

WATERMARKING CITRA DIGITAL MENGGUNAKAN METODE *DISCRETE COSINE TRANSFORM*

Aris Fanani¹, Nurissaidah Ulinnuha²

UIN SunanAmpel Surabaya¹, arisfa@uinsby.ac.id¹
UIN SunanAmpel Surabaya², nuris.ulinnuha@uinsby.ac.id²

Abstrak

Pada paper ini, mengusulkan penyisipan watermark pada citra grayscale dan RGB dengan cara modulating relative size pada blok koefisien DCT. Watermark disisipkan pada blok-blok frekuensi menengah. Modulating relative size pada blok koefisien DCT diterapkan dengan menambahkan atau mengurangi blok-blok koefisien DCT. Dari uji coba yang dilakukan metode yang diusulkan menghasilkan watermark yang tahan terhadap berbagai serangan, serta kualitas yang baik dari citra yang disisipi watermark.

Kata kunci: Watermarking, Citra, DCT

Abstract

In this paper, we propose embedding the grayscale and RGB image by modulating relative size on the block DCT coefficients. Watermark is embedded in the intermediate frequency blocks. Modulating relative to the block size DCT coefficients applied by adding or subtracting blocks of DCT coefficients. From experiments performed proposed methods produce watermarks that are resistant to a variety of attacks, as well as good quality of the watermark inserted image.

Keywords: Watermarking, Image, DCT

1. Pendahuluan

Pesatnya pertumbuhan teknologi semakin mempermudah penyebaran media digital. Kemajuan semacam ini telah menyebabkan maraknya tindakan seperti duplikasi dan penyebaran data secara ilegal, serta penyalahgunaan Hak Kekayaan dan Intelektual (HAKI). Berbagai upaya telah dilakukan untuk mengatasi masalah HAKI pada media digital, salah satunya dengan digital watermarking. Watermarking merupakan proses menyembunyikan informasi [1], untuk menunjukkan kepemilikan atau melacak penyalahgunaan hak cipta pada arsip digital seperti citra digital, audio, video [2].

Digital watermarking harus memenuhi beberapa kriteria *robustness*, *imperceptibility*, dan *security*[3]. *Robustness* berarti seberapa tangguh watermark dapat bertahan dari berbagai macam serangan untuk menghilangkan watermark seperti *scaling*, *cropping* dan *compression*. *Imperceptibility* berhubungan dengan keberadaan watermark yang tidak boleh tampak oleh kasat mata manusia dan degradasi pada citra. *Security* berarti watermark yang disisipkan tidak dapat terdeteksi dengan analisa statistik atau metode lain.

Watermarking citra digital berdasarkan domain aplikasi dibagi menjadi

dua kelompok: domain spasial dan domain transformasi [4]. Teknik *watermarking* pada domain spasial seperti *Least Significant Bit* (LSB) pernah dilakukan oleh [5] yang menggabungkan *Discrete Wavelet Transform* (DWT) dan LSB untuk aplikasi biometrik. Metode ini memiliki keunggulan dalam kapasitas informasi yang disisipkan, tetapi mudah di dideteksi oleh beberapa program [6]. Meskipun metode domain spasial terlihat sederhana, teknik *watermarking* pada domain transformasi lebih tangguh terhadap serangan daripada metode domain spasial. Pada domain transformasi, teknik yang banyak digunakan adalah *Discrete Cosine Transform*(DCT). Beberapa penelitian memperkenalkan berbagai teknik penyisipan pada domain DCT, diantaranya metode dengan menggunakan strategi pemilihan block tepi, *recursive matrix*, dan kriteria pemilihan koefisien terbesar untuk menentukan lokasi penyisipan *watermark* [7]. Saad Al Momen [8] mengusulkan penyisipan *watermark* citra grayscale pada 8x8 block koefisien DCT, dengan perubahan koefisien DCT pada frekuensi menengah dan frekuensi tinggi. Akan tetapi, salah satu kelemahan dari penyisipan pada frekuensi yang berbeda adalah citra asli terdistorsi oleh noise karena *watermark* itu sendiri.

