3) [4].

$$PSNR = \frac{XY \max_{x,y} p^2{}_{x.y}}{\sum_{x.y} \left(P_{x,y} - \overline{P}_{x,y} \right)^2} \quad (3)$$

$P_{x,y}$ adalah citra *host* *X, Y* adalah ukuran citra.

$\overline{P_{x,y}}$ adalah citra yang telah diberi *watermark*.

PSNR dalam satuan decibels (dB) dapat dihitung dengan rumus (4) [4].

$$PSNR = 10 \log_{10} .PSNRdB \quad (4)$$

Nilai PSNR yang tinggi adalah lebih baik karena berarti rasio sinyal terhadap derau juga tinggi. Sinyal adalah citra asli dan derau adalah kesalahan dalam merekonstruksi kembali citra. Untuk mengukur kemiripan label *watermark* asli dan label *watermark* hasil ekstraksi secara kuantitatif digunakan *Normalized Cross Correlation* (NC) yang didefinisikan pada rumus (5) [6].

$$\mathrm{NC} = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{M-1} W(i,j) W'(i,j)}{\sum_{i=0}^{M-1} \sum_{j=0}^{M-1} \left[W(i,j) \right]^2} \quad (5)$$

$M \times M$ adalah ukuran dari label *watermark*

W' adalah label *watermark* hasil ekstraksi W adalah label *watermark* asli

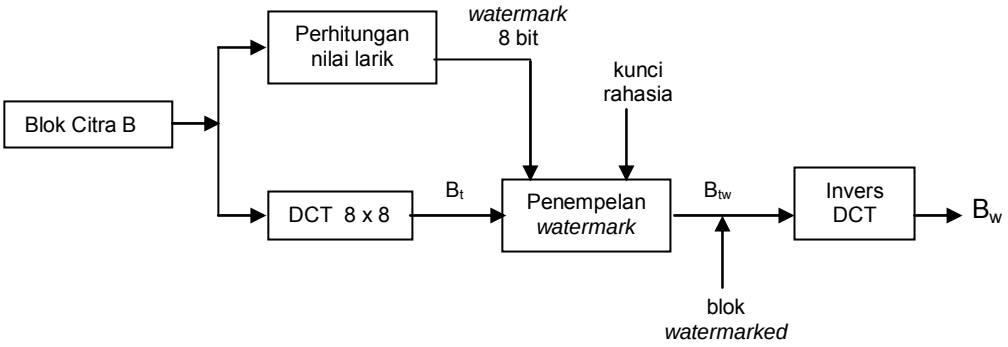
2. BAHAN DAN METODE PENELITIAN

Penelitian ini menggunakan citra dengan format *grayscale*. Ada dua jenis citra yang akan digunakan. Citra yang pertama disebut citra *host* (citra asli). Sedangkan citra yang kedua disebut label/*watermark. Watermark* akan disisipkan ke dalam citra *host* dan menghasilkan sebuah citra yang selanjutnya disebut sebagai citra *watermarked*.

Langkah-langkah umum yang dilakukan dalam penempelan *watermark* adalah sebagai berikut:

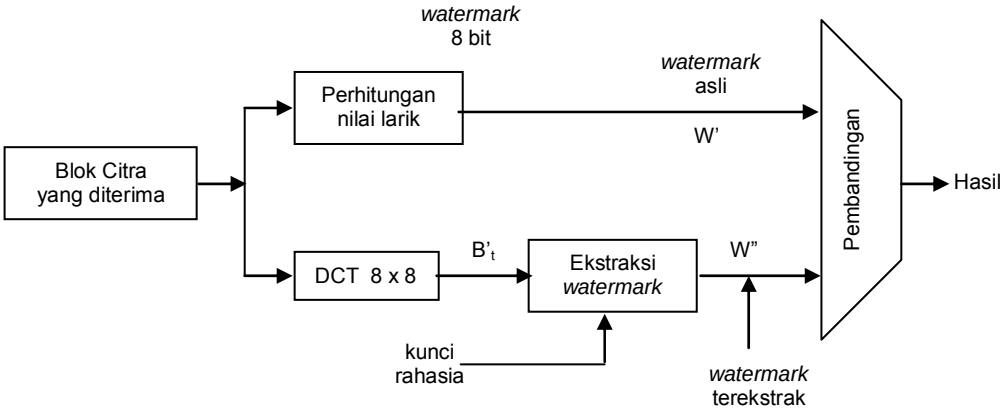
a. Untuk setiap bit *watermark* diubah ke dalam larikan bit-bit (vektor).
b. Citra blok *B* ditransformasikan ke dalam domain DCT, misalnya B_t yang dibagi ke dalam 8 blok-blok 8 x 8 dan setiap blok dihitung koefisien DCT-nya. Bit-bit *watermark* ditempelkan di dalam *middle-band* koefisien DCT untuk membuat blok DCT yang diberi *watermark* B_{tw} di dalam domain DCT
c. Langkah yang terakhir dalam proses penempelan *watermark* adalah menerapkan invers DCT (IDCT) pada blok B_{tw} hasil transformasi DCT untuk menciptakan blok B_w.

