

Optimasi Keamanan *Watermarking* pada *Daubechies Transform* Berbasis *Arnold Cat Map*

Abdussalam¹, Eko Hari Rachmawanto^{2*}, Noor Ageng Setiyanto³, De Rosal Ignatius Moses Setiadi⁴, Christy Atika Sari⁵

^{1,2,3,4,5}Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro, Semarang
^{1,2,3,4,5}Jln. Imam Bonjol 207 Semarang, 50131, Indonesia

email: ²grey.salam@dsn.dinus.ac.id, ²eko.hari@dsn.dinus.ac.id, ³noor.ageng@dsn.dinus.ac.id, ⁴moses@dsn.dinus.ac.id,
⁵atika.sari@dsn.dinus.ac.id

Copyright ©2019, Politeknik Harapan Bersama, Tegal

Abstract – Digital image security using Transform Domain algorithms such as Discrete Wavelet Transform (DWT) has been widely used. To improve the security of the DWT algorithm needs to randomize the pixel coefficient, namely Arnold Cat Map (ACM). Computing ACM as one of the chaos functions is known to be fast and fits with Transform Domain. DWT has been implemented in the Daubechies filter which is the development of the Haar filter. In this paper, we proposed the message insertion model using a combination of DWT and ACM on a 512x512 piskel grayscale image and a 64x64 pixel message on the LL subband. The experiments were performed on 2 different images to determine the ability produced by the combined algorithm. The ability test for message insertion process is done through Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and comparison between original image histogram and image insertion histogram. While in the process of message extraction, algorithmic capability test is done by calculating Normalized Cross Correlation (NCC) and its correlation. The highest MSE result is 2.9502 and the highest PSNR is 43.4323 dB, while the NCC value is 237.3584 with correlation 0.7181.

Abstrak – Pengamanan citra digital menggunakan algoritma Transform Domain seperti Discrete Wavelet Transform (DWT) telah banyak digunakan. Untuk meningkatkan keamanan pada DWT perlu adanya algoritma dalam mengacak koefisien piksel, yaitu Arnold Cat Map (ACM). Komputasi ACM sebagai salah satu fungsi chaos diketahui cepat dan cocok dengan Transform Domain. DWT telah diimplementasikan pada filter Daubechies yang merupakan pengembangan dari filter Haar. Dalam makalah ini, di sajikan model penyisipan pesan menggunakan gabungan DWT dan ACM pada citra grayscale berukuran 512x512 piksel dan pesan 64x64 piksel pada subband LL. Percobaan dilakukan pada 2 buah gambar berbeda untuk mengetahui kemampuan yang dihasilkan oleh gabungan algoritma tersebut. Uji kemampuan pada proses penyisipan pesan dilakukan melalui perhitungan Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) dan komparasi antara histogram citra asli dengan histogram citra hasil penyisipan pesan. Sedangkan pada proses ekstraksi pesan, uji kemampuan algoritma dilakukan dengan menghitung Normalized Cross Correlation (NCC) dan korelasinya. Hasil MSE tertinggi yaitu 2.9502 dan PSNR tertinggi yaitu 43.4323 dB, sedangkan nilai NCC yaitu 237.3584 dengan korelasi 0.7181.

*) **Corresponding author:** (Eko Hari Rachmawanto)
Email: eko.hari@dsn.dinus.ac.id

Kata Kunci – Watermarking, Discrete Wavelet Transform, Filter Daubechies, Arnold Cat Map, Peak Signal to Noise Ratio.

I. PENDAHULUAN

Watermark atau tanda air dapat digunakan sebagai salah satu upaya untuk mengamankan data. Jenis data yang sering diamankan menggunakan teknik *watermarking* yaitu citra digital. Media berupa citra digital lebih rentan terhadap serangan misalnya replikasi dan manipulasi data. Teknik *watermarking* merupakan ilmu untuk mengamankan data [1], dimana media yang akan diamankan tidak akan berubah bentuk dan berubah tampilan seperti yang terjadi pada teknik kriptografi. Orang awam sering kali tidak menyadari bahwa citra digital yang di dapat dari media internet telah diamankan menggunakan teknik *watermarking*.

