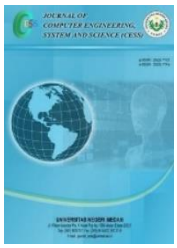
CESS
(Journal of Computing Engineering, System and Science) July 2022 470-481

e-ISSN: 2502-714x
p-ISSN: 2502-7131

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: https://jurnal.unimed.ac.id/2012/index.php/cess



Penerapan Metode Arnold *Cat Map* dan *Logistic Map* untuk Pengamanan Citra Data Penduduk

Application Of Arnold Cat Map and Logistic Map Methods for Securing Citizens' Data Image

Thomas Adi Putra[1], Ikhwan Ruslianto[2], Syamsul Bahri[3*]
[1,2,3]Jurusan Rekayasa Sistem Komputer, Fakultas MIPA Universitas Tanjungpura
Jl. Prof. Dr. H. Hadari Nawawi, Bansir Laut, Kec. Pontianak Tenggara, Kota Pontianak, Kalimantan Barat 78124
email: [1]thomas_adi_putra@student.untan.ac.id, [2]ikhwanruslianto@siskom.untan.ac.id, [3]syamsul.bahri@siskom.untan.ac.id

Submitted: 30 Juni 2022 | Revision: 19 Juli 2022 | Accepted: 29 Juli 2022

A B S T R A K

Keamanan data merupakan salah satu isu yang sangat penting terutama untuk data yang bersifat pribadi baik dalam bentuk tulisan maupun citra. Penerapan kriptografi dapat digunakan untuk mengamankan data agar tidak dapat dimengerti oleh sembarang orang. Pada penelitian ini dilakukan pengamanan data berupa citra KTP dan citra KK menggunakan metode Arnold *Cat Map* dan *Logistic Map*. Pada pengujian sensitivitas kunci, diperoleh bahwa perubahan kunci dekripsi sebesar 0,0001 dari kunci enkripsi menghasilkan citra yang sangat berbeda dengan citra asal. Pada pengujian analisis diferensial diperoleh nilai rata-rata NPCR dan UACI untuk citra KTP sebesar 99,60745% dan 39,50400% sedangkan nilai rata-rata NPCR dan UACI untuk citra KK sebesar 99,60671% dan 35,55296%. Pada pengujian koefisien korelasi, diperoleh nilai rata-rata koefisien korelasi untuk citra KTP sebesar -0,00082 untuk citra KK sebesar -0,00112 yang berarti citra hasil enkripsi memiliki korelasi yang sangat lemah dengan citra asal. Berdasarkan hasil pengujian, diketahui bahwa penerapan metode Arnold *Cat Map* dan *Logistic Map* dapat digunakan untuk mengamankan citra data penduduk.

Kata Kunci: *Kriptografi; Enkripsi; Dekripsi Arnold Cat Map; Logistic Map*

A B S T R A C T

Data security is a very important issue, especially for personal data in the form of text and images. The application of cryptography can be used to secure data so that it cannot be understood by just anyone. In this study, data security in the form of KTP and KK images was carried out using the Arnold *Cat Map* and *Logistic Map* methods. In the key sensitivity test, it was found that changing the decryption key of 0,0001 from the encryption key produced an

**Penulis Korespondensi:*
email: syamsul.bahri@siskom.untan.ac.id

image that was very different from the original image. In the differential analysis test, the average value of NPCR and UACI for the KTP image was 99,60745% and 39,50400%, while the average value of NPCR and UACI for the KK image was 99,60671% and 35,55296%. In testing the correlation coefficient, the average value of the correlation coefficient for the KTP image is -0,00082 and for the KK image is -0,00112, which means that the encrypted image has a very weak correlation with the original image. Based on the test results, it is known that the application of the Arnold *Cat Map* and *Logistic Map* methods can be used to secure the citizens' data image.

Keywords: *Cryptography; Encryption; Decryption; Arnold Cat Map; Logistic Map*

1. PENDAHULUAN

Kemajuan di bidang teknologi telah memungkinkan untuk melakukan pertukaran data secara *online* [1]. Di sisi lain, meningkatnya jumlah kejahatan siber dan makin berkembangnya teknik-teknik kejahatan siber menjadi ancaman pada bidang teknologi dalam hal keamanan data [2]. Masalah keamanan data merupakan hal yang sangat penting terutama untuk data yang bersifat sensitif. Keamanan data merupakan aspek untuk menjaga sebuah data maupun informasi supaya aman dan tidak mudah dibaca [3].

