

Dekomposisi dan Rekombinasi Pengacakan Citra Digital dengan *Logistic Mapping*

Steven¹, Ivan Audris², Vanessa Priscilla Wijaya³, Ng Poi Wong⁴, Wenripin Chandra⁵,
STMIK Mikroskil, Jl. Thamrin No. 112, 124, 140, Telp. (061) 4573767, Fax. (061) 4567789
Program Studi Teknik Informatika, STMIK Mikroskil, Medan
161110153@students.mikroskil.ac.id, 161110382@students.mikroskil.ac.id,
161110889@students.mikroskil.ac.id, poiwong@mikroskil.ac.id, wenripin@mikroskil.ac.id

Abstrak

Beberapa citra digital membutuhkan privasi dan kerahasiaan, seperti citra medis, citra diagnosa medis jarak jauh, citra rahasia melalui komunikasi internet, atau citra rahasia kemiliteran. Salah satu cara untuk mengamankan informasi di dalam citra digital adalah dengan melakukan pengacakan (*scrambling*).

Penelitian ini mengacak nilai piksel citra digital dengan mengubah nilai piksel dari sistem bilangan desimal menjadi bilangan basis empat (*kuartener*), kemudian mengurai (*dekomposisi*) keempat bit *kuartener* dan melakukan pengacakan terhadap keempat posisi bit berdasarkan pada bilangan acak yang dihasilkan oleh algoritma *logistic mapping*, kemudian bit hasil pengacakan digabungkan kembali (*rekombinasi*) untuk menghasilkan nilai piksel baru. *Logistic mapping* merupakan penghasil bilangan acak yang mampu menghasilkan deretan bilangan yang acak berdasarkan nilai kunci μ ($3.569945 < \mu < 4$) dan nilai awal x_0 ($0 < x_0 < 1$).

Hasil penelitian ini dapat melakukan pengacakan terhadap citra digital dengan dekomposisi dan rekombinasi nilai piksel berdasarkan pada nilai acak yang dihasilkan oleh algoritma *logistic mapping*. Hasil pengujian menunjukkan bahwa pasangan kunci-1 (μ_1, x_1) memiliki sensitivitas paling tinggi dalam mengacak citra, kemudian diikuti oleh pasangan kunci-2 (μ_2, x_2), pasangan kunci-3 (μ_3, x_3) dan pasangan kunci-4 (μ_4, x_4).

Kata kunci— citra digital, dekomposisi, *logistic mapping*, rekombinasi

Abstract

Some digital images require privacy and confidentiality, such as medical images, remote medical diagnostic images, secret images via internet communications, or secret military images. One of information securing for digital images is scrambling.

This research scrambling the pixel value of the digital image by changing the pixel value from the decimal number system to the quaternary number system, then decomposes the four quaternary bits and scrambling the four bits position based on the random numbers generated by the logistic mapping algorithm, then the scrambling bits result are recombined to generate a new pixel value. Logistic mapping is a random number generator capable of generating random numbers based on the key value μ ($3.569945 < \mu < 4$) and the initial value x_0 ($0 < x_0 < 1$).

The results of this research can perform digital images scrambling with pixel value decomposition and recombination based on random values generated by a logistic mapping algorithm. The test results shown the key-1 pair (μ_1, x_1) have the highest sensitivity in scrambling the image, then followed by the key-2 pair (μ_2, x_2), the key-3 pair (μ_3, x_3) and the key-4 pair (μ_4, x_4).

Keywords— decomposition, digital images, *logistic mapping*, recombination

1. PENDAHULUAN

Citra digital memiliki peranan yang penting dalam teknologi multimedia untuk menyajikan informasi dalam bentuk visual. Beberapa bidang implementasi citra digital membutuhkan privasi dan kerahasiaan, seperti citra medis, citra diagnosa medis jarak jauh, komunikasi internet, dan komunikasi di bidang militer [1]. Citra rahasia perlu diproteksi agar informasi visual yang terdapat pada citra tidak dapat diketahui oleh pihak lain yang tidak berkepentingan dan hanya dapat diakses oleh orang-orang tertentu.

