

# Rama Paper

*by* Liana Liana

---

**Submission date:** 08-Mar-2023 06:01AM (UTC-0500)

**Submission ID:** 2032031739

**File name:** Rama\_Jurnal\_Ilmiyah\_Teknologi\_dan\_Rekayasa.docx (1.11M)

**Word count:** 3199

**Character count:** 19242

# Enkripsi Citra Digital Menggunakan Komposisi Transposisi Cat Map dan Substitusi Key Stream Logistic Map

<sup>1\*</sup>Rama Dian Syah, <sup>2</sup>Sarifuddin Madenda, <sup>3</sup>Ruddy J. Suhatri, <sup>4</sup>Suryadi Harmanto

<sup>1,3</sup>Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Gunadarma, <sup>2,4</sup>Program Doktor Teknologi Informasi, Universitas Gunadarma  
Jl. Margonda Raya No. 100, Depok 16424, Jawa Barat

<sup>1\*</sup>rama\_ds@staff.gunadarma.ac.id, <sup>2</sup>sarif@staff.gunadarma.ac.id, <sup>3</sup>ruddyjs@staff.gunadarma.ac.id, <sup>4</sup>suryadi@gunadarma.ac.id

## Abstrak

Transmisi pertukaran data digital melalui jaringan internet menjadi hal penting pada kemajuan teknologi. Risiko pembajakan oleh pihak yang tidak bertanggung jawab mungkin terjadi karena kemudahan dalam pertukaran data. Pengembangan metode enkripsi data yang andal dan kuat adalah solusi untuk risiko ini. Penelitian ini mengusulkan algoritma enkripsi data baru melalui komposisi enkripsi transposisi Cat Map dan enkripsi substitusi Logistic Map. Algoritma yang diusulkan secara bersamaan mengubah posisi data dan mengubah nilai data secara acak. Penelitian telah dilakukan dengan menggunakan beberapa citra dengan berbagai fitur dan ukuran yang berbeda. Analisis keacakan citra hasil enkripsi menunjukkan bahwa histogram intensitas warna piksel memiliki distribusi yang seragam dengan nilai korelasi rendah mendekati 0. Hasil analisis peak signal to noise ratio (PSNR) menunjukkan citra hasil dekripsi sama dengan citra asli. Algoritma yang diusulkan memiliki ruang kunci  $3,24 \times 10^{68}$ . Hasil NPCR, UACI dan Entropi menunjukkan algoritma yang diusulkan tahan terhadap serangan diferensial dan serangan entropi.

**Kata Kunci:** Enkripsi, Dekripsi, Citra Digital, Transposisi Cat Map, Substitusi Key Stream Logistic Map

## Abstract

Digital data transmission through the internet network is important in technological advances. The risk of hijack by irresponsible parties may occur because of the ease in exchanging data. Development of reliable and strong data encryption methods is the solution to this risk. This research proposes a new data encryption algorithm through the composition of Cat Map transposition encryption and Logistic Map substitution encryption. The proposed algorithm simultaneously changes data positions and changes data values randomly. Research has been carried out using several images with different features and sizes. Analysis of the randomness of the encrypted image shows that the histogram of pixel color intensity has a uniform distribution with a low correlation value close to 0. The results of the peak signal to noise ratio (PSNR) analysis show that the decrypted image is the same as the original image. The proposed algorithm has a key space of  $3.24 \times 10^{68}$ . The NPCR, UACI and Entropy results show that the proposed algorithm is resistant to differential attacks and entropy attacks.

**Keywords:** Encryption, Decryption, Digital Image, Cat Map Transposition, Logistic Map Keystream Substitution

## PENDAHULUAN

Saat ini data dan informasi citra digital dapat diperoleh dengan mudah melalui kamera atau internet. Citra digital yang mengandung data atau informasi pribadi membutuhkan sistem keamanan untuk mencegah kejahatan dunia maya. Citra digital yang ditransmisikan melalui internet dapat diakses dengan akses yang tidak sah. Metode kriptografi dapat diimplementasikan pada citra digital untuk mengatasi akses tidak sah seperti modifikasi konten, pelanggaran hak cipta dan sebagainya. Kriptografi citra digital menggunakan berbagai metode matematis untuk mengamankan informasi dalam citra [1].

