

ANALISA ROBUSTNESS CITRA DIGITAL PADA WATERMARKING DCT-DWT

Christy Atika Sari^{1*}, Titien Suhartini Sukamto² dan Eko Hari Rachmawanto¹

¹Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro

²Jurusan Sistem Infomasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Imam Bonjol 207, Kode Pos 50131, Semarang, Jawa Tengah

*Email: christy.atika.sari@dsn.dinus.ac.id

Abstrak

DCT dan DWT adalah domain frekuensi pada pengolahan citra digital yang sudah sering digunakan. Beberapa penerapan DCT-DWT dilakukan dengan tujuan perolehan aspek invisibility, robustness maupun pencapaian payload data. Pada penelitian sebelumnya, pengembangan DDCT-DWT telah dilakukan dengan menukar posisi aloritma namun belum menghasilkan output maksimal. Pada makalah ini, kami telah melakukan analisa robustness pada watermarking dengan mengimplementasikan filter haar pada DWT dengan oerasi pertama DCT terlebih dahulu. Level 2 pada DWT dipilih karena lebih invisible, sedangkan DCT menggunakan koefisien DC. Hasil program menyatakan nilai PSNR yang tidak terlalu tinggi namun tahan terhadap serangan. Hal ini dibuktikan dengan perhitungan NC yang lebih baik dari penelitian sebelumnya yang telah kami lakukan. Dalam penelitian ini, nilai NC yang diperoleh yaitu 1 pada citra tanpa serangan pengolahan citra, sedangkan CC tertinggi yang diperoleh yaitu 0.9449 pada serangan JPEG Compression. Sedangkan pada serangan salt and pepper dan gaussian noise nilai yang didapat berturut-turut yaitu 0.9217 dan 0.9342. Terdapat beberapa nilai CC dan NC yang sedikit berbeda dengan penelitian pembeding telah diulas pada makalah ini.

Kata kunci : DCT, DWT, watermarking, gambar

1. PENDAHULUAN

Mengunduh data melalui internet kemudian merubah data tersebut merupakan hal yang sering dilakukan netizen. Aktivitas semacam ini rentan terhadap keamanan data. Manipulasi dapat saja merugikan pihak pemilik data. Di dalam data yang dimanipulasi tersebut mungkin terdapat informasi atau pesan rahasia yang tidak boleh diketahui oleh orang lain. Apabila data tersebut diubah ke dalam bentuk lain, tentu pemilik data semakin dirugikan. Penyembunyian pesan melalui teknik tertentu terkadang menimbulkan kecurigaan baik dari hal penglihatan maupun pendengaran (Beker and Piper, 1982). Terdapat satu teknik yang dikenal dengan nama *watermarking*. Teknik ini dapat digunakan untuk mengubah suatu atau menyisipkan suatu pesan ke dalam media induk dengan tampilan akhir yang tidak terdeteksi oleh mata manusia. Biasanya teknik ini digunakan pada media citra digital. Beberapa fungsi watermarking sangat membantu dalam memecahkan masalah *tamper proofing*, *copyright protection* (Singh and Singh, 2017), *feature location*, *annotation*.

Dalam *watermarking* terdapat domain yang digunakan untuk proses penyisipan pesan yaitu domain frekuensi dan domain spasial. Komputasional pada domain spasial lebih cepat sehingga sering dipilih untuk menyisipkan data sederhana. Spasial domain unggul dalam kecepatan namun tidak tahan terhadap serangan pengolahan citra, sedangkan domain frekuensi lebih tahan serangan dan lebih lama dalam pemrosesan (Nana, 2016). Kedua domain dapat digunakan dalam proses kombinasi teknik misalnya pada steganografi dan enkripsi data. Algoritma dalam spasial domain antara lain *Least Significant Bit* (LSB), *Most Significant Bit* (MSB), *Pixel Value Defferencing* (PVD), serta *Chinese Remainder Theorem* (CRT). Beberapa contoh algoritma domain frekuensi yaitu *Discrete Cosine Transform* (DCT), *Discrete Wavelet Transform* (DWT), *Fourier Transform* (FT). Dibanding FF, DCT lebih cepat dan lebih robust khususnya pada jenis serangan kompresi citra. DWT juga dikenal *robust* terhadap serangan *noise*, *filtering*, *blurring*, dan *cropping*. Menurut Goswami, DWT-DCT diterapkan dalam teknik steganografi citra. Penelitian lain dengan algoritma DCT yang dihybrid dengan Kriptografi *One Time Pad* (OTP) juga telah dilakukan pada media citra digital (Goswami, 2016). Menurut Devi (Devi and Sujatha, 2015), DCT dalam eksperimennya digunakan untuk melakukan analisa kompresi gambar dengan serangan *JPEG Compression* dan hasilnya sangat memuaskan.