Teknik *watermarking* bukan hanya sekedar memberikan tanda air atau memberikan label tertentu pada tampilan media namun terdapat operasi khusus yang melibatkan algoritma tertentu dengan tujuan menambah keamanan pada media [2]. Menurut bentuknya, *watermarking* dibedakan menjadi *visible* dan *invisible watermarking*. *Visible watermarking* sudah jarang digunakan karena mudah dikenali, sedangkan *invisible watermarking* masih terus berkembang hingga saat ini.

Dalam teknik *watermarking*, terdapat satu atau lebih algoritma yang digunakan pada proses penyisipan maupun ekstraksi pesan. Beberapa contoh algoritma yang sering digunakan yaitu *Discrete Cosine Transform (DCT)* [3] dan *Discrete Wavelet Transform (DWT)*. DWT mempunyai karakter khusus dalam hal penyisipan pesan melalui koefisien *wavelet* dimana koefisien tersebut juga dapat digunakan pada proses rekonstruksi citra. Dalam hal kompresi citra, DWT juga tidak mempunyai distorsi yang terlalu tinggi dan DWT juga mempunyai *bit rate* yang rendah [4]. *Bit rate* merupakan perbandingan antara bit yang salah dan total bit yang disisipkan. Dengan adanya beberapa keunggulan yang dimiliki oleh DWT, maka DWT hasil penyisipan pesan terlihat lebih halus dan hampir tidak tampak oleh mata manusia.

Dalam makalah ini, DWT akan digunakan untuk melakukan penyisipan pesan. Hasil penyisipan DWT sudah bagus namun belum sempurna, sehingga untuk menyempurnakan diperlukan algoritma lain yang sesuai.

Peningkatan keamanan pada proses penyisipan dapat dilakukan dengan mengacak koefisien yang ada pada DWT. Proses pengacakan dapat menggunakan algoritma *Arnold Cat Map (ACM)* yang diketahui tidak merubah nilai piksel namun hanya mengacak saja [5]. Lain halnya ketika menggunakan algoritma *One Time Pad (OTP)* [6] dan *Rivest Shamir Adleman (RSA)* [7], dimana nilai piksel yang diacak akan berubah tempat dan berubah harga sehingga mempengaruhi nilai *Peak Signal to Noise Ratio (PSNR)* yang dihasilkan. ACM diketahui cepat dalam hal komputasi dan cocok digunakan pada jenis algoritma transform domain.

II. PENELITIAN YANG TERKAIT

Menurut Meharwade [8], teknik *watermarking* dapat dikombinasi dengan enkripsi data dimana algoritma *Discrete Cosine Transform (DCT)* telah berhasil dikombinasi dengan *Arnold Cat Map (ACM)* dengan tujuan untuk memperoleh keamanan ganda pada *copyright protection* dan mengurangi kompleksitas komputasi. Pada karya ilmiah tersebut, performa diuji dengan berbagai jenis perhitungan antara lain *Number of Pixels Change Rate (NPCR)* dan *Unified Average Changing Intensity (UACI)*, *Encryption Quality (EQ)*, *Mean Square Error (MSE)*, *Root Mean Square Error (RMSE)*, *Signal to Noise Ratio (SNR)*, *Peak Signal to Noise Ratio (PSNR)* dan *Similarity Factor (SF)*.

Menurut Al-Mokhtar [9], Video *watermarking* dalam penelitiannya direpresentasikan dengan menggabungkan 3-D DCT, 2D-DWT, *Arnold Cat Map* dan *Peano-Raster Scanning* untuk meningkatkan keamanan informasi dan menghasilkan informasi pada data multi-blok 8x8. Watermark yang digunakan yaitu citra biner dengan model pengujian menggunakan *Peak Signal to Noise Ratio (PSNR)*, *Mean Square Error (MSE)*, *Normal Cross Correlation (NCC)* and *Normalized Hamming Distance (NHD)*. Dalam penelitian ini DCT diimplementasikan pada DC koefisien untuk menyisipkan data, dimana hasil penyisipan juga di uji dengan beberapa bentuk noise seperti *speckle*, *median filter*, *gamma*, dan *posion* dimana nilai PSNR tertinggi yang didapatkan yaitu 39.2454 dB pada hasil proses cropping.