Data yang bersifat sensitif dan rahasia tidak boleh jatuh ke tangan orang yang tidak bertanggungjawab karena dapat disalahgunakan untuk melakukan kegiatan ilegal seperti pengajuan peminjaman online, penjualan data penduduk, dan berbagai kegiatan merugikan lainnya [4]. Guna mengantisipasi penyalahgunaan data yang bersifat rahasia seperti KTP, KK dan data lainnya, maka data tersebut harus dilindungi. Penerapan kriptografi dapat digunakan untuk melakukan pengamanan data agar tidak dapat dibaca dan dipahami oleh orang yang tidak bertanggung jawab [5].

Pengamanan citra yang berisikan data pribadi sudah pernah dilakukan pada penelitian terdahulu Lizy dan Raj pada tahun 2021 melakukan pengamanan *aadhar card* menggunakan algoritma RK-RSA. Hasil penelitian menunjukkan metode RK-RSA menghasilkan *cipherimage* yang cukup baik. Hal ini dapat dilihat dari nilai rata-rata *avalanche effect* algoritma RK-RSA sebesar 53,65 [6]. Yang membedakan penelitian ini dengan penelitian Lizy dan Raj adalah penelitian ini menggunakan metode Arnold *Cat Map* dan *Logistic Map* yang bersifat *chaos.* Metode enkripsi dengan sifat *chaos* yang memiliki tingkat keamanan yang lebih tinggi [7].

Pada tahun 2020, Iqbal, dkk melakukan enkripsi citra menggunakan metode Arnold *Cat Map* dan *Logistic Map* secara terpisah. Hasil penelitian ini menunjukkan bahwa masing-masing metode memiliki keunggulan tersendiri. metode *Logistic Map* memiliki keunggulan berupa nilai NPCR dan UACI lebih tinggi, sedangkan metode Arnold *Cat Map* memiliki keunggulan yaitu nilai koefisien korelasi antara *plain image* dengan *cipher image* lebih rendah [8].

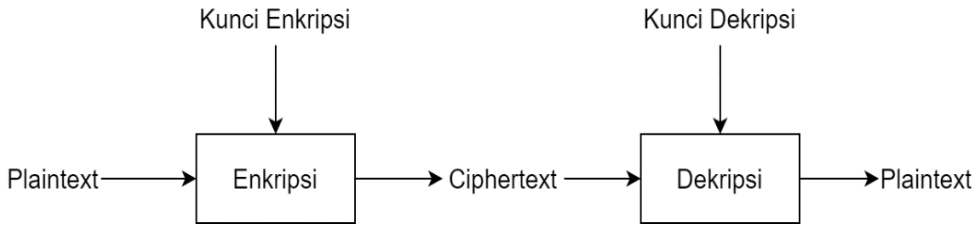
Penggunaan kombinasi metode Arnold *Cat Map* dan *Logistic Map* pernah dilakukan oleh Hamdani dan Listiyani pada tahun 2019*.* Pada pengujian sensitivitas *keystream*, ditemukan bahwa perubahan *keystream* sebesar 0,0001 menyebabkan *cipher image* tidak dapat kembali ke *plain image*. Selain itu, pada penelitian ini ditemukan pula bahwa koefisien korelasi mendekati 0 yang berarti *plain image* dan *cipher image* sangat berbeda sehingga dapat dikatakan bahwa citra akan lebih aman. Perbedaan penelitian ini dengan penelitian Hamdani dan Listiyani adalah pada penelitian ini melakukan enkripsi terhadap citra KTP dan KK yang dimana citra KTP dan KK berisikan informasi pribadi yang rahasia [9].

Pada penelitian ini dibuat sistem pengamanan citra data penduduk menggunakan metode Arnold *Cat Map* dan *Logistic Map*. Metode tersebut digunakan karena memiliki sensitivitas kunci yang tinggi, nilai NPCR dan UACI yang tinggi, serta nilai koefisien korelasi yang rendah. Dengan dibuatnya penelitian ini diharapkan dapat membuat citra KTP dan KK tidak dapat dibaca dan dipahami oleh orang tidak bertanggungjawab. Untuk menguji tingkat keamanan citra, maka akan dilakukan beberapa pengujian yaitu analisis sensitivitas kunci, analisis diferensial berupa NPCR & UACI, serta analisis koefisien korelasi. Adapun tujuan yang ingin dicapai pada penelitian ini adalah melakukan pengamanan citra data penduduk serta menguji tingkat keamanan berdasarkan nilai NPCR, UACI, dan koefisien korelasi.