Berdasarkan keunggulan yang dimiliki oleh DCT dan DWT, serta kesamaan model operasi pada jenis domain frekuensi maka dalam makalah ini diusulkan kombinasi DCT-DWT pada teknik watermarking dengan tujuan *tamper proofing*. Untuk lebih jelasnya, hasil eksperimen telah dirangkum dan dibandingkan dengan penelitian lain.

2. METODOLOGI

2.1. Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) sering digunakan dalam *data hiding* dengan tujuan untuk kuantisasi citra, analisa serangan kompresi citra, maupun model optimisasi misalnya kombinasi dengan *Singular Value Decomposition* (SVD) atau *Particle Swarm Optimization* (PSO). DCT sangat tahan terhadap serangan *JPEG Compression* karena termasuk algoritma *lossy compression*. Secara umum, model operasi DCT dapat diilustrasikan pada persamaan (1).

$$\sum_{x=0}^{N-1} \sum_{y=0}^{M-1} \alpha(x) \cdot \alpha(y) \cdot f(x, y) \cdot \cos\left(\frac{\pi(2x+1)u}{2N}\right) \cos\left(\frac{\pi(2y+1)v}{2M}\right) \quad (1)$$

2.2. Discrete Wavelet Transform (DWT)

Algoritma *Discrete Wavelet Transform* (DWT) merupakan algoritma pemrosesan citra yang menggunakan perhitungan matematika sama seperti DCT. DWT mempunyai karakteristik pada model dekomposisi citra menjadi empat bagian (*subband*) yaitu LL, LH, HL, dan HH. Frekuensi L adalah *Low* dan H adalah *High*. DWT juga meruokan *orthogonal transform* dengan proses komputasi yang cepat.

3. HASIL PENELITIAN

Pada makalah ini, kombinasi DCT-DWT diimplementasikan pada kasus *tamper proofing*. Analisa kapabilitas DCT-DWT diuji dengan citra digital berukuran 512x512 piksel sebagai citra induk dan citra pesan pada 32x32 piksel. Dalam makalah ini, *robustness* citra diukur menggunakan *Cross Correlation* (CC) sesuai persamaan (2) dan *Normalized Correlation* (NC) sesuai persamaan (3).

$$CC = \frac{\sum_m \sum_n (X_{mn} - \bar{X})(Y_{mn} - \bar{Y})}{\sqrt{\sum_m \sum_n (X_{mn} - \bar{X})^2} \sqrt{\sum_m \sum_n (Y_{mn} - \bar{Y})^2}} \quad (2)$$

$$NC = \frac{1}{S_x T} \sum_{s=1}^S \sum_{t=1}^T \odot(s, t) x \odot_r(s, t) \quad (3)$$

Tabel 1. Perbandingan NC dan CC tanpa attack dengan penelitian lain

Nama Citra	NC			CC (dari metode usulan)
	Oleh Sari (Sari <i>et al.</i> , 2017)	Oleh Winarno (Winarno <i>et al.</i> , 2017)	Metode usulan (DCT-DWT)	
Lena.bmp	1	1	1	1

Berdasarkan Tabel 1, nilai NC yang didapat pada percobaan ini yaitu 1. Nilai NC=1 yaitu nilai sempurna dan membuktikan bahwa proses ekstraksi berhasil dan tidak menimbulkan bekas pada citra hasil watermark (Nambutdee and Airphaiboon, 2015). Nilai NC tanpa serangan pengolahan citra apapun yang didapat oleh metode yang diusulkan DCT-DWT ternyata sama dengan hasil NC pada penelitian terdahulu yang pernah dilakukan oleh Sari (Sari *et al.*, 2017) dan Winarno (Winarno *et al.*, 2017). Sedangkan untuk menganalisa hasil dengan pemberian serangan, dapat dilihat pada Tabel 2.

Pada Gambar 1, telah diilustrasikan perbandingan citra induk dan citra *watermark* pada citra lena.bmp yang digunakan untuk uji coba. Dapat dilihat bahwa hampir tidak terlihat adanya perbedaan diantara kedua citra tersebut. Hal ini menjadi bukti bahwa proses *tamper proofing* pada teknik *watermarking* DCT-DWT yang digunakan telah berhasil.



Citra induk asli

Citra watermark

Gambar 1. Perbandingan citra induk dan citra hasil watermarking DCT-DWT**Tabel 2. Perbandingan NC dan CC dengan attack pada citra lena.bmp**

Nama Serangan Pengolahan Citra	CC			NC		
	Oleh Al Haj (Al-Haj, 2007)	Oleh Susanto (Susanto <i>et al.</i> , 2017)	Metode yang diusulkan	Oleh Susanto (Susanto <i>et al.</i> , 2017)	Oleh Winarno (Winarno <i>et al.</i> , 2017)	Metode yang diusulkan
JPEG Compression (Q=50)	0.9650	0.9451	0.9477	0.7494	1.0000	0.9449
Salt and Pepper (0.01)	0.9473	0.8309	0.8731	0.8264	0.8825	0.9217
Gaussian Noise (0.002)	0.9878	0.7364	0.9184	0.8264	0.7844	0.9342