Menurut Rao [10] dalam penelitiannya melakukan uji performa pada DCT dan DWT yang dikombinasikan dengan *Arnold Cat Map* pada *Watermarking* citra grayscale. *Subband DWT* yang dipilih pada proses penyisipan yaitu *middle subband* LH dan HL yang hasilnya di inputkan pada setiap blok DCT menjadi koefisien baru. Pada proses ekstraksi citra, digunakan pra-penyaringan, proses penajaman citra dan operasi *Laplacian of Gaussian (LoG)* dengan tujuan mendapatkan informasi yang lebih baik dari citra host. Bit watermark tersebut kemudian diekstrak untuk membandingkan korelasi antara *PN-sequence* dan koefisien yang dihasilkan pada proses DWT-DCT diatas.

Menurut Singh [11], *Arnold Cat Map* telah diimplementasikan pada *blind watermarking* dengan DWT-SVD dan DCT. Dalam karya ilmiah ini, digunakan operasi *Mean Significant Bit (MSB)* dan *Least Significant Bit (LSB)*. Fungsi ACM dalam penelitian ini digunakan sebagai alat penyandian citra sebelum dilakukan penyisipan dengan DWT-SVD dan DCT. Hasil proses penyisipan diuji dengan MSE, PSNR sedangkan proses ekstraksi diuji dengan NCC. Terdapat setidaknya 30 jenis serangan yang digunakan untuk

membuktikan kehandalan kombinasi algoritma yang digunakan.

III. METODE PENELITIAN

A. Discrete Wavelet Transform (DWT)

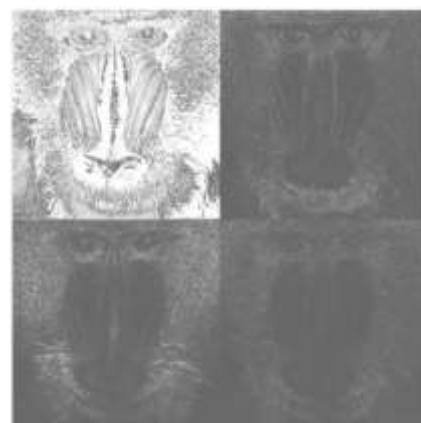
Tranformasi *Wavelet* menjadi salah satu alat penting dalam proses *watermarking* citra digital dengan sifat utamanya yaitu unggul dalam pemadatan energi. Dalam operasinya, DWT memecah setiap citra menjadi 4 bagian yang dikenal dengan nama *subband* yaitu LL, LH, HL dan HH. *Subband* HL dan LH diperoleh dengan *low pass filtering* satu arah dan *high pass filtering* ke arah lainnya. Pada setiap tingkat dekomposisi, besarnya koefisien DWT lebih besar dalam *subband* perkiraan (LL), dan lebih kecil untuk *subband* resolusi tinggi lainnya (HL, LH dan HH). *Subband* resolusi tinggi membantu dalam menemukan tepi dan pola tekstur gambar apa pun. Teknik *watermarking* berbasis DWT memungkinkan lokalisasi lokal yang baik dan memiliki karakteristik multi-resolusi, yang mirip dengan sistem visual manusia (HVS).

B. Daubechies Filter

Daubechies filter merupakan satu dari sekian filter yang dimiliki oleh *Wavelet Transform*. *Daubechies* merupakan model *orthogonal transform* yang dimiliki oleh *Wavelet* dengan pengembangan filter yang disebut dengan *Symlet*. Dalam *Daubechies*, terdapat 4 *subband* layaknya *Wavelet Transform* seperti pada Gbr 1.

Average / Lower Frequency (AF)	Horizontal / middle frequency (HF)
Vertical / middle frequency (VF)	Diagonal / Higher Frequency (DF) Figure

(a)



(b)

Gbr. 1 (a) Koefisien pada *Daubechies Transform*, (b) Representasi *subband* pada *Daubechies Transform* [12]

Dimana $h[n]$ adalah urutan respon impuls rendah-laluan koefisien filter dan $g[n]$ adalah urutan koefisien filter respons impuls *high-pass*, dan koefisiennya adalah:

$$\begin{aligned} h[0] &= (1+\text{SQRT}(3))/(4*\text{SQRT}(2)), \\ h[1] &= (3+\text{SQRT}(3))/(4*\text{SQRT}(2)), \\ h[2] &= (3-\text{SQRT}(3))/(4*\text{SQRT}(2)), \\ h[3] &= (1-\text{SQRT}(3))/(4*\text{SQRT}(2)), \\ g[0] &= h[3], g[1] = -h[2], g[2] = h[1] \text{ dan } g[3] = -h[0]. \end{aligned}$$

Inverse *Daubechies transform* (IDT) adalah operasi serupa dengan proses *Daubechies Transform*, di mana koefisien frekuensi diubah menjadi domain spasial untuk menghasilkan citra pada proses *embedding*.