2. DASAR/TINJAUAN TEORI

2.1. Kriptografi

Kriptografi merupakan ilmu untuk mengamankan data agar tetap aman dalam proses pengiriman data tanpa campur tangan dari pihak yang tidak bertanggungjawab. Terdapat dua proses dalam kriptografi yaitu enkripsi dan dekripsi. Enkripsi adalah proses mengubah *plaintext* menjadi *ciphertext* sedangkan dekripsi adalah proses mengubah *ciphertext* menjadi *plaintext*. Proses enkripsi dan dekripsi menggunakan kunci ditunjukkan pada Gambar 1 [10].



Gambar 1. Proses Enkripsi dan Dekripsi

2.2. Arnold Cat Map

Arnold Cat Map (ACM) merupakan salah metode kriptografi yang bersifat *chaos* yang digunakan pada citra. Konsep metode Arnold Cat Map adalah mengacak posisi piksel. Arnold *Cat Map* melakukan transformasi posisi piksel (x, y) di dalam citra ke posisi piksel yang baru (x_{i+1}, y_{i+1}). Persamaan enkripsi Arnold *Cat Map* dapat dituliskan sebagai berikut.

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod\ (N) \qquad (1)$$

Dimana (x_{i+1} , y_{i+1}) merupakan posisi piksel yang baru setelah transformasi, (x_i , y_i) merupakan posisi piksel di dalam citra saat ini, b dan c merupakan kunci dengan nilai bilangan bulat positif sembarang, serta N merupakan ukuran citra N x N [11].

Hasil dari Arnold *Cat Map* bersifat *reversible* atau dapat dikembalikan menjadi bentuk asli. Untuk mengembalikan hasil enkripsi Arnold *Cat Map* atau invers Arnold *Cat Map* dapat dituliskan sebagai berikut [11].

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix}^{-1} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} mod\ (N) \qquad (2)$$

2.3. *Logistic Map*

Logistic Map merupakan sistem *chaos* sederhana yang digunakan untuk melakukan pembangkitan bilangan acak. Terdapat 4 langkah untuk melakukan enkripsi dan dekripsi menggunakan *Logistic Map*, yaitu sebagai berikut [9].

1. Melakukan pembangkitan kunci menggunakan persamaan sebagai berikut.
$$x_{i+1} = \mu x_i\ (1 - x_i) \quad (3)$$
2. Melakukan fungsi pemotongan terhadap nilai *Logistic Map* yang diperoleh melalui persamaan 3. Fungsi pemotongan dapat ditulis sebagai berikut.
$$k_i = T(x, size) = \ \|x * 10^{count}\|,\ \ x \neq 0 \quad (4)$$
3. Enkripsi *plain image* dengan menjumlahkan nilai piksel dengan kunci kemudian di modulokan dengan 256.
$$c_i = (p_i + k_i)\ mod\ 256 \quad (5)$$
4. Dekripsi *cipher image* dengan melakukan pengurangan nilai piksel dengan kunci kemudian di modulokan dengan 256.
$$p_i = (c_i - k_i)\ mod\ 256 \quad (6)$$

2.4. Analisis Diferensial

Analisis diferensial adalah parameter untuk mengevaluasi tingkat keamanan algoritma dalam mengenkripsi citra. Terdapat dua indikator yang sering digunakan dalam analisis diferensial, yaitu *Number of Pixels Change Rate* (NPCR) dan *Unifer Average Changing Intensity* (UACI) [12].

NPCR digunakan untuk menghitung berapa banyak perbedaan piksel dari dua buah citra. Perhitungan NPCR dapat dilihat pada Persamaan 7:

$$NPCR = \left(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\sum_{k=0}^{o-1}\frac{d_{i,j,k}}{T}\right) \times 100 \quad (7)$$

Dimana T merupakan jumlah total piksel di *cipher image*. Untuk menghitung T maka diperlukan m, n dan o yang melambangkan panjang citra, lebar citra, dan kedalaman citra. Sedangkan $d_{i,j,k}$ melambangkan derajat keabuan dan ditentukan sesuai Persamaan 8.

$$d_{i,j,k} = \begin{cases} 0, jika\ c_{i,j,k}^{(1)} = c_{i,j,k}^{(2)} \\ 1, jika\ c_{i,j,k}^{(1)} \neq c_{i,j,k}^{(2)} \end{cases} \quad (8)$$

Dimana $c_{i,j,k}^{(1)}$ dan $c_{i,j,k}^{(2)}$ melambangkan nilai keabuan dari baris i, kolom j, dan kanal k dari citra $c^{(1)}$ (*plain image*) dan $c^{(2)}$ (*cipher image*)[13].