Logistic Mapping merupakan salah satu algoritma penghasil bilangan acak yang sederhana dan banyak digunakan sebagai bahan pengujian untuk ide-ide baru dalam teori pengacakan serta aplikasi chaos dalam ilmu kriptografi [9]. Steganografi citra dengan *Mode-Based Least Significant Bit* berdasarkan kemunculan nilai piksel terbanyak (modus) dari citra digital menghasilkan PSNR > 60 dB dan MSE < 1 [3]. Enkripsi citra berdasarkan *Random Scrambling* dan *Chaotic Logistic Map* terhadap sejumlah citra grayscale dan berwarna menunjukkan hasil yang bagus dengan tingkat deviasi rata-rata sebesar 0,89626 dan rata-rata koefisien korelasi sebesar 0,268 [10]. Pengacakan citra digital dengan *Logistic Map* dan *Piecewise Linear Chaotic Map* dengan hanya memanfaatkan parameter λ dari *Logistic Map* menghasilkan pengacakan citra paling baik secara visual dengan MSE sebesar 9496,75862, dan dengan parameter p dari *Piecewise Linear Chaotic Map* menghasilkan pengacakan citra paling baik secara visual dengan MSE sebesar 9803,35705 [11].

2. TINJAUAN PUSTAKA

Citra digital adalah citra yang dapat diolah oleh komputer dan merupakan citra yang dihasilkan oleh peralatan digital. Citra digital dapat diproses oleh komputer karena terdapat sistem sampling dan kuantisasi di dalam peralatan digital [12]. Sebuah citra digital dapat didefinisikan sebagai sebuah fungsi dua dimensi, $f(x,y)$ dimana x dan y adalah koordinat bidang (spasial), dan amplitudo dari setiap pasangan koordinat (x,y) dinamakan sebagai intensitas citra pada titik tersebut. Istilah level keabuan mengacu pada intensitas dari citra monokrom, sedangkan citra berwarna menggunakan sistem warna RGB yang memuat tiga citra komponen individual, yaitu red, green dan blue. Hasil dari proses sampling dan kuantisasi adalah matriks yang membuat nilai-nilai riil dan dianggap sebagai representasi dari citra digital. [13].

Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan atau informasi yang dikirim dari satu tempat ke tempat lain [2]. Beberapa implementasi dari kriptografi seperti steganografi yakni ilmu dan seni menyembunyikan pesan rahasia sedemikian hingga keberadaan pesan tidak terdeteksi oleh indera manusia [3], atau generator bilangan acak yang dapat menghasilkan deretan nilai acak yang tidak dapat diprediksi secara keseluruhan [4].

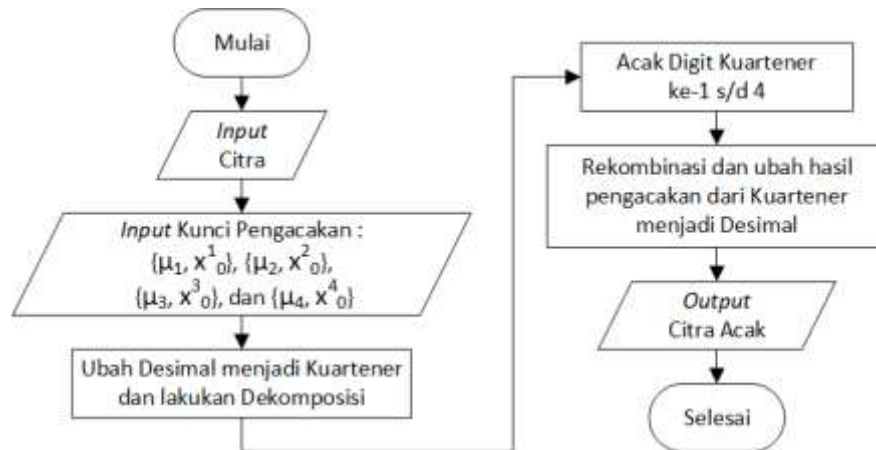
Pengacakan (*scrambling*) adalah salah satu cara untuk mengamankan informasi di dalam citra digital [5]. Terdapat beberapa teknik dalam pengacakan citra digital yang secara umum dibagi menjadi dua kategori. Kategori pertama adalah mengacak posisi piksel (*spatial domain*) yang dapat dilakukan dengan menggunakan *Arnold Transformation* [6] dan *Baker Transformation* [7]. Kategori kedua adalah mengacak nilai piksel citra dengan menggunakan *Pseudo Random Number Generator* [8]. Teknik ini mengacak nilai piksel dengan menggunakan operasi XOR antara nilai piksel dan hasil bilangan acak yang merupakan output dari *Pseudo Random Number Generator* [8].