C. Arnold Cat Map (ACM)

ACM sering digunakan pada teknik kriptografi. Teknik kriptografi hampir sama dengan *watermarking*, namun kriptografi fokus pada proteksi data [13] dimana hasil proses penyisipan menghasilkan citra yang rusak dan lebih mudah dikenali oleh mata manusia [14]. Untuk meningkatkan keamanan *watermarking*, maka citra harus diacak sebelum dimasukkan ke dalam citra *host* [7]. Di antara berbagai cara untuk pengacakan, pada makalah ini kami menggunakan *Arnold Cat Map (Arnold Transform)* yang merupakan proses berulang untuk memindahkan (mengacak) posisi piksel [15]. Dapat diasumsikan bahwa citra memiliki piksel $M \times N$, dimana $S = \{(x, y) | x, y = 0, 1, 2, \dots, N - 1\}$. Secara umum, Transformasi pada ACM dapat diilustrasikan pada Persamaan (1) berikut:

$$\begin{bmatrix} x_k \\ y_k \end{bmatrix} = \left\{ \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \right\}^K \quad (1)$$

Di mana X_k dan Y_k diubah menjadi koordinat yang sesuai dengan koordinat x dan y setelah K iterasi; N adalah tinggi atau lebar gambar persegi yang diproses; p dan q adalah bilangan bulat positif. Ini adalah proses berulang, jika lokasi (x, y) ditransformasikan beberapa kali kemudian kembali ke posisi semula setelah T iterasi. T ini disebut periode transformasi dan tergantung pada parameter p, q dan N . Parameter ini dapat digunakan sebagai kunci rahasia yang diperlukan untuk mendapatkan kembali gambar [16]. Jika pengacakan dilakukan dengan melakukan iterasi K , maka dapat memperoleh kembali gambar aslinya dengan melakukan $(T - K)$ iterasi.

Ada beberapa alasan untuk menggunakan ACM, antara lain [17]:

- Pemetaan adalah pemetaan satu-ke-satu; oleh karena itu, ada hubungan satu-ke-satu antara citra *plaintext* dan citra hasil operasi pengacakan untuk menghindari konflik posisi koordinat.
- ACM dua dimensi memiliki ruang kunci yang besar, dan struktur yang stabil.
- ACM membuat citra dapat dioperasikan secara komputasional dengan cepat.
- ACM sangat sederhana dan dapat dioperasikan melalui matriks.

IV. ALAT UJI PENELITIAN

A. Peak Signal to Noise Ratio (PSNR)

Dalam makalah ini, PSNR digunakan sebagai salah satu alat ukur karena mudah untuk dikomputasi dan dapat digunakan untuk mengukur kapasitas *watermark*. Nilai PSNR didapat dengan menghitung nilai *Mean Square Error (MSE)* terlebih dahulu. Berkembangnya algoritma dan media dalam model pengamanan data membuat pemenuhan terhadap nilai PSNR lebih tinggi, yaitu 40 dB sehingga dapat diterima dengan baik oleh mata manusia [18]. Hal ini berkaitan dengan standar nilai PSNR untuk gambar 8 bit yaitu antara 30 dB sampai 50 dB sesuai persamaan (2) dan persamaan (3) berikut.

$$MSE = \frac{1}{MN} \sum_{n=1}^M \sum_{m=1}^N [X'(n, m) - X(n, m)]^2 \quad (2)$$

$$PSNR = 10 \log_{10} \frac{MSE}{S^2} \quad (3)$$

Dimana nilai M dan N adalah besarnya kolom dan baris dari citra, X' adalah citra hasil sedangkan X adalah citra asli sebelum termanipulasi. S^2 merupakan nilai maksimal dari intensitas piksel citra yang diolah, misalnya 255.

B. Normalized Cross Correlation (NCC)

Pada proses ekstraksi pesan, uji performa dapat dilakukan dengan NCC. Nilai NCC digunakan untuk mengukur tingkat kekokohan citra ter*watermark* [19] sesuai persamaan (4) berikut.

$$NCC = \frac{W^{ij}_x W^{ij}_y}{W^{ij}_x W^{ij}_y} \quad (4)$$

Dimana W^{ij}_x dan W^{ij}_y adalah nilai piksel pada posisi (i, j) pada citra asli dan citra ter*watermark*.