Pada penelitian ini, diusulkan penyisipan *watermark* pada citra grayscale dan RGB dengan cara modulating relative size koefisien DCT, dimana perubahan hanya dilakukan pada frekuensi menengah. Dari metode yang diusulkan bertujuan untuk mendapatkan citra ter*watermark* dengan sedikit distorsi dan tingkat keamanan yang baik.

2. Watermarking Citra Digital Menggunakan Berdasarkan Perubahan Koefisien DCT

2.1 Transformasi DCT

Discrete Cosine Transform (DCT) merupakan dekomposisi sinyal yang

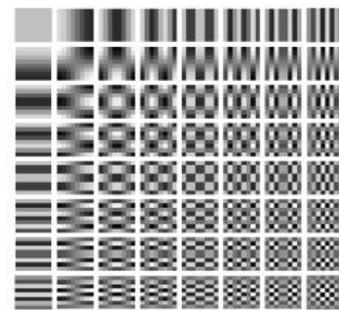
mengkonversikan citra dari domain spasial ke dalam domain frekuensi. Fungsi dua dimensi DCT (2D DCT) untuk matrik s berukuran $n \times n$ diberikan persamaan 1 [9]:

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

dimana

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

Setiap elemen $S(i, j)$ dari hasil transformasi merupakan hasil kali dalam antara elemen-elemen matrik s dengan basis fungsi, dimana basis fungsi merupakan matrik berukuran $n \times n$. Setiap matrik basis dua dimensi (fungsi basis) merupakan hasil kali dari dua basis vektor satu dimensi. Untuk $n = n = 8$, dapat dibentuk sebuah array 8x8 dari matrik basis-matrik basis 8x8. Setiap basis matrik dapat dianggap sebagai sebuah citra. Citra basis sejumlah 64 di dalam array seperti pada Gambar 1.



Gambar 1. Basis fungsi DCT dua dimensi.

Sejumlah nilai matrik s dapat dikembalikan dari transformasi $S(i, j)$ dengan menerapkan fungsi invers DCT (IDCT) dua dimensi:

$$\begin{aligned}
 & \text{piksel}(x, j) \\
 &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} C(i) \times C(j) \times DCT(i, j) \\
 & \times \cos \left[\frac{(2x+1)i\pi}{2n} \right] \cos \left[\frac{(2y+1)j\pi}{2n} \right], \quad (2)
 \end{aligned}$$

dimana

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

2.2 Proses Penyisipan Watermark

Proses penyisipan atau penanaman adalah proses menyisipkan suatu label *watermark* ke dalam *cover host*. Terdapat dua jenis *watermark* yang digunakan dalam desain *watermarking* yaitu pembangkitan secara acak noise dan *watermark* citra logo yang memiliki arti. Karena *watermark* citra logo lebih berisi informasi dan menyakinkan dibandingkan hasil keluaran biner, sehingga citra logo biner dipilih sebagai *watermark*. Pada penelitian ini diusulkan penyisipan *watermark* dengan cara perubahan dua koefisien DCT didalam satu block citra. Proses penyisipan terdiri dari tiga langkah yaitu: transformasi, penyisipan dan invers transformasi seperti pada Gambar 2.

2.1.1 Transformasi

Cover host yang akan disisipi *watermark* terlebih dahulu dibaca sebagai suatu matrik dua dimensi. Matrik tersebut dibagi menjadi sejumlah blok yang telah ditentukan banyaknya (jumlah block adalah 8), dimana satu blok berisi sejumlah pixel. Matrik yang telah dibentuk menjadi sejumlah blok kemudian ditransformasikan dengan menggunakan transformasi DCT seperti dijelaskan pada Persamaan 1. Dari transformasi tersebut blok-blok pada matrik akan terbagi menjadi tiga daerah, yaitu daerah blok-blok dengan frekuensi rendah (FL), daerah blok-blok dengan frekuensi

menengah (FM), dan daerah blok-blok dengan frekuensi tinggi (FH) seperti terlihat pada Gambar 3.