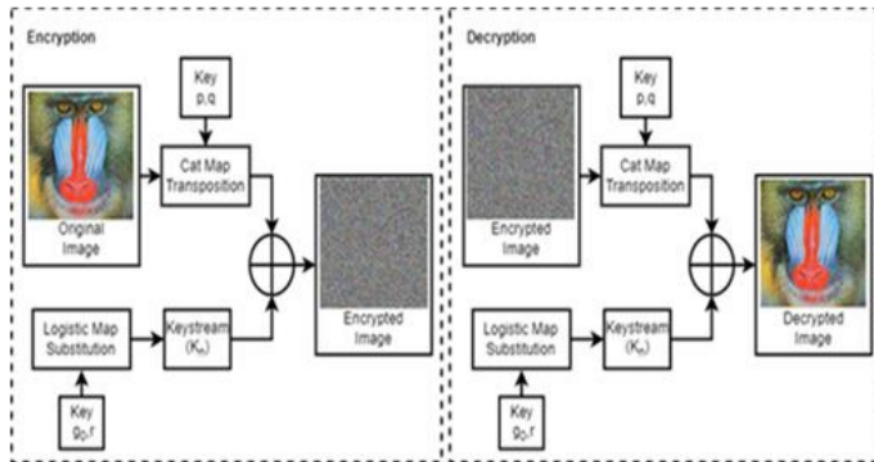
Proses dalam kriptografi citra digital adalah enkripsi dan dekripsi. Enkripsi citra digital adalah transformasi citra asli menjadi citra terenkripsi. Dekripsi citra digital adalah proses mengubah kembali citra terenkripsi menjadi citra asli. Transposisi dan substitusi merupakan dua teknik enkripsi dan dekripsi yang digunakan dalam penelitian ini. Teknik transposisi pada citra digital dilakukan dengan mengacak koordinat piksel, sedangkan teknik substitusi dilakukan dengan mengubah nilai intensitas warna piksel pada citra [2]. Kedua teknik ini digabungkan untuk meningkatkan keamanan algoritma enkripsi. Selain itu, studi terkait transposisi dan teknik substitusi telah dilakukan.

Penelitian [3] mengembangkan fungsi Cat Map sebagai transposisi dan Bernoulli Map sebagai metode substitusi dengan menggabungkan kedua metode tersebut secara berurutan atau sekuensial. Enkripsi citra berwarna dilakukan dengan mengenkripsi setiap kanal warna (R, G, B) secara terpisah yang membutuhkan proses lebih lama. Penelitian [4] mengembangkan transposisi Cat Map 4D yang merupakan enkripsi citra berwarna menggunakan Cat Map 3D dan dilanjutkan dengan transposisi CatMap 4D secara berurutan atau sekuensial. Proses secara sekuensial membutuhkan proses yang lebih banyak sehingga waktu proses lebih lama. Penelitian [5] mengembangkan fungsi transposisi Henon Map yang dikomposisikan dengan substitusi keystream Logistic Map. Proses yang dilakukan secara komposisi atau dilakukan dengan satu proses loop dapat mempercepat waktu proses enkripsi.

Pada penelitian ini enkripsi dan dekripsi dilakukan dengan komposisi Cat Map dan Logistic Map. Algoritma yang diusulkan ini dimaksudkan untuk mempercepat waktu pemrosesan pada enkripsi citra berwarna dengan komposisi Cat Map dan Logistic Map daripada menggunakan algoritma secara berurutan atau sekuensial. Algoritma juga memperbesar ruang kunci sehingga keamanan algoritma enkripsi dapat ditingkatkan. Kontribusi dari penelitian ini adalah mengembangkan algoritma enkripsi dan dekripsi yang kuat terhadap serangan statistik, diferensial, dan *brute force*. Kinerja algoritma yang diusulkan diuji menggunakan alat ukur histogram, korelasi, NPCR, UACI, entropi, PSNR, waktu proses, dan ruang kunci.

## METODE PENELITIAN

Metode enkripsi dan dekripsi citra berwarna pada penelitian ini menggunakan komposisi transposisi Cat Map dan substitusi Logistic Map. Citra berwarna digital direpresentasikan sebagai fungsi matriks 3D  $I(x,y,c)$ , dimana  $x$  dan  $y = (1, 2, \dots, N)$  keduanya didefinisikan sebagai koordinat piksel (elemen matriks) [6]. Variabel  $c$  mewakili channel warna yaitu Merah=1, Hijau=2, dan Biru=3. Gambar 1 adalah skema proses enkripsi dan dekripsi yang diusulkan.