3. METODE PENELITIAN

Penelitian ini mengacak nilai piksel citra dengan mengubah posisi spasial piksel dan kemudian mengacak nilai piksel. Pengacakan citra dilakukan dengan mengurai (dekomposisi) nilai piksel, kemudian melakukan pengacakan terhadap posisi bit hasil dekomposisi, kemudian bit hasil pengacakan digabungkan kembali (rekombinasi) untuk menghasilkan nilai piksel baru. Proses pengacakan posisi bit hasil dekomposisi menggunakan algoritma *Logistic Mapping*. *Logistic mapping* mampu menghasilkan deretan bilangan yang acak berdasarkan nilai kunci μ ($3.569945 < \mu < 4$) dan nilai awal x_0 ($0 < x_0 < 1$). Penelitian ini mengubah nilai piksel dari sistem bilangan desimal menjadi bilangan basis 4, atau disebut juga dengan bilangan kuarterner (*quaternary*), kemudian pengacakan mengubah posisi ke-4 bit bilangan

kuartener antara piksel berdasarkan pada deretan bilangan acak yang dihasilkan oleh *Logistic Mapping*, sehingga nilai piksel akan berubah secara keseluruhan. Dikarenakan pengacakan dilakukan pada 4 set bilangan kuartener, maka nilai kunci yang dibutuhkan juga berjumlah 4 set yaitu $\{\mu_1, x^1_0\}$, $\{\mu_2, x^2_0\}$, $\{\mu_3, x^3_0\}$, dan $\{\mu_4, x^4_0\}$.

Proses dari dekomposisi dan rekombinasi citra digital dengan *Logistic Mapping* dapat dilihat pada gambar 1 berikut.



Gambar 1 *Flowchart* proses dekomposisi dan rekombinasi citra digital dengan *Logistic Mapping*

Pengacakan dilakukan pada 4 set *digit* bilangan kuartener, sehingga nilai kunci yang dibutuhkan juga berjumlah 4 set, yaitu $\{\mu_1, x^1_0\}$, $\{\mu_2, x^2_0\}$, $\{\mu_3, x^3_0\}$ dan $\{\mu_4, x^4_0\}$. Nilai kunci dapat ditentukan secara manual atau dihasilkan secara acak. *Range* nilai kunci μ dibatasi antara nilai 3.569945 sampai 4, sedangkan nilai kunci x dibatasi antara nilai 0 sampai 1.

Nilai piksel dari citra input diubah menjadi matriks 1 dimensi $p(t)$ dengan diambil mulai dari RGB piksel pertama (kiri atas) citra digital, kemudian berlanjut ke piksel di sampingnya, lalu turun ke baris berikutnya dan berlanjut hingga piksel terakhir (kanan bawah). Bentuk matriks nilai piksel dapat dilihat pada tabel 1 berikut.

Tabel 1 Sampel Data Hobi dari 6 *User*

Matriks ke- (t)	Nilai Matriks $p(t)$
0	133
1	96
2	67
3	133
4	97
dstnya	dstnya

Berikutnya adalah mengubah nilai piksel dari bentuk desimal ke bilangan kuartener (bilangan basis 4), sebagai contoh $p(0) = (133)_{10}$ menjadi bilangan kuartener bernilai $(2011)_4$. Lakukan proses konversi untuk semua nilai matriks $p(t)$ dan dekomposisi menjadi 4 set *digit* berdasarkan pada bilangan kuartener, yaitu $r_1(t)$, $r_2(t)$, $r_3(t)$, dan $r_4(t)$. Hasil dekomposisi dapat dilihat pada tabel 2 berikut.

Tabel 2 Hasil dekomposisi piksel citra *input*

Matriks ke-(t)	Nilai Matriks $p(t)$		Dekomposisi (<i>Digit ke-1 s/d 4</i>)			
	Desimal	Kuartener	$r_1(t)$	$r_2(t)$	$r_3(t)$	$r_4(t)$
0	133	2011	2	0	1	1
1	96	1200	1	2	0	0
2	67	1003	1	0	0	3
3	133	2011	2	0	1	1
4	97	1201	1	2	0	1
dstnya	dstnya	dstnya	dstnya	dstnya	dstnya	dstnya

Berikutnya dilakukan pengacakan ke-4 *digit* kuartener hasil dekomposisi dengan menggunakan bilangan acak x dari algoritma *Logistic Mapping*. Untuk pengacakan *digit ke-1* bilangan kuartener $r_1(t)$ menggunakan kunci-1, yakni μ_1 dan x^1_0 , kemudian dilakukan proses perhitungan bilangan acak dengan *Logistic Mapping* berdasarkan persamaan berikut.

$$x_{k+1} = f(x_k) = \mu x_k (1 - x_k) \quad (1)$$

Bilangan acak yang dihasilkan oleh *Logistic Mapping* (10 desimal di belakang koma) berdasarkan pada kunci-1, misalnya $\mu_1 = 3.7580$ dan $x^1_0 = 0.52345$ adalah sebagai berikut:

$$x_0 = 0.52345$$

$$k = 0 \rightarrow x_1 = \mu x_0 (1 - x_0)$$

$$x_1 = 3.7580 * 0.52345 * (1 - 0.52345)$$

$$x_1 = 0.9374334664$$

$$k = 1 \rightarrow x_2 = \mu x_1 (1 - x_1)$$

$$x_2 = 3.7580 * 0.9374334664 * (1 - 0.9374334664)$$

$$x_2 = 0.220414075$$

$$k = 2 \rightarrow x_3 = \mu x_2 (1 - x_2)$$

$$x_3 = 3.7580 * 0.220414075 * (1 - 0.220414075)$$

$$x_3 = 0.6457435682$$

dstnya

Sehingga diperoleh hasil nilai acak *digit-1* seperti tabel 3 berikut.