Gambar 2 memperlihatkan diagram blok proses penempelan *watermark*. Setelah citra *watermarked* terbentuk dan telah banyak mengalami penyimpanan ulang maka *watermark* perlu dibuktikan kembali keberadaannya (diekstrak). Tujuan proses pengekstraksian ini adalah untuk melihat apakah *watermark* tersebut tahan terhadap serangan (diasumsikan citra *watermarked* mengalami serangan sebelum dilakukan proses ekstraksi). Dan untuk membandingkan tingkat kemiripan dari label *watermark* setelah proses ekstraksi maka watermark asli juga disertakan dalam proses ekstraksi.



Gambar 2. Proses Penempelan *Watermark*

Gambar 3 menunjukkan proses umum yang terjadi pada proses ekstraksi. Pertama kali citra yang diterima (citra yang diuji) dibagi menjadi 8 x 8 blok-blok *non-overlapping*. Setiap blok *B'* mempunyai tiga langkah utama dalam pembuktiannya apakah citra tersebut sudah rusak atau belum, yaitu perhitungan *watermark*, ekstraksi *watermark*, dan pembandingan *watermark*.



Gambar 3. Proses Ekstraksi Label *Watermark*

Proses ekstraksi memiliki langkah-langkah utama yaitu :

a. Blok *B'* citra yang diterima ditransformasikan ke domain DCT $B_t^{'}$ yang membagi menjadi 8 blok-blok 8 x 8 dan untuk setiap koefisien blok 8 x 8 DCT dihitung.
b. Larikan PN dihitung bersama dengan kunci rahasia *K*, dan kemudian dibandingkan dengan koefisien *middle-band* DCT dari blok $B_t^{'}$ hasil transformasi.
c. Larikan bit (*bitstream*) yang terekstrak merepresentasikan *watermark W"* yang telah diekstrak.
d. Untuk memverifikasi keaslian blok *B'* pada citra maka *watermark* terekstrak *W"* dibandingkan dengan *watermark* asli *W'*.

Guna menguji ketahanan citra *watermarked*, akan dikenai sebuah serangan. Serangan akan dilakukan dengan persepsi bahwa citra yang telah diserang masih bisa digunakan/ didistribusikan oleh pihak lain baik pihak yang mengetahui bahwa citra tersebut telah ditempeli sebuah pesan atau pihak yang sama sekali tidak mengetahui. Serangan yang akan dilakukan adalah kompresi *lossy* JPEG. Dalam kompresi *lossy* JPEG citra *watermarked* yang berekstensi BMP akan disimpan ulang dengan ekstensi JPG yang sebelumnya ditentukan terlebih dahulu derajat kualitas citra hasil kompresi *lossy* JPEG tersebut. Indeks kompresi yang digunakan adalah 25, 50, 75, dan 100.

Implementasi DCT menggunakan MATLAB versi 7 dengan memanfaatkan fasilitas *Image Processing Toolbox* (IPT) yang ada di Matlab. IPT merupakan kumpulan fungsi-fungsi

untuk menampilkan dan memproses citra. Fungsi tersebut antara lain untuk operasi transformasi citra (*dct*, *dct2*, *idct*, *idct2*), yang digunakan untuk membantu dalam proses membuat citra *watermarked.* Untuk mempermudah dalam proses *watermarking* (menjadi lebih interaktif dan bisa dilihat komponen-komponen yang ada dalam proses *watermarking*), maka alat bantu dalam proses *watermarking* diwujudkan ke dalam sebuah aplikasi berbasis grafis/ *Graphical User Interface* (GUI). Fasilitas pembuatan GUI ini disertakan dalam Matlab versi 7.

