PENGACAKAN CITRA DIGITAL BERWARNA DENGAN KRIPTOGRAFI *ARNOLD CAT MAP* (*ACM*)

Noor Ageng Setiyanto, Eko Hari Rachmawanto[*] dan De Rosal Ignatius Moses Setiadi
Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Imam Bonjol 207, Kode Pos 50131, Semarang, Jawa Tengah
[*]Email: eko.hari@dsn.dinus.ac.id

Abstrak

Implementasi kriptografi dalam konteks watermarking masih jarang digunakan. Untuk menghasilkan keamanan citra yang lebih tinggi, terdapat fungsi chaos dalam kriptografi yang dapat diterapkan pada pengacakan piksel citra digital. Fungsi chaos merupakan salah satu fungsi pengacak bilangan. Dalam makalah ini kami mengevaluasi implementasi Arnold Cat Map (ACM) pada konsep non blind watermarking pada citra digital berwarna. Penggunaan ACM akan berakibat pada distorsi perubahan piksel citra, namun kami akan memodifikasi fungsi ACM sehingga tetap dapat memenuhi aspek imperceptibility melalui histogram citra yang membutktikan tidak terjadinya perubahan piksel secara signifikan. Evaluasi dilakukan dengan melakukan analisa pada hasil enkripsi dengan iterasi berbeda yaitu 10, 50 dan 100 iterasi. Ukuran citra yang digunakan beragam, hal ini di lakukan dengan tujuan pembuatan simpulan terhadap proses enkripsi. Dari percobaan, ACM mengacak citra pada masing-masing ietrasi dengan baik. Proses ini menggunakan fungsi modulo dan telah diimplementasikan dengan Matlab.

Kata kunci : *Arnold Cat Map (ACM), kriptografi, citra warna*

1. PENDAHULUAN

Model enkripsi sering kali diaitkan dengan model kemanan data. Enkripsi merupakan salah satu tahapan dari proses kriptografi, dimana tahapan lain disebut dengan dekripsi. Enkripsi dilakukan untuk melakukan perubaan bentuk pada plainteks menuju cipherteks yang acak dan tidak dapat dibuka oleh orang lain. Konsep enkripsi telah dilakukan sejak zaman yunani kuno menggunakan alat yang disebut *scytale*. Saat ini, kriptografi banyak diterapkan untuk proteksi media citra digital. Salah satu bentuk citra digital yaitu citra berwarna. Untuk mengenkripsi citra berwarna, diketahui lebih sulit dibanding citra grayscale.

Fungsi chaos sebagai salah satu algoritma dalam kriptografi telah diterapkan dalam mengubah posisi citra atau melakukan pengacakan piksel namun nilai dalam piksel tersebut tidak berubah. Fungsi chaos dikategorikan sebagai *pseudo-random number* atau pembangkit bilangan acak. Fungsi tersebut sangat aman untuk dilakukan. Orang lain tidak memahami model perubahan posisi pada citra yang dioperasikan. Fungsi chaoes mempunyai banya cabang, antara lain *logistic map*, *baker map*, *Arnold Cat Map* (ACM). Menurut (Meharwade, Veena and Shankar, 2015), ACM telah diterapkan pada kombinasi kriptografi dan watermarking pada algoritma *Discrete Cosine Transform* (DCT) dan ACM dalam melakukan penyembunyian citra berwarna yang dikomparasi dengan performa algoritma *Advanced Encryption Standard* (AES). *Arnold Cat Map* sebagai salah satu bentuk dari discrete chaotic map yang dilakukan dengan menghitung nilai modulo. Parameter dalam ACM digunakan sebagai kunci dalam enkripsi data.

Berdasarkan pada keunggulan yang dimiliki oleh Arnold Cat Map (ACM), maka dalam penelitian ini akan di lakukan proses enkripsi dan dekripsi citra digital. Dalam penelitian ini, hasil enkripsi dan dekripsi di analisa menggunakan histogram dan lama waktu tempuh operasi.

2. ARNOLD CAT MAP (ACM)

Dalam beberapa tahun terakhir, karena seringnya proses pengiriman citra digital melalui internet (Filler and Fridrich, 2010), telah menjadi penting untuk mengamankan citra dari manipulasi data. Perlu adanya skema pengamanan data salah satu nya menggunakan Arnold Cat Map (ACM), dimana enkripsi dan dekripsi citra menjadi sangat aman. ACM menghasilkan nilai enkripsi yang aman dan efisien serta sangat cepat untuk dilakukan. Dalam kriptosistem ini, arsitektur permutasi-difusi diikuti dengan skema difusi yang efisien (Waghmare *et al.*, 2016). Skema ini terdiri dari dua prosedur difusi, dengan prosedur difusi lain setelagh tahap difusi normal.