Tabel 3 Nilai acak *digit-1* ($\mu_1 = 3.7580$ dan $x^1_0 = 0.52345$)

t	<i>Digit-1</i> $r_1(t)$	$x(t)$
0	2	0.5234500000
1	1	0.9374334664
2	1	0.2204140750
3	2	0.6457435682
4	1	0.8596756167
dstnya	dstnya	dstnya

Berikutnya dilakukan pengurutan $x(t)$ secara *ascending*, sehingga nilai $r_1(t)$ menjadi ikut teracak, seperti tabel 4 berikut. Apabila terdapat nilai $x(t)$ yang sama, maka proses akan mendahulukan nilai t yang lebih kecil.

Tabel 4 Hasil pengacakan *Digit-1* atau $r_1'(t)$

t	$x(t)$	t (sebelumnya)	<i>Digit-1</i> $r_1'(t)$
0	0.2198250599	18	2

1	0.2204140750	2	1
2	0.2403782685	7	1
3	0.2446961783	23	0
4	0.2912369532	12	2
dstnya	dstnya	dstnya	dstnya

Setelah ke-4 digit bilangan kuarterner dilakukan pengacakan dan diperoleh hasil pengacakan $r_1'(t)$, $r_2'(t)$, $r_3'(t)$, dan $r_4'(t)$, maka berikutnya dilakukan proses rekombinasi ke-4 digit hasil pengacakan, kemudian dikonversi kembali menjadi bilangan desimal. Proses rekombinasi dan perubahan ke bilangan desimal dapat dilihat pada tabel 5 berikut.