3. HASIL DAN PEMBAHASAN

3.1. Penyisipan *Watermark* ke dalam Citra Pembawa (Citra *Host*)

Dalam penyisipan *watermark* ke dalam citra *host* menggunakan program bantu, yang berisi algoritma proses penyisipan *watermark* yang telah diberi tambahan fungsi untuk mencari nilai PSNR yang digunakan untuk menguji kualitas citra *watermarked*. Untuk memperjelas proses penyisipan dibuat GUI dengan tampilan seperti pada Gambar 4 yang mempunyai bagian utama program yang digunakan untuk proses penyisipan *watermarking* dan pencarian PSNR.

Gambar 4. Tampilan GUI Program Sisip *Watermark*

3.2. Serangan Kompresi *Lossy* JPEG pada Citra *Watermarked*

Serangan dilakukan pada citra *watermarked* untuk menguji ketahanan *watermark* yang ada dalam citra *watermarked* tersebut. Serangan menggunakan program bantu yang berisi fungsi untuk menyerang citra *watermarked* yang telah diberi tambahan fungsi untuk mencari nilai PSNR yang digunakan untuk menguji kualitas citra *watermarked* setelah diserang. Serangan yang diberikan adalah kompresi *lossy JPEG* pada kualitas 25, 50,75, dan 100.

3.3. Ekstraksi *Watermark* dari Citra *Watermarked*

Ekstraksi *watermark* menggunakan program bantu berisi algoritma proses pengambilan *watermark* yang telah diberi tambahan fungsi untuk mengetahui nilai NC *watermark* asli dan *watermark* hasil ekstraksi dari proses ekstraksi *watermarking*. Untuk memperjelas proses ekstraksi *watermark* dibuat GUI yang mempunyai bagian utama program yang digunakan untuk proses ekstraksi *watermark* dan penentuan nilai NC.

Citra *host* yang digunakan adalah citra ukuran 256x256 *gray level* dan *watermark* berukuran 32x32 *gray level* 256. Algoritma yang dibuat menetapkan bahwa *watermark* harus lebih pendek ukurannya dibandingkan dengan ukuran citra *host* (ukuran diperoleh setelah kedua citra diubah ke dalam data larik/vektor). Ukuran citra *host* dan *watermark* dalam satuan piksel. Faktor ketahanan k dalam penelitian ini menggunakan lima buah variasi yaitu : 10, 20, 30, 40, dan 50. Faktor ketahanan k akan berpengaruh pada kualitas citra *watermarked*. Pengaruh ini dapat dilihat pada Tabel 2 yang memuat nilai PSNR untuk masing-masing citra *watermarked*.

Tabel 2. PSNR untuk Citra *Host* 256x256 dan Label *Watermark* 32x32

No	Faktor k	PSNR (dB)
1	10	64,5
2	20	58,7
3	30	55,3
4	40	53,1
5	50	51,2

Pada Tabel 2 dapat dilihat nilai PSNR yang cukup besar dan berdasarkan pada Tabel 1 (tabel kriteria kualitas citra) maka dapat dikatakan bahwa citra *watermarked* hasil proses *watermarking* menggunakan algoritma yang telah dibuat menghasilkan citra *watermarked* dengan kualitas *reasonable* sampai dengan *excellent*, karena PSNR berkisar antara 51,2 dB sampai 64,5 dB.

Penerapan serangan terhadap citra *watermarked* akan dikenakan pada citra *watermarked* dengan faktor k = 30. Untuk memperlihatkan *robustness watermark* terhadap kompresi lossy JPEG, pertama kali citra *watermarked* dikompres dengan indeks 25, 50, 70, dan 100. *Watermark* akan diekstrak dari citra hasil kompresi *lossy* JPEG tersebut. Tabel 3 memperlihatkan kualitas citra *watermarked* berdasarkan PSNR sesuai pendekatan pada Tabel 1. setelah citra tersebut dikenai proses serangan kompresi lossy JPEG. Citra yang digunakan di sini adalah citra *host* berukuran 256x256 dan label *watermark* 32x32 dengan faktor ketahanan 30 (citra *watermarked* hasil serangan di atas).