UACI berfokus pada interval perbedaan nilai piksel dari kedua citra. Perhitungan UACI didefinisikan seperti pada Persamaan 9:

$$UACI = \left(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\sum_{k=0}^{0-1}\frac{\left|c_{i,j,k}^{(1)} - c_{i,j,k}^{(2)}\right|}{F \times T}\right) \times 100\% \quad (9)$$

Dimana F merupakan nilai piksel terbesar yang kompatibel dengan format *cipher image* [13]. Batas minimal indikator NPCR sebesar 99,609375% dan batas minimal UACI sebesar 33,463541% untuk citra grayscale dan RGB [14].

2.5. Koefisien Korelasi

Analisis koefisien korelasi digunakan untuk mengukur hubungan antara *plain image* dan *cipher image*. Koefisien korelasi dapat diukur dengan Persamaan 10 sebagai berikut:

$$CorrCoef(x, y) = \frac{\sum_{i=1}^{n}(x_i - \mu(x))(y_i - \mu(y))}{\sigma(x)\sigma(y)} \quad (10)$$

Dimana $\mu(x)$ dan $\mu(y)$ adalah nilai rata-rata dari masing-masing *plain image* dan *cipher image* yang diperoleh menggunakan Persamaan 11.

$$\mu(x) = \frac{1}{n}\sum_{i=1}^{n} x_i \quad \text{dan} \quad \mu(y) = \frac{1}{n}\sum_{i=1}^{n} y_i \quad (11)$$

Dimana $\sigma(x)$ dan $\sigma(y)$ adalah standar deviasi dari masing-masing *plain image* dan *cipher image* yang diperoleh menggunakan Persamaan 12 [13].

$$\sigma(x) = \sqrt{\sum_{i=1}^{n}\left(x_i - \mu(x)\right)^2} \quad \text{dan} \quad \sigma(y) = \sqrt{\sum_{i=1}^{n}\left(y_i - \mu(y)\right)^2} \quad (12)$$

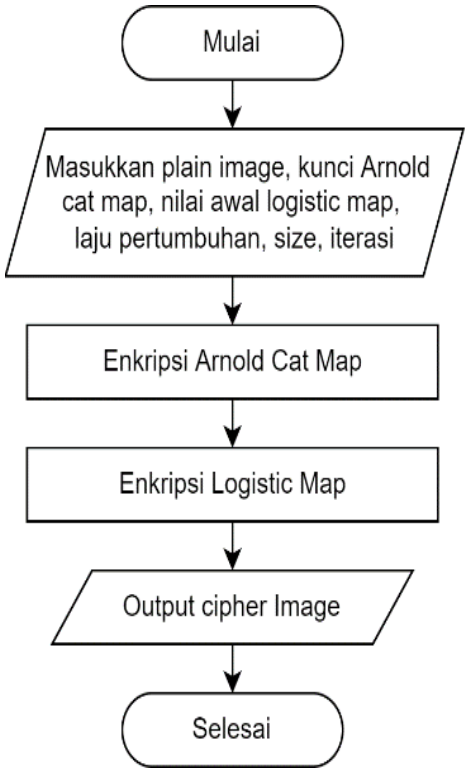
Nilai koefisien korelasi berkisar antara +1,00 sampai -1,00. Nilai koefisien korelasi bernilai positif menunjukkan bahwa semakin besar nilai piksel pada *plain image* diikuti semakin besar nilai piksel pada *cipher image,* atau sebaliknya semakin kecil nilai piksel pada *plain image* diikuti semakin kecil nilai piksel pada *cipher image*. Nilai koefisien korelasi bernilai negatif menunjukkan bahwa terjadi hubungan secara terbalik, yaitu semakin besar nilai piksel pada *plain image* diikuti semakin kecil nilai piksel pada *cipher image,* atau sebaliknya semakin kecil nilai piksel pada *plain image* diikuti semakin besar nilai piksel pada *cipher image* [15]. Jika koefisien korelasi sama dengan satu, itu berarti *plain image* dan *cipher image* adalah sama (korelasi sempurna). Sebaliknya jika koefisien korelasi sama dengan nol, itu berarti *cipher image* benar-benar berbeda dari *plain image* (tidak ada korelasi) [16].

3. METODE

Pada penelitian ini, proses pengamanan data dilakukan menggunakan enkripsi sebanyak dua kali. Proses enkripsi pertama dilakukan dengan menerapkan Arnold *Cat Map* untuk mengacak posisi piksel. Proses enkripsi kedua dilakukan dengan menggunakan *Logistic Map* untuk mensubstitusi nilai piksel hasil metode Arnold *Cat Map*.

3.1. Alur Proses Enkripsi

Alur proses enkripsi yang dilakukan pada penelitian ini dapat dilihat pada Gambar 2.