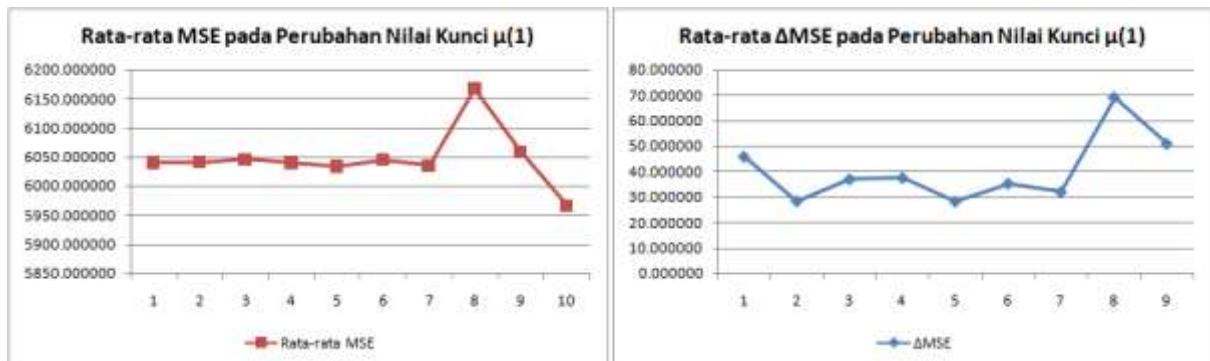
Tabel 5 Hasil rekombinasi

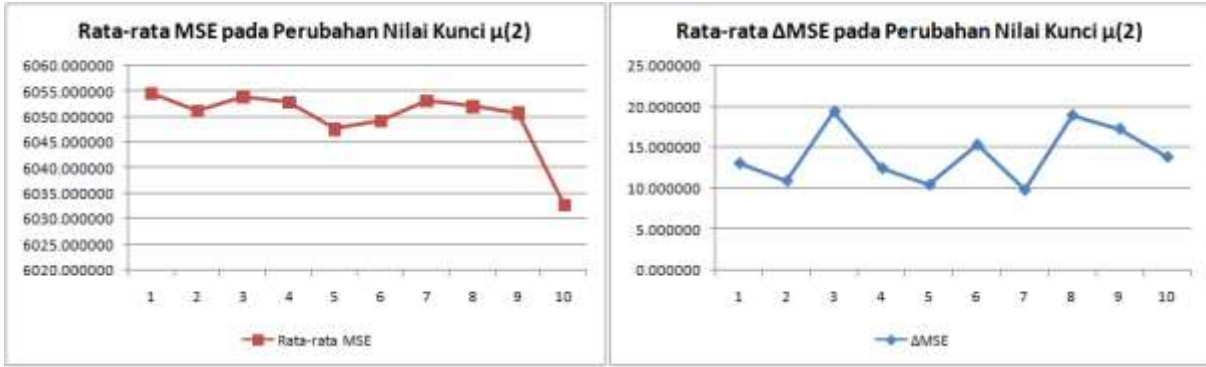
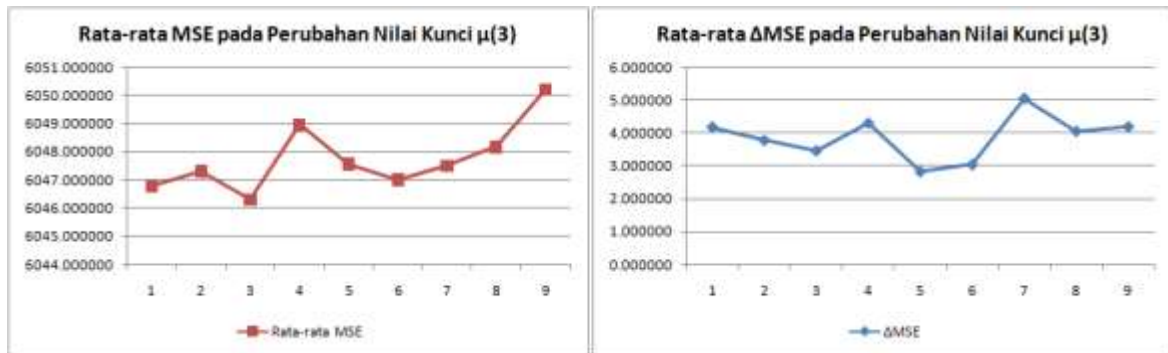
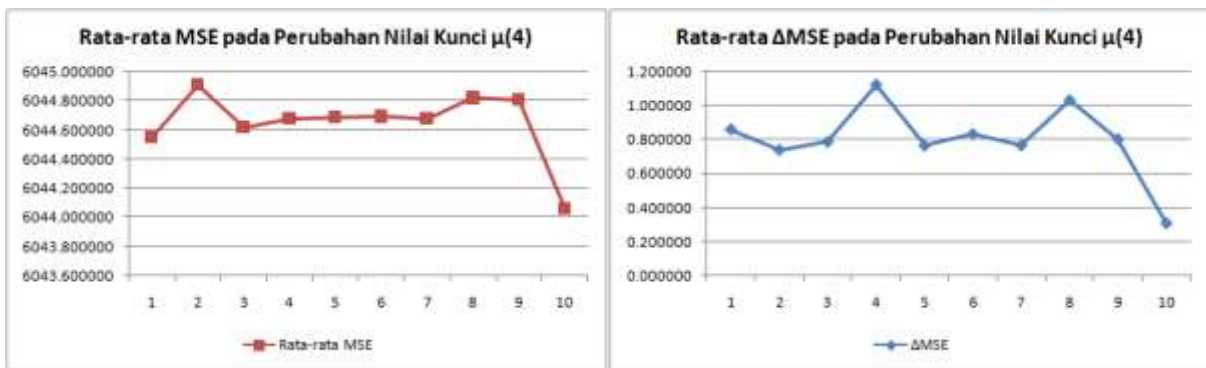
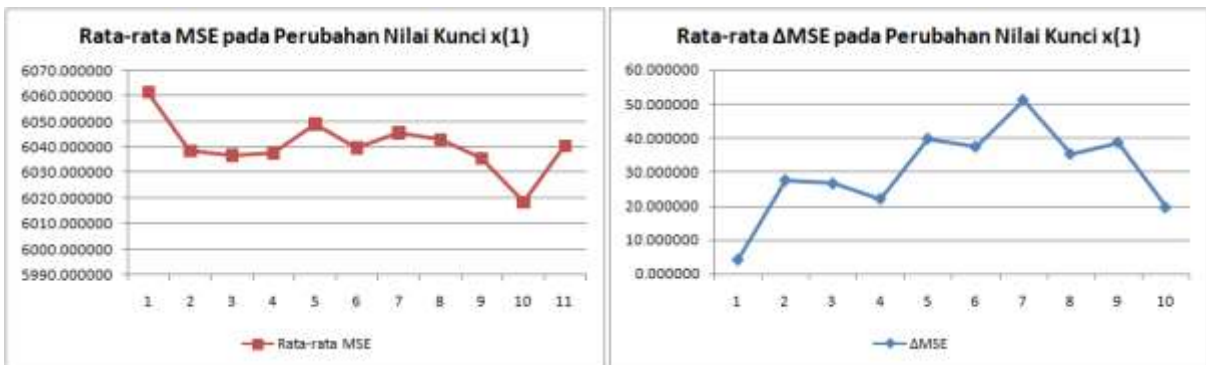
Matriks ke-(t)	Hasil Pengacakan (Kuartener)				Nilai Matriks $p'(t)$	
	Digit-1 $r_1'(t)$	Digit-2 $r_2'(t)$	Digit-3 $r_3'(t)$	Digit-4 $r_4'(t)$	Rekombinasi (Kuartener)	Desimal
0	2	0	0	1	2001	129
1	1	1	0	1	1101	81
2	1	2	0	1	1201	97
3	0	0	1	2	0012	6
4	2	2	0	1	2201	161
dstnya	dstnya	dstnya	dstnya	dstnya	dstnya	dstnya