Nilai CC dan NC telah dikomparasi dan seperti dijabarkan pada Tabel 2, dapat dilihat bahwa penelitian lain yang dilakukan Al-Haj dengan implementasi DCT-DWT dengan model kuantisasi citra mendapatkan nilai CC yang tinggi. Sedangkan pada penelitian yang dilakukan oleh Susanto juga mendapatkan hasil tinggi. Untuk metode yang diusulkan juga menghasilkan nilai CC tinggi meski lebih rendah dibanding penelitian yang dilakukan oleh Al-Haj. Di sisi lain, nilai NC yang diperoleh metode usulan lebih tinggi pada jenis serangan *salt and pepper* serta *gaussian noise* jika dibandingkan hasil NC milik Susanto dan Winarno. Sedangkan nilai NC *JPEG Compression* metode yang diusulkan memang lebih rendah dibanding penelitian yang dilakukan oleh Winarno namun lebih tinggi dibanding hasil penelitian yang dilakukan oleh Susanto. Sehingga dapat disimpulkan bahwa metode usulan DCT-DWT memang robust dan dapat melakukan proses ekstraksi citra pesan dengan baik.

4. KESIMPULAN

Pada makalah ini, diusulkan metode kombinasi DCT-DWT pada teknik *watermarking* untuk tujuan *tamper proofing*. Proses *embedding* dan ekstraksi citra berhasil dilakukan dengan pad acitra sampel yaitu lena.bmp. Ukuran citra induk yaitu 512x512 piksel sedangkan citra pesan 32x32 piksel. Hasil penelitian pada makalah ini telah dikomparasi sesuai Tabel. 1 dan Tabel. 2 untuk merepresentasikan nilai NC dan CC baik dalam keadaan tanpa serangan maupun dengan serangan pengolahan citra. Jenis serangan yang dipilih yaitu *JPEG Compression* untuk membuktikan bahwa terdapat proses *lossy compression* dalam DCT, *salt and pepper* serta *gaussian noise* untuk membuktikan citra tahan pada serangan *noise addition*. Secara umum, hasil penelitian ini terbukti lebih *robust* dibanding penelitian sebelumnya yang dilakukan oleh Winarno dan Susanto dalam perolehan nilai CC dan NC citra pesan.

DAFTAR PUSTAKA

Al-Haj, A. (2007) 'Combined DWT-DCT Digital Image Watermarking', *Journal of Computer*

- Science*, 3(9), pp. 740–746.
- Beker, H. J. and Piper, F. C. (1982) ‘Communications security: a survey of cryptography’, *IEE Proceedings A Physical Science, Measurement and Instrumentation, Management and Education, Reviews*, 129(6), p. 357. doi: 10.1049/ip-a-1.1982.0063.
- Devi, R. and Sujatha, P. (2015) ‘An Overview of Digital Watermarking with a Performance Analysis of Wavelet Families for Image Compression’, *Indian Journal of Science and Technology*, 8(29), pp. 1–5. doi: 10.17485/ijst/2015/v8i29/85286.
- Goswami, A. (2016) ‘Coloured and Gray Scale Image Steganography using Block Level DWT DCT Transformation’, *International Journal of Computer Applications (0975 – 8887)*, 148(7), pp. 4–6.
- Nambutdee, A. and Airphaiboon, S. (2015) ‘Medical image encryption based on DCT-DWT domain combining 2D-DataMatrix Barcode’, in *2015 8th Biomedical Engineering International Conference (BMEiCON)*. IEEE, pp. 1–5. doi: 10.1109/BMEiCON.2015.7399508.
- Nana, Z. (2016) ‘Watermarking algorithm of spatial domain image based on SVD’, in *2016 International Conference on Audio, Language and Image Processing (ICALIP)*. IEEE, pp. 361–365. doi: 10.1109/ICALIP.2016.7846588.
- Sari, W. S. *et al.* (2017) ‘A Good Performance OTP Encryption Image based on DCT-DWT Steganography’, *TELKOMNIKA*, 15(4), pp. 1987–1995. doi: 10.12928/TELKOMNIKA.v15i4.5883.
- Singh, D. and Singh, S. K. (2017) ‘DWT-SVD and DCT based Robust and Blind Watermarking Scheme for Copyright Protection’, *Multimedia Tools and Applications*. Multimedia Tools and Applications, 76(11), pp. 13001–13024. doi: 10.1007/s11042-016-3706-6.
- Susanto, A. *et al.* (2017) ‘Hybrid method using HWT-DCT for image watermarking’, in *2017 5th International Conference on Cyber and IT Service Management, CITSM 2017*. doi: 10.1109/CITSM.2017.8089252.
- Winarno, A. *et al.* (2017) ‘Image Watermarking using Low Wavelet Subband based on 8x8 Sub-block DCT’, in *International Seminar on Application for Technology of Information and Communication*, pp. 11–15.