Blok-blok yang dipilih sebagai daerah penyisipan *watermark* adalah blok-blok pada frekuensi menengah. Alasan penanaman pada blok-blok frekuensi menengah karena penanaman pada daerah tersebut tidak akan merusak citra secara signifikan dibandingkan jika penanaman dilakukan pada blok frekuensi tinggi dan rendah. Penanaman pada blok frekuensi rendah dan tinggi sangatlah tidak cocok, karena penglihatan manusia lebih peka terhadap perubahan *cover host* jika dilakukan modifikasi terhadap block frekuensi tinggi dan rendah.

2.1.2 Penyisipan

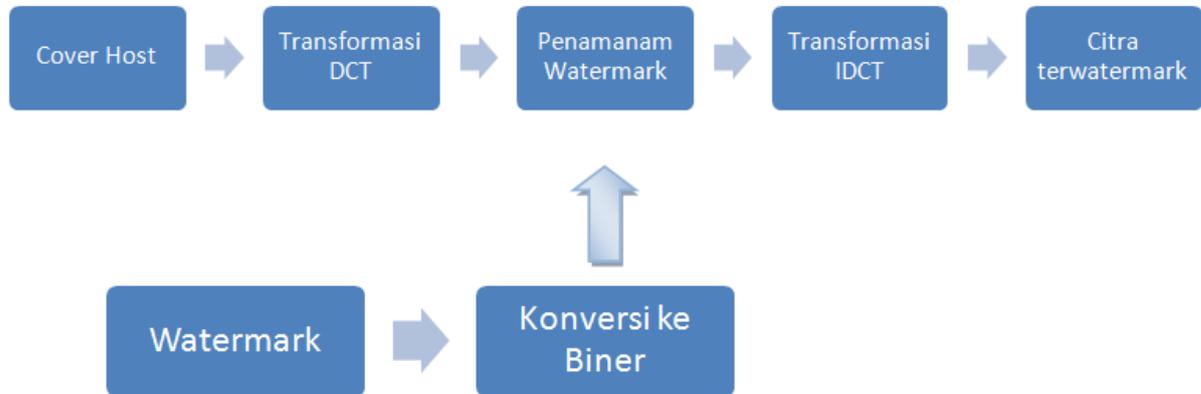
Setelah menentukan blok frekuensi menengah, langkah selanjutnya adalah memilih dua blok pada blok frekuensi menengah. Dua blok yang telah ditentukan sebagai area penanaman *watermark* selanjutnya dilakukan penukaran nilai koefisien DCT antara keduanya dengan cara membandingkannya. Sedangkan untuk menyisipkan suatu *watermark* ke dalam citra diperlukan parameter (K), dimana K merupakan bilangan yang menjadikan blok-blok koefisien DCT yang telah ditukar antara dua blok yang telah ditentukan sebagai area penanaman *watermark* memiliki selisih tertentu. Pada citra RGB, *channel blue* yang akan dijadikan sebagai kandidat penyisipan *watermark*. Karena mata manusia kurang sensitif terhadap modifikasi pada *channel blue* dari pada *channel red* dan *channel green*[9]. Algoritma penyisipan seperti pada Gambar 4.