Gambar 2. Alur Proses Enkripsi

Penjelasan dari alur proses enkripsi pada Gambar 2 adalah sebagai berikut:

1. Masukkan *plain image*, kunci Arnold *Cat Map*, nilai awal *Logistic Map*, laju pertumbuhan, *size*, dan iterasi.

2. Enkripsi Arnold *Cat Map.* Langkah pertama pada enkripsi Arnold *Cat Map* adalah memasukkan *plain image*, kunci, dan iterasi. Kemudian dilanjutkan dengan menghitung posisi baru menggunakan Persamaan (1). Selanjutnya, pindahkan nilai piksel ke posisi yang baru sehingga akan menghasilkan *cipher image*. Langkah menghitung posisi baru dan memindahkan nilai piksel ke posisi baru dilakukan sebanyak jumlah iterasi yang dimasukkan.
3. Enkripsi *Logistic Map.* Langkah pertama pada enkripsi *Logistic Map* yang dilakukan adalah memasukkan *plain image*, nilai awal *Logistic Map*, laju pertumbuhan dan iterasi. Langkah berikutnya yaitu menghitung nilai *Logistic Map* yang baru menggunakan Persamaan (3). Setelah diperoleh nilai *Logistic Map* yang baru maka nilai tersebut akan dilakukan fungsi pemotongan menggunakan Persamaan (4). Setelah proses pemotongan nilai *Logistic Map*, langkah berikutnya adalah mencari nilai piksel yang baru menggunakan Persamaan (5). Perhitungan nilai *Logistic Map* baru sampai mencari nilai piksel yang baru dilakukan sampai seluruh piksel pada citra selesai dan diulangi sesuai dengan iterasi yang dimasukkan.
4. *Output cipher image*. Dari proses enkripsi yang telah dilakukan pada langkah sebelumnya diperoleh citra ter enkripsi atau *cipher image*.

3.2. Alur Proses Dekripsi

Alur proses dekripsi yang dilakukan pada penelitian ini adalah sebagai berikut:

1. Masukkan *cipher image*, kunci Arnold *Cat Map*, nilai awal *Logistic Map*, laju pertumbuhan, *size*, dan iterasi.
2. Dekripsi *Logistic Map.* Langkah pertama pada dekripsi *Logistic Map* memasukkan *cipher image*, nilai awal *Logistic Map*, laju pertumbuhan, *size* dan iterasi. Langkah berikutnya yaitu menghitung nilai *Logistic Map* yang baru menggunakan Persamaan (3). Kemudian nilai *Logistic Map* yang baru akan diterapkan fungsi pemotongan menggunakan Persamaan (4). Setelah proses pemotongan nilai *Logistic Map*, langkah berikutnya adalah mencari nilai piksel yang baru. Langkah perhitungan nilai *Logistic Map* sampai mencari nilai piksel yang baru dilakukan sampai seluruh piksel pada citra selesai dan diulangi sesuai dengan iterasi yang dimasukkan.
3. Dekripsi Arnold *Cat Map.* Langkah pertama pada dekripsi Arnold *Cat Map* adalah memasukkan *cipher image*, kunci, dan iterasi. Kemudian dilanjutkan dengan menghitung invers kunci yang dimasukkan. Setelah diperoleh invers kunci, proses dilanjutkan dengan menghitung posisi baru menggunakan Persamaan (2). Langkah berikutnya adalah memindahkan nilai piksel ke posisi yang baru sehingga akan menghasilkan *plain image*. Langkah memindahkan nilai piksel ke posisi baru dilakukan sebanyak jumlah iterasi yang dimasukkan.
4. *Output plain image.* Dari proses dekripsi yang telah dilakukan pada langkah sebelumnya diperoleh citra asal atau *plain image*.

4. HASIL DAN PEMBAHASAN

4.1. Proses Enkripsi dan Dekripsi Menggunakan Metode Arnold *Cat Map* dan *Logistic Map*

Perhitungan matematis pada proses enkripsi dan dekripsi dapat dicontohkan menggunakan *plain image* yang dapat dilihat pada **Error! Reference source not found.** dan kunci yang dapat dilihat pada Tabel 1.

x_i / y_i	0	1	2
0	255 0 0	96 169 23	227 200 0
1	170 0 255	130 90 44	27 161 226
2	100 118 135	30 255 20	216 0 115

Gambar 3. *Plain Image* 3 x 3 Piksel dengan Koordinat

Tabel 1. Kunci Enkripsi dan Dekripsi

Kunci	Nilai
b	2
c	2
Nilai awal *Logistic Map* (x_0)	0,2345
Laju pertumbuhan (μ)	4
Size	3
Iterasi	10

Proses enkripsi pertama dilakukan menggunakan metode Arnold *Cat Map*. Langkah pertama yaitu melakukan perhitungan posisi baru sesuai dengan Persamaan (1).