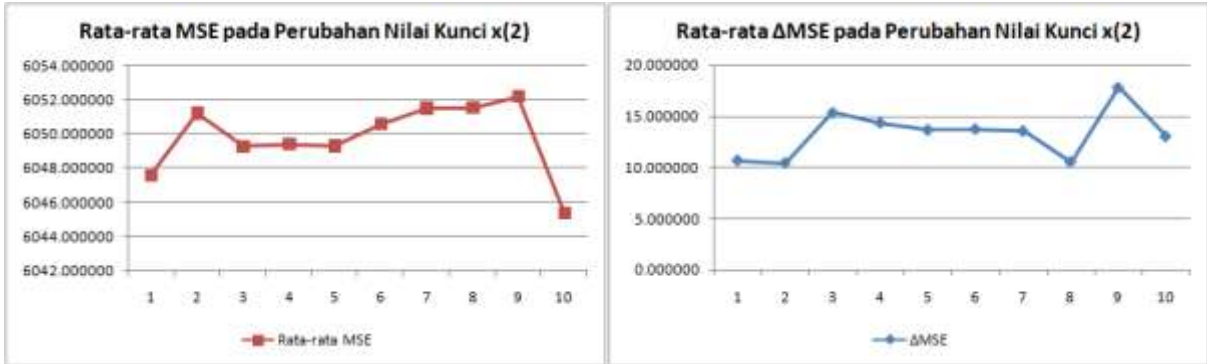
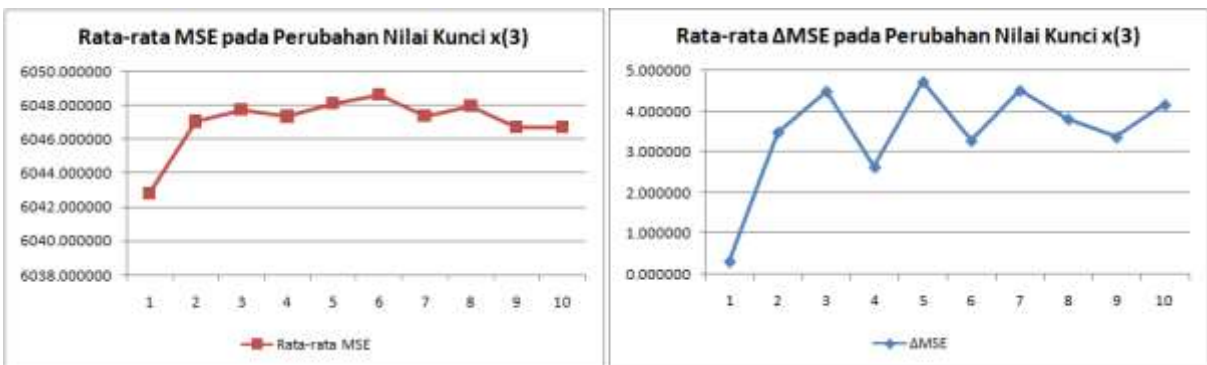
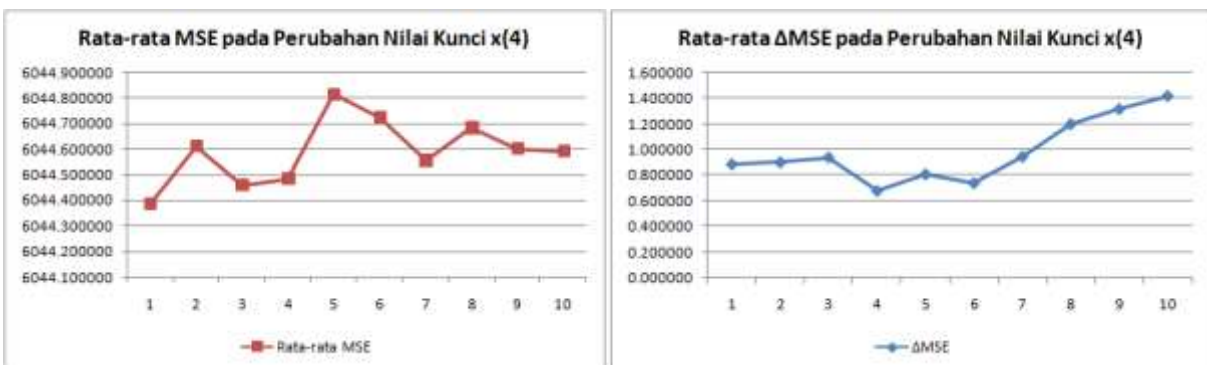
Dari hasil rekombinasi di atas, nilai matriks $p'(t)$ berupa desimal kemudian disusun kembali menjadi nilai piksel RGB dan menghasilkan *output* berupa citra acak.