2.1.3 Invers Transformasi

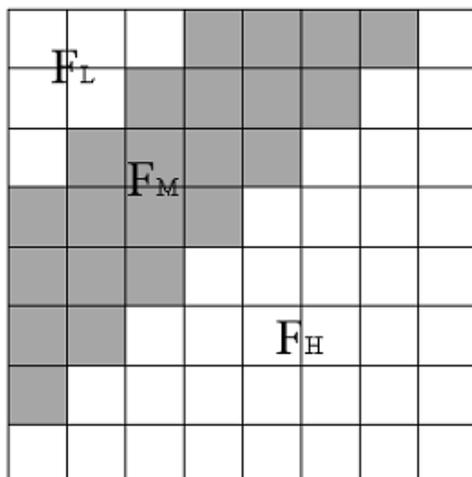
Proses selanjutnya dilakukan transformasi balik dengan menggunakan transformasi IDCT untuk mendapatkan citra *terwatermark*.

2.2 Proses Pengekstrakan *Watermark*

Seperti ditunjukkan pada Gambar 5, proses pengestrakan *watermark* dari *cover host* terdiri dari dua proses, yaitu:



Gambar 2. Proses Penyisipan *watermark*



Gambar 3. Pendefinisian Blok pada DCT

```

    For i = 1 : panjang pesan
    If m=0 then
      If blok (u1,v1) < blok (u2,v2) then
        Tukar blok (u1,v1) dan blok (u2,v2)
      End if
    Else
      If Blok (u1,v1) > Blok (u2,v2) then
        Tukar Blok (u1,v1) dan Blok (u2,v2)
      End if
    End
    if (blok(u1,v1) > bloc(u2,v2))
      if (blok(u1,v1) - blok(u2,v2) < k)
        blok(u1,v1) = blok(u1,v1) + (k/2);
        blok(u2,v2) = blok(u2,v2) - (k/2);
      end
    else
      if (dct_block(u2,v2) - dct_block(u1,v1) < k)
        blok(u2,v2) = blok(u2,v2) + (k/2);
        blok(u1,v1) = blok(u1,v1) - (k/2);
      end
    end
  end
  
```

Gambar 4. Algoritma penyisipan

2.2.1 Transformasi DCT

Proses awal pengestrakan adalah citra *terwatermark* ditransformasikan dengan menggunakan transformasi DCT.

2.2.2 Pengekstrakan *Watermark*

Setelah dilakukan transformasi DCT pada citra *terwatermark*, akan terbentuk blok-blok DCT. Blok-blok koefisien DCT pada dua blok frekuensi menengah yang digunakan sebagai tempat penyisipan dibandingkan untuk mendapatkan citra *watermark*. Pada ekstraksi juga dibutuhkan citra *watermark* asli yang digunakan sebagai

pembanding ukuran dalam pembentukan citra *watermark* hasil ekstraksi. Proses perbandingan dua blok sesuai kriteria sebagai berikut:

$$m_i = \begin{cases} 0, & \text{untuk } (u_1, v_1) > (u_2, v_2) \\ 1, & \text{untuk } (u_1, v_1) < (u_2, v_2) \end{cases} \quad (3)$$



Gambar 5. Proses Pengekstrakan *watermark*

3. Skenario Uji Coba

Serangkaian uji coba dilakukan pada beberapa citra standart 512x512 citra berwarna dan 256x256 citra grayscale. *Watermark* yang digunakan dalam percobaan adalah citra logo dengan ukuran 32x32. Contoh *cover host* dan *watermark* seperti pada Gambar 6.

Blok-blok koefisien DCT pada frekuensi menengah (FM) yang dipilih sebagai tempat penyisipan *watermark* adalah blok(5,2) dan blok (4,3). Semakin besar penentuan nilai parameter K yang digunakan akan mengakibatkan penurunan kualitas citra[10]. Nilai K yang digunakan pada ujicoba adalah $K = \{0.5, 1, 2, 3, 5, 10, 20, 30, 40 \text{ dan } 50\}$

Untuk mengukur kualitas citra pada *watermarking*, diperlukan alat ukur yang akan digunakan sebagai parameter. Alat ukur tersebut adalah *Peak Signal to Noise Ratio* (PSNR). Parameter PSNR menunjukkan perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut [4], diukur dalam satuan desibel (dB). Pada penelitian ini, PSNR digunakan untuk mengetahui kualitas *cover host* yang disisipi *watermark*.