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \end{bmatrix} mod(3) = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Proses perhitungan posisi baru dilakukan sampai seluruh koordinat citra diperoleh posisi barunya. Langkah berikutnya yaitu memindahkan nilai piksel ke posisi barunya. Proses perhitungan posisi baru dan pemindahan nilai piksel dilakukan sesuai jumlah iterasi. Dari perhitungan yang telah dilakukan diperoleh *cipher image* metode Arnold *Cat Map* yang dapat dilihat pada Gambar 4.

255 0 0	227 200 0	96 169 23
100 118 135	216 0 115	30 255 20
170 0 255	27 161 226	130 90 44

Gambar 4. *Cipher Image* metode Arnold *Cat Map*

Proses enkripsi kedua dilakukan menggunakan *Logistic Map* dan menggunakan citra hasil enkripsi metode Arnold *Cat Map.* Langkah pertama pada proses enkripsi *Logistic Map* adalah mencari nilai *Logistic Map* yang baru.

$$x_1 = \mu x_0(1 - x_0) = 0{,}718039$$

Setelah diperoleh nilai *Logistic Map* yang baru selanjutnya dilakukan fungsi pemotongan agar dapat digunakan sebagai kunci.

$$k_1 = T(x_1, size) = 718$$

Proses selanjutnya adalah mencari nilai piksel *cipher image* dengan menjumlahkan nilai piksel plain image dengan kunci kemudian dimodulokan dengan 256.

$$c_1 = (p_1 + k_1)\ mod\ 256 = (255 + 718)\ mod\ 256 = 205$$

Proses enkripsi metode *Logistic Map* dilakukan sebanyak jumlah iterasi. Dari perhitungan yang telah dilakukan diperoleh *cipher image* menggunakan metode *Logistic Map* yang dapat dilihat pada Gambar 5.

11	31	179
12	4	252
12	60	106
223	74	206
241	114	175
2	229	196
46	223	181
132	101	141
131	166	95

Gambar 5. *Cipher Image* Metode *Logistic Map*

Untuk mengembalikan *cipher image* menjadi *plain image* harus menggunakan dekripsi. Proses dekripsi pertama kali dilakukan menggunakan metode *Logistic Map.* Proses dekripsi menggunakan metode *Logistic Map* hampir sama dengan proses enkripsi, hanya saja terdapat perbedaan pada pencarian nilai piksel.

$$p_i = (c_i - k_i)\ mod\ 256 = (11 - 718)\ mod\ 256 = 61$$

Dari perhitungan yang dilakukan terhadap *cipher image* sebanyak jumlah iterasi, diperoleh *plain image* metode *Logistic Map* yang dapat dilihat pada Gambar 6.

255	227	96
0	200	169
0	0	23
100	216	30
118	0	255
135	115	20
170	27	130
0	161	90
255	226	44

Gambar 6. *Plain Image* Metode *Logistic Map*

Langkah berikutnya adalah melakukan dekripsi dengan menggunakan metode Arnold *Cat Map.* Proses dekripsi metode Arnold *Cat Map* hampir sama dengan proses enkripsi, hanya saja sebelum dilakukan perhitungan posisi baru, kunci harus di invers terlebih dahulu.

$$k = \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}^{-1} = \begin{bmatrix} 5 & -2 \\ -2 & 1 \end{bmatrix}$$

Setelah diperoleh kunci dekripsi metode Arnold *Cat Map*, dilakukan perhitungan posisi baru dan pemindahan posisi piksel sebanyak jumlah iterasi. Hasil dekripsi metode Arnold *Cat Map* dapat dilihat pada Gambar 7.

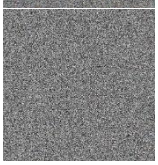
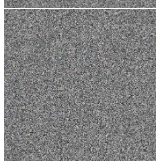
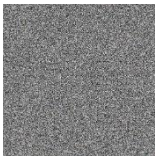
255 0 0	96 169 23	227 200 0
170 0 255	130 90 44	27 161 226
100 118 135	30 255 20	216 0 115

Gambar 7. *Plain Image* Metode Arnold *Cat Map*

4.2. Pengujian Sensitivitas Kunci

Pengujian sensitivitas kunci dilakukan dengan menjalankan proses dekripsi menggunakan kunci yang berbeda dengan kunci enkripsi. Pada proses enkripsi citra *Logistic Map*, nilai x_0 yang digunakan adalah 0,2345. Sedangkan pada proses dekripsi, nilai x_0 yang digunakan adalah 0,2346. Hasil pengujian sensitivitas kunci dapat dilihat pada Tabel 2.