Gambar 1. Metode Enkripsi dan Dekripsi

Proses enkripsi dilakukan menggunakan Cat Map untuk mentranspose setiap koordinat piksel secara acak dan dilanjutkan dengan Logistic Map untuk mensubstitusi nilai intensitas warna piksel. Citra terenkripsi  $I'(x',y',c)$  merupakan hasil dari proses enkripsi. Proses dekripsi dilakukan dengan transposisi Cat Map untuk mengembalikan setiap koordinat piksel dan dilanjutkan dengan substitusi Logistic Map untuk mengembalikan nilai intensitas warna piksel. Citra dekripsi  $I(x,y,c)$  merupakan hasil proses dekripsi.

#### A. Transposisi Cat Map

Transposisi Cat Map digunakan untuk mengubah koordinat piksel citra secara acak dan dapat diterapkan pada citra berukuran persegi dengan ukuran  $N \times N$  [7]. Fungsi Cat Map ditunjukkan oleh persamaan (1) dan (2), dimana  $p$  dan  $q$  adalah parameter kunci yang memiliki bilangan bulat positif dengan range  $(p, q) \in \mathbb{Z}^+$ . Proses enkripsi fungsi transposisi Cat Map mengubah piksel koordinat citra asli  $I(x,y,c)$  menjadi citra terenkripsi  $I(x',y',c)$  secara acak. Namun, proses dekripsi mengembalikan piksel koordinat citra terenkripsi  $I(x',y',c)$  menjadi citra dekripsi  $I(x,y,c)$ .

$$I(\hat{x}, \hat{y}, c) \leftarrow I(x, y, c) \text{ dimana } \begin{cases} \hat{x} = x + py \text{ mod } (N) \\ \hat{y} = qx + (pq + 1)y \text{ mod } (N) \end{cases} \quad (1)$$

$$I(x, y, c) \leftarrow I(\hat{x}, \hat{y}, c) \text{ dimana } \begin{cases} x = 1 - \hat{x} + p\hat{y} \text{ mod } (N) \\ y = q\hat{x} + (pq + 1)\hat{y} \text{ mod } (N) \end{cases} \quad (2)$$

#### B. Substitusi Logistic Map

Logistic Map adalah fungsi yang memiliki perilaku acak tergantung pada nilai awal dengan sifat non-periodik [7]. Proses penggantian nilai intensitas warna piksel menggunakan keystream yang dihasilkan oleh fungsi logistic map. Fungsi ini ditunjukkan oleh persamaan (3), dimana  $n = (0, 1, \dots, L-1)$ ,  $L = N \times N$  sebagai jumlah piksel citra. Parameter kunci  $g_0$  dan  $r$  adalah bilangan real positif dengan range  $3.5699 < r \leq 4$  dan  $0 < g_0 < 1$ .

$$g_{n+1} = r \times g_n \times (1 - g_n) \quad (3)$$

Selanjutnya *key stream* dihitung dengan persamaan (4). *Key stream* direpresentasikan sebagai  $k_n = (k_0, k_1, \dots, k_{L-1})$ , di mana  $k_n$  adalah angka acak positif dalam rentang  $k_n \in [0, 255]$ . Substitusi intensitas warna piksel dilakukan dengan operasi XOR ( $\oplus$ ) seperti yang ditunjukkan oleh persamaan (5), di mana  $I(x', y', c)_n$  adalah gambar terenkripsi dari transposisi Cat Map dan  $I(x', y', c)_n$  adalah gambar terenkripsi dari substitusi Logistic.

$$k_n = \text{round}(|g_n \times 10000|) \bmod 256 \quad (4)$$

$$\hat{I}(x', y', c)_n = k_n \oplus I(x', y', c)_n \quad (5)$$

### C. Algoritma pembangkit *Key Stream*

Keystream dihitung menggunakan fungsi Logistic Map pada persamaan (3) dan (4) dan dihasilkan sebanyak jumlah piksel pada citra. Parameter kunci dari algoritma pembangkitan keystream adalah  $g_0$  dan  $r$ . Langkah-langkah algoritma pembangkit *key stream* [8] sebagai berikut:

---

#### Algoritma 1: Pembangkit Key Stream

---

```

1: function Logistic(N, g0, r)
2:   L ← N × N
3:   for n ← 0 to L-1 do
4:     gn+1 ← r × gn × (1 - gn)
5:     kn ← round(gn+1 × 10000) mod(256)
6:   end for
7: end function