Untuk menentukan PSNR, terlebih dahulu harus diketahui nilai rata-rata kuadrat dari error (*Mean Square Error - MSE*). Semakin besar nilai PSNR berarti semakin mirip citra *terwatermark* dengan *cover host*. Hal ini juga berarti bahwa skema *watermark* semakin efektif. Citra dengan nilai PSNR >35 dB dapat dikatakan memiliki kualitas yang baik [11]. Persamaan 4 menunjukkan rumus PSNR.

$$PSNR = 10 \log_{10} \frac{E_{max}^2 \times I_w \times I_h}{\sum (I_{x,y} - I_{x,y}^*)^2} \quad (4)$$

dimana I_w, I_h merupakan lebar dan tinggi citra *terwatermark*, $I_{x,y}$ nilai piksel *cover host* pada koordinat (x,y) dan $I_{x,y}^*$ nilai piksel *cover host* yang ditukar pada koordinat (x,y). E_{max} merupakan nilai maksimum piksel (yaitu, $E_{max} = 255$ untuk 256 citra gray-level).

Ujicoba pertama yang dilakukan adalah memproses *watermarking* dan mengekstrak *watermark* untuk beberapa nilai parameter K serta mencatat nilai PSNR. Sedangkan ujicoba kedua yang dilakukan adalah memberikan serangan terhadap citra *terwatermark*, dan kemudian *watermark* yang disisipkan di ekstrak. Serangan ini berupa beberapa operasi citra untuk membuktikan seberapa efektif skema *watermarking*.



Gambar 6. (a) *Cover Host* Berukuran 512x512 ;
(b) *Cover Host* Berukuran 256x256; (c)
Watermark

4. Hasil Uji Coba

Tabel 1 menunjukkan hasil percobaan terhadap citra RGB Lenna dengan logo *watermark* "ITS", dimana dilakukan proses *watermarking* dan ekstraksi *watermark*. Dari Tabel 1 terlihat bahwa untuk rentang $K = (0.5, 1, 2, 3, 4, 5, 10, 20, 30, 40, 50)$ citra *terwatermark* dengan kualitas yang dapat diterima semuanya. Karena tidak ada citra *terwatermark* dengan nilai PSNR dibawah 35dB. Sedangkan pada proses ekstraksi *watermark*, nilai K berpengaruh terhadap *watermark* yang terekstrak. Dari uji coba yang dilakukan untuk $K \geq 3$, didapatkan *watermark* terekstrak mirip dengan *watermark* asli. Serangkaian serangan juga

dilakukan untuk mengetahui efektifitas skema *watermarking*. Dari Tabel 2 terlihat bahwa dengan beberapa serangan citra *watermark* dengan kasat mata dapat terekstrak hampir sama dengan citra asli *watermark*.

Tabel 1. Nilai PSNR dan *Watermark* Terekstrak dengan Nilai Parameter *K* Berbeda

Parameter <i>K</i>	PSNR (dB)	<i>Watermark</i> Terekstrak
0.5	62.73	ITS
1	62.67	ITS
2	62.61	ITS
3	62.36	ITS
4	62.07	ITS
5	61.62	ITS
10	59.81	ITS
20	57.55	ITS
30	56.18	ITS
40	54.98	ITS
50	53.97	ITS

Tabel 2. Nilai PSNR dan *Watermark* Terekstrak dengan Nilai Parameter *K*

Serangan Citra Terwatermark (<i>k=3</i>)	PSNR	<i>Watermark</i> Terekstrak
	25.38	ITS
Auto Level	25.38	ITS
	14.29	ITS
Clear	25.30	ITS

	16.74	ITS
--	-------	-----

Tabel 3. Nilai PSNR dan *Watermark* Terekstrak dengan Nilai Parameter *K* Berbeda