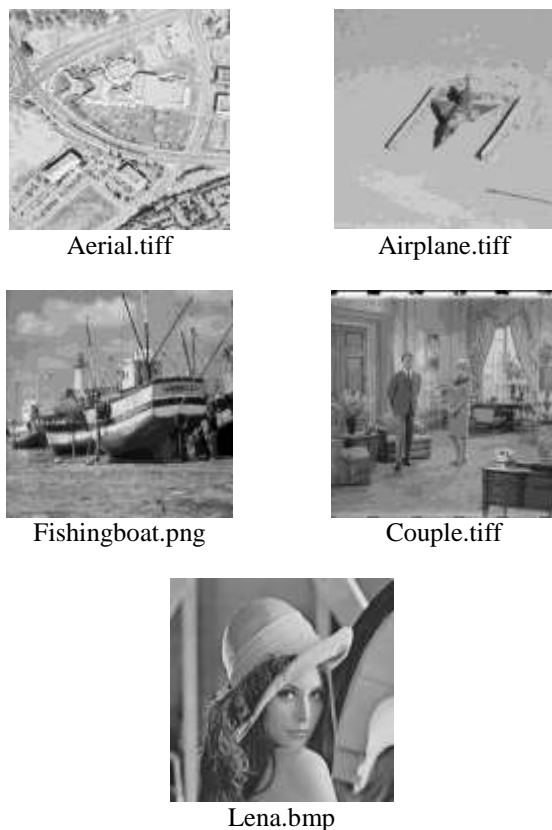
V. HASIL DAN PEMBAHASAN

Proses *watermarking* dilakukan dengan melakukan proses penyisipan pesan berupa citra 64x64 piksel biner ke dalam citra *host* 512x512 piksel *grayscale*. *Daubechies filter* yang digunakan yaitu pada *2D-Daubechies Filter (db1)* dengan posisi penyisipan dalam *subband LL3*.

Kami telah melakukan uji coba pada 5 buah citra *host* yang didapat dari *SIPI image database* seperti pada Gbr.2. Proses penyisipan telah berhasil dilakukan, sesuai *pseudocode* yang telah kami kembangkan berikut:

```
w_LL3=h_LL3+(enkrip*k);
w_LL2=idwt2(w_LL3,h_LH3,h_HL3,h_HH3,'db1');
w_LL=idwt2(w_LL2,h_LH2,h_HL2,h_HH2,'db1');
watermarked_image=idwt2(w_LL,h_LH,h_HL,h_HH,'db1');
```

Hasil proses penyisipan pada *Daubechies Transform* dengan model pengacakan piksel menggunakan ACM pada teknik kriptografi dapat diilustrasikan sesuai Tabel 1.



Gbr. 2 Citra Host

NE

Gbr. 3 Citra Pesan: ne.bmp

TABEL I
 UJI PERFORMA DAUBECHIES- ACM PADA PENYISIPAN PESAN

Nama Citra	MSE	PSNR (No Attack)
Lena.bmp	2.9502	43.4323
Couple.tiff	2.9452	43.4397
Aerial.tiff	2.9442	43.4411
Boat.tiff	2.9502	43.4323

Berdasarkan Tabel I, dapat disimpulkan bahwa pada seluruh citra yang digunakan untuk percobaan telah menghasilkan nilai PSNR lebih dari 40 dB. Dengan demikian hasil proses penyisipan pesan dapat diterima oleh sistem penglihatan manusia (HVS). nilai PSNR tertinggi yang didapatkan yaitu 43.4411 dB pada citra aerial.tiff. Sedangkan 3 buah citra lainnya mendapatkan PSNR yang sama yaitu 43.4323 Db. Melalui percobaan yang telah dilakukan, diketahui bahwa format citra dengan format *.bmp dan format *.tiff tidak berpengaruh terhadap proses penyisipan pesan. Untuk citra pesan yang digunakan yaitu citra biner berukuran 64x64 piksel sesuai Gbr 3.