4. HASIL DAN PEMBAHASAN

Hasil penelitian ini dilakukan pengujian terhadap pengaruh kunci $\mu_1, \mu_2, \mu_3, \mu_4, x_1, x_2, x_3$, dan x_4 terhadap MSE dengan dilakukan penambahan nilai kunci (*increment*) sebesar +0.0000000001, +0.0000000010, +0.0000000100 hingga +0.1000000000, dengan masing-masing tahapan penambahan nilai (*increment*) dilakukan sebanyak 20 iterasi, dengan kunci μ berada di antara nilai 3.569945 sampai 4, dan kunci x berada di antara nilai 0 hingga 1. Bila nilai kunci berada di luar *range*, maka pengujian tidak dilakukan dan iterasi dihentikan. Setelah itu, dilakukan rekapitulasi data dengan menghitung nilai rata-rata MSE dari semua iterasi, serta menghitung nilai rata-rata fluktuasi MSE (Δ MSE) pada setiap tahap *increment*. Berikut adalah grafik hasil pengujian pengaruh kunci $\mu_1, \mu_2, \mu_3, \mu_4, x_1, x_2, x_3$, dan x_4 terhadap MSE.

Gambar 2 Grafik hasil pengujian pengaruh kunci terhadap μ_1 MSE

Gambar 3 Grafik hasil pengujian pengaruh kunci terhadap μ_2 MSEGambar 4 Grafik hasil pengujian pengaruh kunci terhadap μ_3 MSEGambar 5 Grafik hasil pengujian pengaruh kunci terhadap μ_4 MSEGambar 6 Grafik hasil pengujian pengaruh kunci terhadap x_1 MSE

Gambar 7 Grafik hasil pengujian pengaruh kunci terhadap x_2 MSEGambar 8 Grafik hasil pengujian pengaruh kunci terhadap x_3 MSEGambar 9 Grafik hasil pengujian pengaruh kunci terhadap x_4 MSE

Dari hasil pengujian pengaruh kunci μ_1 , μ_2 , μ_3 , μ_4 , x_1 , x_2 , x_3 , dan x_4 terhadap MSE, jika direkapitulasi nilai rata-rata MSE dan Δ MSE untuk semua nilai kunci, maka akan diperoleh data pengujian seperti tabel 6 berikut.

Tabel 6 Rekapitulasi nilai rata-rata MSE dan Δ MSE hasil pengujian

Perubahan Nilai Kunci	Rata-rata MSE	Rata-rata Δ MSE
Perubahan pada kunci μ_1	6047.722182	40.576446
Perubahan pada kunci μ_2	6049.838520	14.189133
Perubahan pada kunci μ_3	6047.758009	3.874230
Perubahan pada kunci μ_4	6044.653294	0.802902
Perubahan pada kunci x_1	6040.710160	30.184122
Perubahan pada kunci x_2	6049.802148	13.332765

Perubahan pada kunci x_3	6047.025957	3.476530
Perubahan pada kunci x_4	6044.591579	0.982330

5. KESIMPULAN

Dari penelitian ini dapat dihasilkan beberapa kesimpulan sebagai berikut :