Dalam modul difusi tambahan, parameter kontrol dari AM yang dipilih telah diubah oleh citra resultan yang dihasilkan setelah operasi difusi normal. Model operasi pada ACM dapat dilihat persamaan (1) berikut.

$$\begin{bmatrix} F'_x \\ F'_y \\ F'_z \end{bmatrix} = \left(\begin{bmatrix} 1 & a & b \\ c & ac+1 & bc \\ d & abcd & bd+1 \end{bmatrix} \begin{bmatrix} F_x \\ F_y \\ F_z \end{bmatrix} \right) \bmod(N) \quad (1)$$

Dari persamaan (1), nilai *a, b, c, d* dan *e* adalah bilangan bulat positif, F_x dan F_y adalah posisi piksel asli sedangkan F'_x dan F'_y adalah posisi piksel orak-arik. F_z adalah parameter *temp* dan F'_z adalah nilai piksel orak-arik. Teknologi enkripsi citra yang berbasis pada chaos adalah teknologi enkripsi kode yang telah berkembang dalam beberapa tahun terakhir. Fungsi ini melihat citra asli sebagai aliran data biner yang sesuai dengan beberapa mode yang dikodekan, lalu mengenkripsi gambar dengan menggunakan sinyal. Alasan bahwa Chaos cocok dengan enkripsi gambar terkait erat dengan beberapa karakteristik dinamiknya. Sinyal chaos memiliki penyembunyian alami, sensibilitas tinggi terhadap kondisi awal dan gerakan perturbasi yang kecil sekalipun, yang membuat sinyal chaos memiliki kemampuan baik (Keshari, 2011). Keamanan sistem enkripsi ini bergantung pada tingkat aproksimasi antara sinyal dan bilangan acak yang dihasilkan oleh generator arus kunci rahasia. Aliran kunci rahasia mendapatkan keamanan yang lebih tinggi saat mendekati angka acak, padahal mudah dipecahkan. Peta logistik adalah contoh di antara persamaan nonlinier yang dapat diterapkan pada penelitian matematik eksperimen dengan penuh kemenangan (Waghmare *et al.*, 2016). Meski sederhana, bisa mewujudkan semua sifat fenomena nonlinier seperti terlihat pada persamaan (2).

$$X_{n+1} = f(\mu, X_n) = \mu X_n (1 - X_n) \quad (2)$$

Dimana, $\mu \in (3.57, 4, Xn \in (0,1)$. Jika $\mu = 4$ maka sistem dalam keadaan kacau, dan urutan yang dihasilkan sistem sekarang memiliki karakteristik keacakan, dan kepekaan sensibilitas terhadap nilai asli yaitu (0, 1). Semua karakteristik ini dapat memberikan hasil yang sangat baik untuk operasi enkripsi gambar.

3. HASIL PENELITIAN DAN PEMBAHASAN

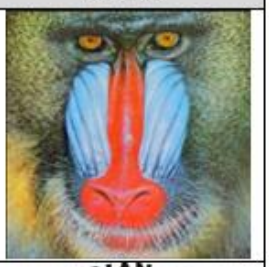
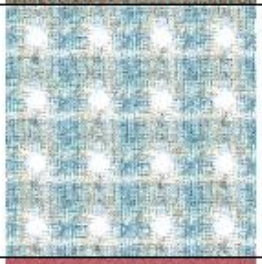
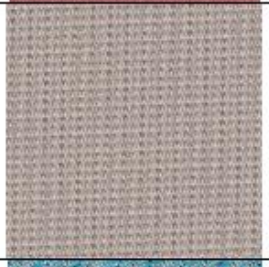
Dalam penelitian ini, skema ACM diterapkan dengan citra berwarna pada citra berwarna dengan ukuran beragam. Citra tersebut dalam format bmp, jpg, dan png. Dalam ekperimen, ACM dilakukan pada tiga buah jumlah iterasi berbeda yaitu 10, 50 dan 100 iterasi. Pada Gambar 1 telah diilustrasikan skema implementasi ACM pada citra berwarna yang diterapkan. Sedangkan Gambar 2 merupakan citra implementasi.

Gambar 1. Citra untuk implementasi

Berdasarkan hasil eksperimen, secara visual hasil implementasi pengacakan piksel citra dapat dilihat pada Tabel 1.