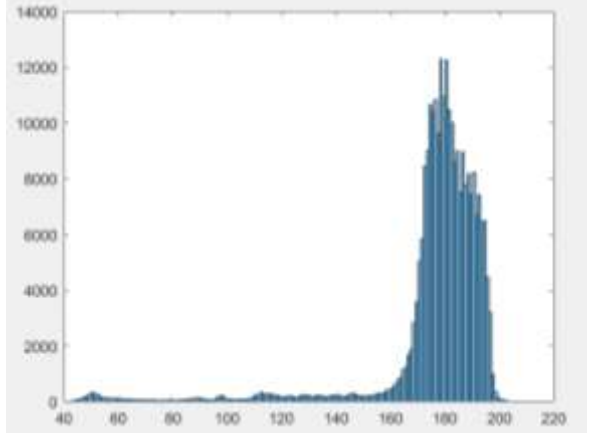
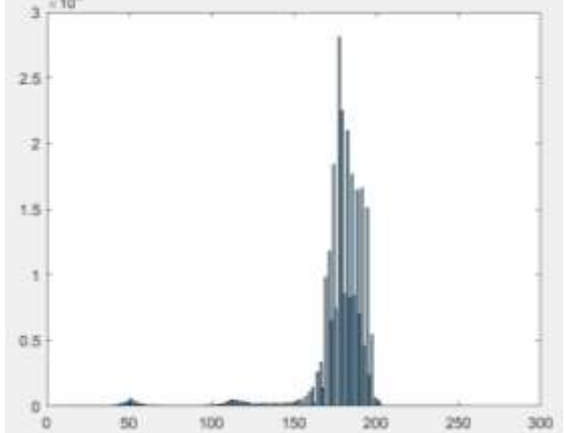
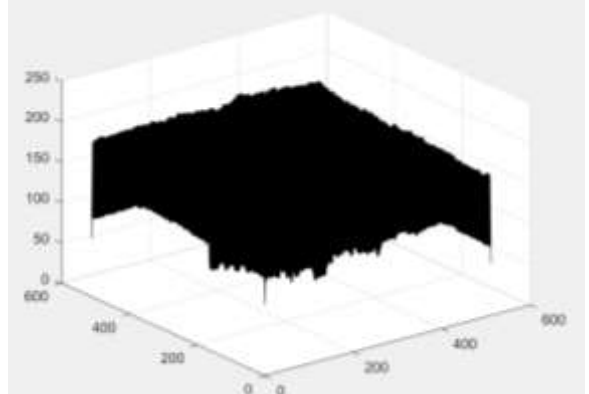
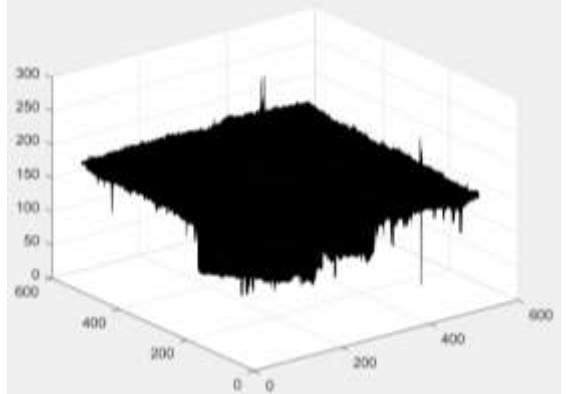
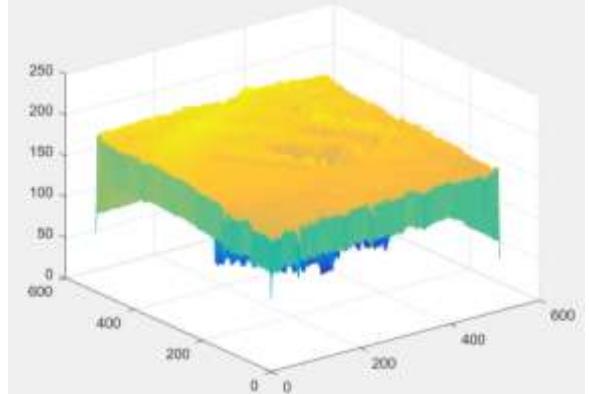
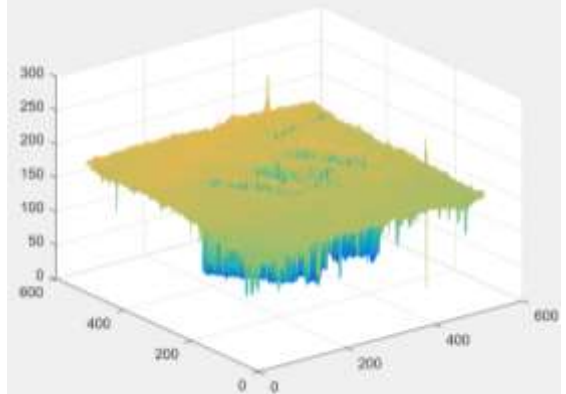
TABEL III
 JENIS SERANGAN YANG DIUJIKAN PADA CITRA WATERMARKING