Tabel 3. Kualitas Citra *Watermarked cam256* Setelah Kompresi

citra *watermarked* dengan faktor k = 30			
No	**Jenis Serangan**	**PSNR (dB)**	**Kualitas**
1.	Kompresi JPEG indeks 25	46,9	*Reasonable*
2.	Kompresi JPEG indeks 50	49, 4	*Good*
3.	Kompresi JPEG indeks 75	52,4	*Good*
4.	Kompresi JPEG indeks 100	76,3	*Excellent*

Dalam proses ekstraksi melibatkan *watermark* asli guna membuktikan kepemilikan citra *host* dan *watermark*, karena algoritma yang digunakan mengharuskan melibatkan *watermark* asli.

Kemiripan antara kedua *watermark* yaitu *watermark* yang tidak diproses (*watermark* asli) dan *watermark* yang diperoleh dari hasil ekstraksi pemrosesan citra secara kuantitatif diukur dengan menggunakan *Normalized Cross Correlation* (NC). Hasil perhitungan untuk citra *host* dan *watermark* dapat dilihat pada Tabel 4.

Tabel 4. Nilai NC *Watermark* Terekstrak dari Citra *Host cam256*

No	Operasi Proses pada Citra ***Watermarked***	NC
1.	JPEG Indeks 25	0,988
2.	JPEG Indeks 50	0,970
3.	JPEG Indeks 75	0,973
4.	JPEG Indeks 100	0,965

Tabel 4 menunjukkan bahwa hasil uji terhadap penerapan *watermarking* memanfaatkan transformasi DCT memiliki ketahanan yang baik terhadap serangan kompresi *lossy* JPEG.

4. KESIMPULAN

Dari penelitian ini dapat ditarik kesimpulan bahwa algoritma dan teknik *watermarking* yang diimplementasikan menunjukkan bahwa kualitas citra *watermarked* masih dalam keadaan baik yaitu berkualitas *reasonable* sampai dengan *excellent*, karena PSNR berkisar antara 46,9 dB sampai 76,3 dB dan keberadaan *watermark* masih dapat dipertahankan setelah dilakukan serangan (pemrosesan citra) pada citra *watermarked* dengan kompresi *lossy* JPEG dengan melihat nilai *Normalized Cross Correlation* (NC) yang berada pada 0,965 sampai dengan 0,988.

DAFTAR PUSTAKA

[1] Cummins, J., Diskin, P., Lau, L., and Parlett, R., "**Steganography And Digital Watermarking**", School of Computer Science, The University of Birmingham, 2004
[2] Gonzales, R. C., and Wintz, P., "**Digital Image Processing***"*, Prentice Hall, Addison Wesley Publishing, USA, 1987
[3] Herdiaman, A.I., "**Pengamanan Informasi dengan Menggunakan Teknik Least Significant Bits (LSB) pada Metode *Steganography* dengan Delphi**", Skipsi S-1, Universitas Ahmad Dahlan, Yogyakarta, 2004.
[4] Shoemaker,C.,"**Hidden Bits: A Survey of Techniques for Digital Watermarking**", 2002 http://www.vu.union.edu/~shoemakc/watermarking/
[5] Suhono, H., Supangkat, Kuspriyanto dan Juanda, "**Watermarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital**", Jurnal, Departemen Teknik Elektro Institut Teknologi Bandung, Bandung, 2001
[6] Tsai, C. C and Chang, C. C., **"Embedding Robust Gray-level Watermark in an Image Using Discrete Cosine Transformation***"*, Department of Computer Science and Information Engineering National Chung Chang University, Taiwan, ROC.
[7] http://www.wipro.com/dsp, "**Digital Watermarking : A Technology Overview"**
[8] http://www.ece.purdue.edu/~ace/jpeg-tut/jpgimag1.html.
[9] http://www.ctr.Columbia.edu/~shsram/vis/hwk1/psnr.html.