ISBN 978-602-99334-9-9

Tabel 1. Tampilan hasil enkripsi dan dekripsi citra pada iterasi 100

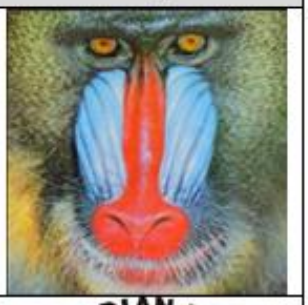
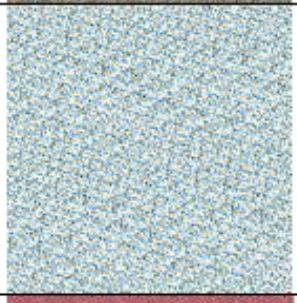
Nama Citra	Citra asli	Enkripsi	Dekripsi
Babbon			
Udinus			
Lena			
noor			
eko			

```
red1=img(:,:,1);
green1=img(:,:,2);
blue1=img(:,:,3);
tic
%enkripsi
p=1; q=1; jumlah_iterasi=100;
M=[1 p; q p*q+1];
for iter=1:jumlah_iterasi
    for x=1:N
        for y=1:N
            hasil=mod(M*[x;y], N);
            red2(x,y)=red1(hasil(1)+1, hasil(2)+1);
            green2(x,y)=green1(hasil(1)+1, hasil(2)+1);
            blue2(x,y)=blue1(hasil(1)+1, hasil(2)+1);
        end
    end
    red1=red2;
    green1=green2;
    blue1=blue2;
end
```

Gambar 2. Skema ACM yang digunakan pada coding Matlab

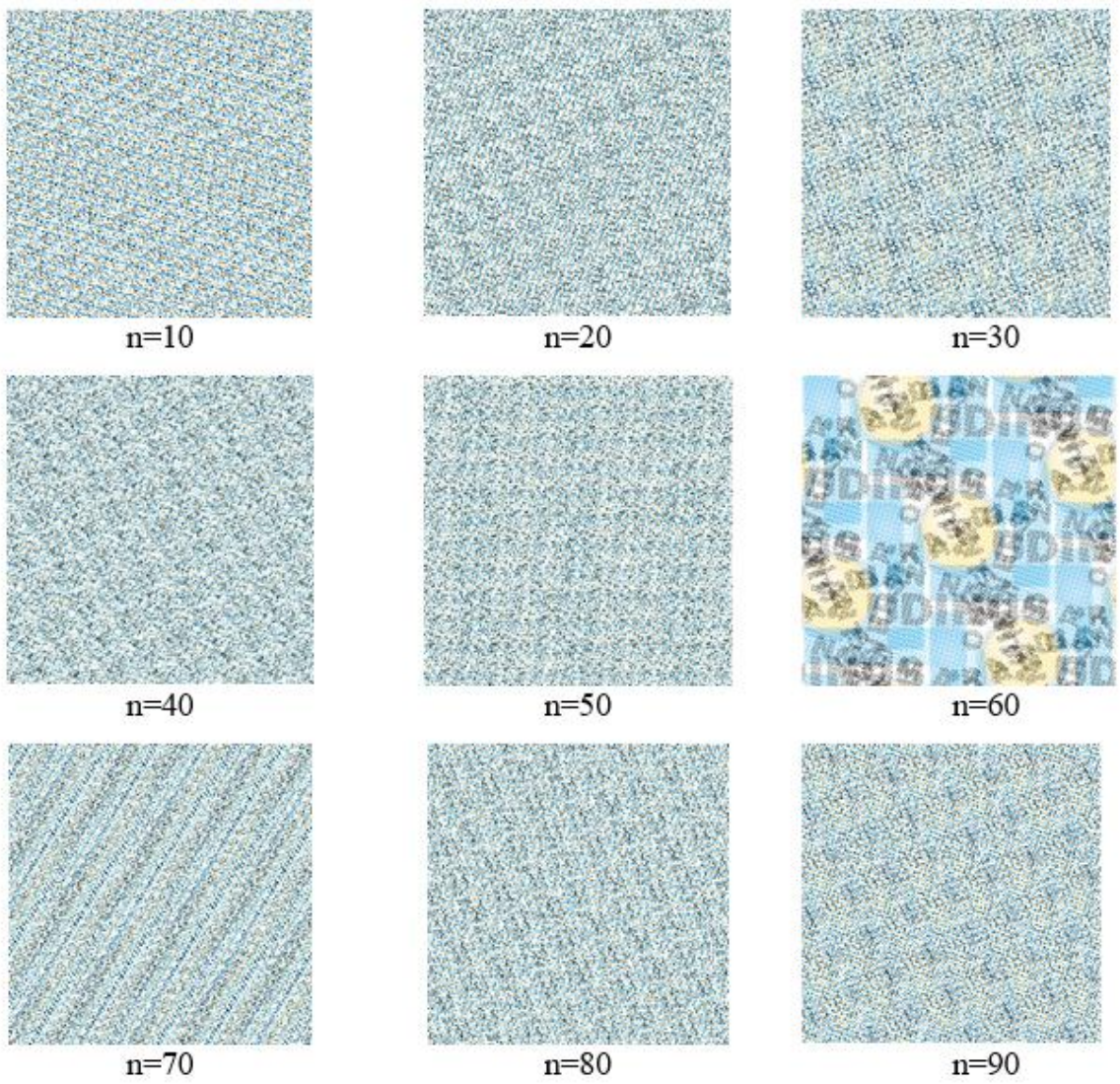
Untuk menganalisa lebih dalam, pada Tabel 2 telah diimplemnetasikan hasil enkripsi dekripsi citra pada jumlah iterasi = 10. Dengan mengguankan ietrasi yang sedikit saja, ternyata ACM dapat mengcak citra dengan baik, bahkan citra tersebut tidak dapat dikenali secara kasat mata.