Tanpa serangan	Salt and pepper	Gaussian Noise	JPEG Compression (Q=50)	JPEG Compression (Q=90)	Median Filtering





Pada Tabel II, citra hasil penyisipan pesan telah diuji performanya menggunakan berbagai serangan antara lain: *salt and pepper*, *Gaussian noise*, *rotasi*, *JPEG Compression* dengan $Q=50$ dan $Q=90$, *histogram equalization* dan *median filtering*. Dari seluruh citra yang diberikan serangan, semua citra membuktikan bahwa dengan serangan yang besar sekalipun citra tetap dapat terbaca oleh mata manusia. Biasanya, serangan *salt and pepper* digunakan pada nilai $a=0.001$, sedangkan pada penelitian ini kami menggunakan

nilai $a=0.5$ dan citra masih tetap dapat terbaca. Semakin besar nilai a maka sangat berpengaruh terhadap *imperceptibility* citra. Di sisi lain, pada serangan *JPEG compression* yang biasa dilakukan penelitian lain dengan $Q=50$ telah diuji coba pula. Dalam penelitian ini, citra hasil serangan *JPEG Compression* pada $Q=90$ ternyata masih tetap dapat dilihat oleh mata manusia. Untuk mengetahui perbedaan antara citra asli dan citra hasil ekstraksi pesan pada Tabel III telah diilustrasikan terjadinya sedikit perubahan pada piksel citra.

TABEL III
 SAMPLE PERBEDAAN CITRA ASLI DAN CITRA HASIL WATERMARKING PADA CITRA LENA

Keterangan	Citra Asli	Citra Hasil Ekstraksi
Histogram		
Surf		
Mesh		

TABEL IV
 HASIL EKSTRAKSI WATERMARK DAN PERHITUNGAN COOR PADA DAUBECHIES- ACM

Citra Host	No Attack	JPEG Compression (Q=50)	JPEG Compression (Q=90)	Median Filtering	Gaussian Noise	Salt and Pepper
Lena.bmp	NE 1.0000	NE 0.9710	NE 1.0000	NE 0.8557	 0.2172	NE 0.5669
Couple.tiff	NE 1.0000	NE 0.9658	NE 1.0000	NE 0.7756	 0.2149	NE 0.5196
Aerial.tiff	NE 1.0000	NE 0.9645	NE 1.0000	NE 0.6269	 0.2025	NE 0.5481
Boat.tiff	NE 1.00000	NE 0.9729	NE 1.0000	NE 0.7797	 0.1782	NE 0.5347

Pada Tabel IV, tampak bahwa hasil ekstraksi citra pesan ne.bmp telah berhasil diekstrak meskipun apabila diperhatikan kembali masih tampak adanya perbedaan terhadap piksel yang dihasilkan. Namun hal ini dapat dikategorikan bahwa proses ekstraksi pesan telah berhasil dilakukan. Ukuran piksel hasil ekstraksi juga tidak berubah, tetap pada 64x64 piksel biner.

VI. KESIMPULAN

Berdasarkan percobaan yang telah dilakukan dalam melakukan penyisipan citra pesan ke dalam *host* berupa citra menggunakan teknik *watermarking* berhasil kami lakukan. Beberapa penelitian terkait telah dilakukan dengan dengan *Discrete Cosine Transform (DWT)*. Untuk meningkatkan hasil *imperceptibility* citra, maka dalam penelitian ini kami mengoptimasi DWT dengan *Arnold Cat Map (ACM)*. ACM digunakan untuk mengacak piksel dalam proses penyisipan pesan melalui proses kriptografi. Hasilnya, seluruh citra menghasilkan nilai PSNR tinggi yaitu 43 dB sesuai Tabel I dan Tabel II. Pada proses ekstraksi dapat menghasilkan citra *host* dan citra pesan dengan baik ditandai dengan perubahan piksel yang tidak signifikan sesuai Tabel III, sedangkan ekstraksi citra pesan dapat dilihat pada Tabel IV. Citra pesan hasil ekstraksi tidak mengalami perubahan ukuran namun mengalami perubahan piksel.