Parameter <i>K</i>	PSNR (dB)	<i>Watermark</i> Terekstrak
0.5	44.53	ARIS
1	44.52	ARIS
2	44.51	ARIS
3	44.46	ARIS
4	44.41	ARIS
5	44.31	ARIS

Tabel 4. Nilai PSNR dan *Watermark* Terekstrak dengan Nilai Parameter *K*

Serangan Citra Terwatermark (<i>k=4</i>)	PSNR	<i>Watermark</i> Terekstrak
Cropping	19.22	ARIS
Clear	18.78	ARIS

Tabel 3 menunjukkan hasil percobaan terhadap citra *grayscale* lenna dengan *watermark* "ARIS", dimana dilakukan proses *watermarking* ekstraksi *watermark*. Sama seperti pada citra RGB, untuk $K \geq 3$ mendapatkan *watermark* terekstrak hampir mirip dengan *watermark* asli. Akan tetapi memiliki kualitas yang menurun. Dari Tabel 4, terlihat juga bahwa dengan beberapa serangan

5. Penutup

Dari uji coba yang dilakukan dapat disimpulkan bahwa semakin besar nilai *K* yang digunakan akan menghasilkan kualitas citra terwatermark yang semakin menurun sehingga secara kasat mata tampak adanya perubahan pada *cover host*. Metode yang diusulkan juga menghasilkan citra terwatermark yang tahan terhadap serangan.

Referensi

- [1] Z. Wei, J. Dai, and J. Li., 2006. “Genetic *Watermarking* Based on DCT Domain Techniques”. **Canadian Conference on Electrical and Computer Engineering**, CCECE 06: 2365 - 2368.
- [2] B. Isac and V. Santhi., 2011. “A Study on Digital Image and Video *Watermarking* Schemes using Neural Networks”. **International Journal of Computer Application**, vol. 12: 1-6.
- [3] Langelaar, G. Setyawan, I. Legendijk, R.L., 2000. “*Watermarking* Digital Image And Video Data”. **IEEE Signal Processing Magazine**, Vol. 17: 20-43.
- [4] M. Rafigh and M.E. Moghaddam, 2010. “A Robust Evolutionary Based Digital Image *Watermarking* Technique in DCT Domain”. **2010 Seventh International Conference on Computer Graphics, Imaging and Visualization**, pp. 105-109.
- [5] G.-J. Lee, E.-J. Yoon, and K.-Y. Yoo, 2008. “A New LSB Based Digital *Watermarking* Scheme with Random Mapping Function”. **2008 International Symposium on Ubiquitous Multimedia Computing**, pp. 130-134.
- [6] M. Habib, S. Sarhan, and L. Rajab, 2005 “A Robust-Fragile Dual *Watermarking* System in the DCT Domain”. **Springer-Verlag Berlin Heidelberg**, pp. 548-553.
- [7] D. Salomon, 2007 “Data Compression: The Complete Reference”, **Springer, forth edition**.
- [8] Al-momen, Saad. E.Goerge, Loay, 2010. ”Image Hiding Using Magnitude Modulation on the DCT Coefficients”. **Journal of Applied Computer Science and Mathematics**, 8: 1-6.
- [9] P.-T. Yu, H.-H. Tsai, J.-S. Lin, 2001. ”Digital *watermarking* based on neural networks for color images”. **Signal Process.** **81 (3)** : 663–671.
- [10] Johnson, N.F. Katezenbeisser, S.C, 1999. “**A Survey of Steganographic Techniques**” in Information Techniques for Steganography and Digital *Watermarking*, S.C. Katezenbeisser et al., Eds. Northwood, MA: Artec House.
- [11] W. Na and W. Yunjin, 2009 “A Novel Robust *Watermarking* Algorithm based on DWT and DCT,” **2009 International Conference on Computational Intelligence and Security**