1. Hasil pengujian membuktikan bahwa penambahan nilai pada salah satu variabel kunci, walaupun hanya sebesar +0.0000000001, mampu menghasilkan citra acak dengan nilai MSE hampir sama dengan nilai MSE hasil pengacakan menggunakan penambahan nilai kunci yang lebih besar, misalnya + 0.1.
2. Penambahan nilai kunci pada variabel kunci tidak berhubungan dengan kenaikan nilai MSE, karena pengacakan *Logistic Mapping* dilakukan berdasarkan pada nilai kunci dan tidak bergantung pada besarnya nilai kunci. Nilai kunci yang berbeda, walaupun hanya sebesar 0.0000000001 akan menghasilkan pengacakan yang berbeda pula.
3. Pasangan kunci-1 (μ_1, x_1) memiliki sensitivitas paling tinggi dalam mengacak citra, kemudian diikuti oleh pasangan kunci-2 (μ_2, x_2) dan pasangan kunci-3 (μ_3, x_3). Pasangan kunci-4 (μ_4, x_4) memiliki sensitivitas paling rendah. Hal ini dikarenakan pasangan kunci (μ_1, x_1) mengacak digit-1 kuartener yang merupakan bit paling berpengaruh (*Most Significant Bit*), sedangkan perubahan pada variabel kunci (μ_4, x_4) menghasilkan perbedaan nilai MSE paling kecil karena variabel kunci (μ_4, x_4) mengacak *digit-4* kuartener yang merupakan bit paling tidak berpengaruh (*Least Significant Bit*).

6. SARAN

Dari penelitian ini, dapat diberikan saran untuk penelitian lebih lanjut, yakni dapat dilakukan penelitian terhadap prinsip integritas data dan autentikasi terhadap citra digital yang telah diacak dengan algoritma *Logistic Mapping*.

DAFTAR PUSTAKA

- [1] Das, D. dan Lanjewar, U. A., 2012, Realistic Approach of Strange Number System from Unary to Decimal, *International Journal of Computer Technology and Applications (IJCTA)*, Vol. 3, Issue 1, 235-241.
- [2] Mukhtar, H., 2018, Kriptografi untuk Keamanan Data, Deepublish, Yogyakarta.
- [3] Wong, N. P., Hardy, Megawan, S., dan Andri, 2019, Steganography using Mode-Based Least Significant Bit (MBLSB) Method, *Fourth International Conference on Informatics and Computing (ICIC)*, Semarang, Indonesia, 1-3.
- [4] Sanjaya, M. B., dan Telnoni, P. A., 2015, Implementasi Blum-Blum-Shub dan Chaotic Function untuk Modifikasi Key Generating pada AES, *Jurnal Elektro Telekomunikasi Terapan (JETT)*, Vol. 2, No. 2, 154-165.
- [5] Wang, D., Chang, C. C., Liu, Y., Song, G., dan Liu, Y. 2015, Digital Image Scrambling Algorithm Based on Chaotic Sequence and Decomposition and Recombination of Pixel Values, *International Journal of Network Security (IJNS)*, Vol. 17, No. 3, 322-327.
- [6] Bireki, M. F. M. E., Abdullah, M. F. L., Ukasha, A. A. M., dan Elrowayati, A. A., 2016, Digital Image Watermarking Based On Joint (DCT-DWT) and Arnold Transform, *International Journal of Security and Its Applications*, Vol. 10, No. 5, 107-118.
- [7] Liu, Z., 2018, Comparative Evaluations of Image Encryption Algorithms, *Tesis*, Degree of Master of Computer and Information Sciences, Auckland University of Technology, School of Engineering, Computer and Mathematical Sciences.
- [8] Wang, Y., Liu, Z., dan Ma., J., 2015, A pseudorandom number generator based on piecewise logistic map, *An International Journal of Nonlinear Dynamics and Chaos in Engineering Systems*, Springer,

Vol. 83, 2373-2391.

- [9] Awad, A., dan Saadane, A., 2010, New Chaotic Permutation Methods for Image Encryption, *IAENG International Journal of Computer Science*, Vol. 37, Issue 4.
- [10] Yadav, S. S., dan Singh, Y., 2018, Image Encryption Based on Random Scrambling and Chaotic Logistic Map, *International Journal of Grid and Utility Computing (IJGUC)*, Vol. 9, No. 3, 228-234.
- [11] Andrew, Andrian, Kuantan, S., Setia, R., dan Christnatalis, 2019, Pengacakan Citra Digital dengan Menggunakan Logistic Map dan Piecewise Linear Chaotic Map, *Jurnal Teknik, Kesehatan dan Ilmu Sosial*, Vol. 1, No. 1, 96-102.
- [12] Andono, P. N., Sutojo, T., dan Muljono, 2017, Pengolahan Citra Digital, Andi Offset, Yogyakarta.
- [13] Sianipar, R. H., 2018, Dasar Pemrosesan Citra Digital dengan MATLAB, Andi Offset.