DAFTAR PUSTAKA

[1] B. Wang, J. Ding, Q. Wen, X. Liao, and C. Liu, "An image watermarking algorithm based on DWT DCT and SVD," in *2009 IEEE International Conference on Network Infrastructure and Digital*

Content, 2009, pp. 1034–1038.

[2] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "A Good Performance OTP Encryption Image based on DCT-DWT Steganography," *TELKOMNIKA*, vol. 15, no. 4, pp. 1987–1995, 2017.

[3] A. Susanto, S. D.R.I.M., C. A. Sari, and E. H. Rachmawanto, "Hybrid Method using HWT-DCT for Image Watermarking," in *5th International Conference on Information Technology for Cyber and IT Service Management (CITSM 2017)*, 2017.

[4] G. Ardiansyah, C. A. Sari, D. Setiadi, and E. H. Rachmawanto, "Hybrid Method using 3-DES , DWT and LSB for Secure Image Steganography Algorithm," in *2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 2017, pp. 248–253.

[5] T. Pan and D. Li, "A Novel Image Encryption Using Arnold Cat," *Int. J. Secur. Its Appl.*, vol. 7, no. 5, pp. 377–386, 2013.

[6] N. Nagaraj and P. G. Vaidya, "One-Time Pad , Arithmetic Coding and Logic Gates : An Unifying Theme Using Dynamical Systems," pp. 1–9, 2008.

[7] R. D. Ardy, O. R. Indriani, C. A. Sari, D. R. Ignatius, and M. Setiadi, "Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5)," in *International Conference on Smart Cities, Automation & Intelligent Computing Systems*, 2017, pp. 1–6.

[8] H. S. Meharwade, S. Veena, and A. R. Shankar, "Joint encryption / watermarking based on Arnold cat map and DCT," *Int. J. Softw. Hardw. Res. Eng.*, vol. 3, no. 3, pp. 1–5, 2015.

[9] Z. T. Al-mokhtar, *High Security Video Watermarking Scheme Based on 3-D DCT and 2-D DWT with Arnold Map Algorithm*.

[10] D. V. N. K. Rao, Y. Madhuri, S. V. R. Kumar, and Y. V. S. Babu, "Robust Image Watermarking using DCT & Wavelet Packet Denoising," *Int. J. Sci. Eng. Res.*, vol. 3, no. 5, pp. 1–7, 2012.

[11] D. Singh and S. K. Singh, "DWT-SVD and DCT based Robust and Blind Watermarking Scheme for Copyright Protection," *Multimed. Tools Appl.*, vol. 76, no. 11, pp. 13001–13024, 2017.

[12] Rafael C. Gonzales, R. E. Woods, and Steven L. Eddins, *Digital image processing using MATLAB*, no. 2. 2014.

[13] E. J. Kusuma, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, "An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption," in *International Conference on Innovative and Creative Information Technology (ICITech)*, 2017, pp. 1–5.

- [14] N. Sharma, Prabhjot, and H. Kaur, "A Review of Information Security using Cryptography Technique.," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 4, pp. 323–326, 2017.
- [15] Y. Wu, S. Agaian, and J. P. Noonan, "A New Family of Generalized 3D Cat Maps," *arXiv:1205.3208*, pp. 1–10, 2012.
- [16] A. Waghmare, A. Bhagat, A. Surve, and S. Kalgutkar, "Chaos Based Image Encryption and Decryption," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 4, pp. 64–68, 2016.
- [17] C. Pradhan, V. Saxena, and A. K. Bisoi, "Imperceptible Watermarking Technique using Arnold's Transform and Cross Chaos Map in DCT Domain," *Int. J.*, vol. 55, no. October 2012, pp. 50–53, 2012.
- [18] J. Chandra and R. S. Wahono, "Integrasi Discrete Wavelet Transform dan Singular Value Decomposition pada Watermark ing Citra untuk Perlindungan Hak Cipta," *J. Intell. Syst.*, vol. 1, no. 2, pp. 127–135, 2015.
- [19] P. Singh, S. Shivani, and S. Agarwal, "A chaotic map based DCT-SVD watermarking scheme for rightful ownership verification," in *2014 Students Conference on Engineering and Systems*, 2014, pp. 1–4.