Tabel 2. Hasil Pengujian Sensitivitas Kunci

Plain Image	**Enkripsi** $(x_0 = 0,2345)$	**Dekripsi** $(x_0 = 0,2346)$
		
		
		
		

4.3. Pengujian Analisis Diferensial

Pengujian analisis diferensial yang dilakukan adalah pengujian NPCR dan UACI. Pengujian NPCR dilakukan untuk mengetahui berapa banyak piksel pada *plain image* yang berubah sedangkan pengujian UACI dilakukan untuk mengetahui berapa interval perubahan nilai piksel. Pengujian dilakukan menggunakan 100 data yang terdiri dari 50 citra KTP dan 50 citra KK. Hasil pengujian analisis diferensial ditampilkan pada Tabel 3.

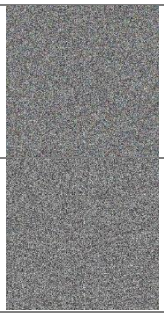
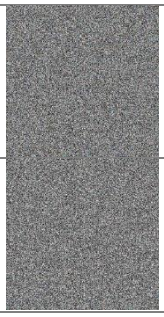
Tabel 3. Hasil Pengujian Analisis Diferensial

Plain Image	***Cipher Image***	**NPCR (%)**	**UACI (%)**
		99,604257	38,280020
		99,609502	34,797612
⋮	⋮	⋮	⋮
		99,603971	32,592625
		99,605179	34,547473

4.4. Pengujian Koefisien Korelasi

Pengujian analisis diferensial yang dilakukan adalah pengujian NPCR dan UACI. Untuk menghasilkan *cipher image* yang baik, maka nilai koefisien korelasi harus mendekati 0. Pengujian dilakukan menggunakan 100 data uji yang terdiri dari 50 citra KTP dan 50 citra KK. Hasil koefisien korelasi ditampilkan dalam Tabel 4.

Tabel 4. Hasil Pengujian Koefisien Korelasi

Plain Image	***Cipher Image***	**Koefisien Korelasi**
		-0,000126
		-0,000045
⋮	⋮	⋮
		-0,002912
		-0,000352

4.5. Pembahasan

Berdasarkan hasil pengujian sensitivitas kunci, diketahui bahwa perubahan nilai awal *Logistic Map* sebesar 0,0001 tidak dapat mengembalikan *cipher image* menjadi citra asal. Hasil dekripsi menggunakan nilai awal *Logistic Map* dengan beda sebesar 0,0001 juga tampak sangat berbeda dengan citra asal. Hal ini membuktikan bahwa penggunaan kunci dekripsi yang berbeda dengan kunci enkripsi tidak dapat digunakan untuk melakukan *cipher image* menjadi citra asal.

Berdasarkan pengujian analisis diferensial dan koefisien korelasi terhadap 50 citra KTP diperoleh nilai rata-rata NPCR dan UACI adalah 99,60745% dan 39,50400%, serta nilai rata-rata koefisien korelasi adalah -0,00082. Sedangkan pada pengujian analisis diferensial dan koefisien korelasi terhadap 50 citra KK diperoleh nilai rata-rata NPCR dan UACI adalah 99,60671% dan 35,55296%, serta nilai rata-rata koefisien korelasi adalah -0,00112. Berdasarkan nilai rata-rata NPCR citra KTP dan citra KK, diketahui bahwa penerapan metode Arnold *Cat Map* dan *Logistic Map* belum memenuhi batas minimal NPCR namun masih menghasilkan *cipher image* yang sangat acak. Sedangkan berdasarkan nilai rata-rata UACI citra KTP dan citra KK, diketahui bahwa telah memenuhi batas minimal UACI sehingga menghasilkan interval perbedaan nilai piksel yang cukup jauh. Selain itu, berdasarkan nilai rata-rata koefisien korelasi citra KTP dan citra KK, diketahui bahwa korelasi antara *plain image* dengan *cipher image* mendekati nol sehingga korelasi antara *plain image* dengan *cipher image* sangat lemah.

5. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan dapat disimpulkan bahwa metode Arnold Cat Map dan Logistic Map sangat sensitif terhadap kunci yang dimasukkan. Hal ini dapat dilihat perubahan kunci dekripsi sebesar 0,0001 tidak dapat mengembalikan citra ke asalnya. Nilai rata-rata NPCR untuk citra KTP dan citra KK sebesar 99,60745% dan 99,60671%. Nilai NPCR yang dihasilkan berada sedikit dibawah batas indikator yaitu 99,609375% namun masih menghasilkan citra yang sangat acak. Selain itu, diperoleh pula nilai rata-rata UACI untuk citra KTP dan citra KK sebesar 39,50400% dan 35,55296% yang berarti interval perbedaan nilai piksel cukup jauh. Berdasarkan nilai koefisien korelasi citra KTP dan citra KK diketahui bahwa korelasi antara *plain image* dengan *cipher image* sangat lemah sehingga citra sulit untuk dikenali. Dari hasil penelitian diketahui bahwa penerapan metode Arnold *Cat Map* dan *Logistic Map* dapat digunakan untuk mengamankan citra data penduduk baik itu citra KTP maupun citra KK karena citra sudah tidak dapat dibaca dan dipahami.

REFERENSI

[1] F. Alfiah, R. Sudarji, and D. Taqiyyuddin Al Fatah, "Aplikasi Kriptografi dengan Menggunakan Algoritma Elgamal Berbasis Java Desktop pada PT. Wahana Indo Trada Nissan Jatake," *ADI Bisnis Digit. Interdisiplin J.*, vol. 1, no. 1, pp. 22–34, 2020.

[2] A. N. Ulfah, N. Lizarti, D. Sudyana, and M. K. Anam, "Pelatihan Secure Computer User untuk Meningkatkan Kesadaran Siswa Terhadap Keamanan Data dan Informasi," *J-PEMAS*, vol. 2, no. 1, pp. 17–24, 2021.

[3] R. Nur Ibrahim, "Perangkat Lunak Keamanan Data Menggunakan Algoritma Kriptografi Simetri Tiny Encription Algorithm (TEA)," *J. Comput. Bisnis*, vol. 13, no. 1, pp. 1–10, 2019, [Online]. Available: www.jevuska.com

[4] H. Mukhtar, *Kriptografi Untuk Keamanan Data*. Yogyakarta: Deepublish, 2018.

[5] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *J. Inform. Mulawarman*, vol. 10, no. 1, pp. 20–31, 2015, doi: 10.30872/jim.v10i1.23.

[6] R. F. S. Lizy and V. J. Raj, "Image Encryption Using RK-RSA Algorithm in Aadhaar Card," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 3, pp. 4683–4693, 2021, doi: 10.17762/turcomat.v12i3.1887.

[7] M. Bin Younas and J. Ahmad, "Comparative Analysis of Chaotic and Non-chaotic Image Encryption Schemes," *Int. Conf. Emerg. Technol.*, no. January, pp. 81–86, 2014, doi: 10.1109/ICET.2014.7021021.

[8] Iqbal, Kusrini, and A. Nasiri, "Komparasi Hasil Enkripsi Arnold Cat Map dan Logistic Map Pada Citra Digital," *J. Ilm. Inf. Technol. d'Computare*, vol. 10, pp. 10–16, 2020.

[9] M. Hamdani and N. Listiyani, "Implementasi Metode Arnold's Cat Map dan Logistic Map pada Proses Enkripsi-Dekripsi untuk Keamanan Pengiriman Citra," *Sainstech J. Penelit. dan Pengkaj. Sains dan Teknol.*, vol. 29, no. 1, pp. 15–24, 2019, doi: 10.37277/stch.v29i1.312.

[10] D. Ariyus, *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*, 1st ed. Yogyakarta: Andi, 2008.

[11] N. H. Masruri, K. Kusrini, and A. Sunyoto, "Meningkatkan Keamanan Pesan Menggunakan Enkripsi Arnold Cat Map dan Steganografi Pixel Value Differencing," *inotek*, vol. 3, no. 1, pp. 113–118, 2019.

[12] E. Y. Putri, "Implementasi Vigenere Chiper pada Penyandian Citra Berbasis Pembangkitan Kunci Algoritma Advanced Encryption Standart (AES)," Universitas Jember, 2018.

[13] Y. Mao, G. Chen, and S. Lian, "A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps," *Int. J. Bifurc. Chaos*, vol. 14, no. 10, pp. 3613–3624, 2004, doi: 10.1142/S021812740401151X.

[14] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," *J. Sel. Areas Telecommun.*, 2011.

[15] T. Cahyono, *Statistik Uji Korelasi*, 1st ed. Purwokerto: Yayasan Sanitarian Banyumas (Yasamas), 2017.

[16] A. Mousa, O. S. Faragallah, S. EL-Rabaie, and E. M. Nigm, "Security Analysis of Reverse Encryption Algorithm for Databases," *Int. J. Comput. Appl.*, vol. 66, no. 14, pp. 19–27, 2013.