Tabel 2. Tampilan hasil enkripsi dan dekripsi citra pada iterasi 10

Nama Citra	Citra asli	Enkripsi	Dekripsi
Babbon			
Udinus			
Lena			
noor			
eko			

ISBN 978-602-99334-9-9

Dapat dilihat bahwa pada Tabel 2, hasil pengacakan citra tetap tidak terlihat meskipun apabila dibandingkan dengan Tabel 1 masih jauh berbeda. Pada jumlah iterasi = 10, citra enkripsi tetap dalam keadaan acak. Berikut ini pada citra 'Uidnus' dengan ukuran 300 x 300 piksel telah dilkakukan komparasi hasil enrkripsi pada jumlah iterasi berbeda seperti pada Gambar 3.



Gambar 3. Perbandingan visualisasi enkripsi dengan ACM pada jumlah iterasi *(n)* berbeda

Berdasarkan Gambar 3, dapat dilihat perubahan hasil pengacakan piksel sesuai dengan jumlah iterasi yang digunakan. Pada jumlah iterasi = 60, hasil enkripsi lebih menyerupai citra asli sedangkan pada jumlah iterasi lainnya telah acak sepenuhnya dan tidak dapat dikenali lagi bentuk asli dari citra yang dioperasikan.

4. KESIMPULAN

Kriptografi simteris dengan model pengacakan piksel citra telah selesai diimplementasikan. Hasil enkripsi pada sejumlah iterasi berbeda juga menghasilkan visualisasi citra berbeda. Dalam makalah ini, 5 buah citra berbeda format dan berbeda ukuran terlah dikaji. Secara khusus, pada citra 'Udinus' telah diuji menggunakan iterasi mulkai dari 10 sampai 100. Komparasi ini dilakukan untuk mengetahui model dan pola pengacakan piksel pada hasil visualisasi citra hasil enkripsi. Bagi penelitian selanjutnya, ACM dapat digunakan untuk proses verifikasi citra digital khususnya pada topik digital signature.

DAFTAR PUSTAKA

Al-Haj, A. (2007) 'Combined DWT-DCT Digital Image Watermarking', *Journal of Computer Science*, 3(9), pp. 740–746.

Filler, T. and Fridrich, J. (2010) 'Steganography using Gibbs random fields', in *Proceedings of the 12th ACM workshop on Multimedia and security - MM&Sec '10*. New York, New York, USA: ACM Press, p. 199. doi: 10.1145/1854229.1854266.

Keshari, S. (2011) 'Image Encryption Algorithm based on Chaotic Map Lattice and Arnold cat map for Secure Transmission', *IJCST*, 2(2), pp. 132–135.

Meharwade, H. S., Veena, S. and Shankar, A. R. (2015) 'Joint encryption / watermarking based on Arnold cat map and DCT', *International Journal of Software & Hardware Research in Engineering*, 3(3), pp. 1–5.

Munir, R. (2012) 'Algoritma Enkripsi Citra Digital Berbasis Chaos Dengan Penggabungan Teknik Permutasi Dan Teknik Substitusi Menggunakan Arnold Cat Map Dan Logistic Map', in *Seminar Nasional Pendidikan Teknik Informatika (SENAPATI 2012)*, pp. 107–124.

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.

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.

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.

Waghmare, A. *et al.* (2016) 'Chaos Based Image Encryption and Decryption', *International Journal of Advanced Research in Computer and Communication Engineering*, 5(4), pp. 64–68. doi: 10.17148/IJARCCE.2016.5417.

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.

ISBN 978-602-99334-9-9