```

---

### D. Algoritma Enkripsi

Proses enkripsi dilakukan dengan transposisi Cat Map dan substitusi Logistic. Proses tersebut akan mentranspose piksel koordinat dan diikuti dengan memodifikasi setiap intensitas piksel warna dari citra asli secara acak menjadi koordinat piksel baru dan intensitas warna citra terenkripsi. Enkripsi menggunakan persamaan (1), (5), dan keystreams  $k_n$  yang dihasilkan oleh algoritma 1. Algoritma enkripsi sebagai berikut:

---

#### Algoritma 2: Prosedur Enkripsi

---

**Input:** Kunci  $p, q, k_n$ , Citra asli  $I(x, y, c)$

**Output:** Citra Terenkripsi  $I'(x', y', c)$

```

1: N ← ukuran I(x, y, c)
2: n ← 0
3: kn ← Logistic(N, g0, r)
4: for x ← 0 to N-1 do
5:   for y ← 0 to N-1 do

```

```

6:    $x' \leftarrow (x + py) \bmod (N)$ 
7:    $y' \leftarrow (qx + (pq + 1)y) \bmod (N)$ 
8:    $I'(x', y', c) \leftarrow k_n \oplus I(x, y, c)$ 
9:    $n \leftarrow n + 1$ 
10:  end for
11:  end for

```

---

#### E. Algoritma Dekripsi

Proses dekripsi adalah mengembalikan setiap koordinat piksel dan intensitas warna piksel. Parameter kunci dan keystream pada proses dekripsi sama dengan proses enkripsi. Algoritma dekripsi adalah sebagai berikut:

---

#### Algoritma 3: Prosedur Dekripsi

**Input:** Kunci  $p, q, k_n$ , Citra Terenkripsi  $I'(x', y', c)$

**Output:** Citra Asli  $I(x, y, c)$

```

1:   $N \leftarrow \text{ukuran } I(x, y, c)$ 
2:   $n \leftarrow 0$ 
3:   $k_n \leftarrow \text{Logistic}(N, g_0, r)$ 
4:  for  $x \leftarrow 0$  to  $N - 1$  do
5:    for  $y \leftarrow 0$  to  $N - 1$  do
6:       $x' \leftarrow (x + py) \bmod (N)$ 
7:       $y' \leftarrow (qx + (pq + 1)y) \bmod (N)$ 
8:       $I(x, y, c) \leftarrow k_n \oplus I'(x', y', c)$ 
9:       $n \leftarrow n + 1$ 
10:    end for
11:  end for

```

---

## HASIL DAN PEMBAHASAN

Penelitian dilakukan dengan menggunakan berbagai citra RGB dengan ukuran  $(N \times N)$  dan fitur yang berbeda. Contoh parameter yang digunakan adalah sebagai berikut:  $p = 30$ ,  $q = 40$ ,  $g_0 = 0.2$  dan  $r = 3.7$ . Perangkat penelitian yang digunakan adalah Matlab R2018a yang berjalan di komputer dengan spesifikasi prosesor Intel (R) Core (TM) i7-4790 CPU 3.60 Ghz, RAM 16 GB, dan sistem operasi Microsoft Windows 10.

#### A. Analisis Histogram

Histogram digunakan untuk menunjukkan sebaran intensitas warna piksel pada citra [9]. Penelitian ini menggunakan histogram untuk merepresentasikan distribusi intensitas warna piksel yang dapat menunjukkan kinerja keacakan piksel pada citra terenkripsi yang dihasilkan oleh algoritma yang diusulkan. Informasi citra dapat dengan mudah dibaca jika histogram membentuk pola tertentu. Sebaliknya, informasi sulit dibaca jika histogram membentuk pola yang seragam.

Pada Tabel 1, kolom 5 dan 6 menunjukkan histogram semua citra asli membentuk pola tertentu, sedangkan histogram semua citra terenkripsi membentuk pola seragam. Hal ini menunjukkan bahwa algoritma yang diusulkan dapat mengubah semua koordinat piksel secara acak dan mengubah nilai intensitas warna pada citra terenkripsi. Informasi dalam citra terenkripsi menjadi sulit dibaca.

#### B. Analisis Korelasi

Korelasi adalah parameter untuk mengukur tingkat kesamaan antara dua piksel yang berdekatan secara horizontal [ $I(x,y)$  dan  $I(x+1,y)$ ], secara vertikal [ $I(x,y)$  dan  $I(x,y+1)$ ], dan secara diagonal [ $I(x,y)$  dan  $I(x+1,y+1)$ ] dari sebuah citra. Jika nilai korelasi mendekati 1 atau -1 maka dua piksel yang berdekatan berkorelasi tinggi atau warna kedua piksel serupa. Sebaliknya, jika nilai korelasi mendekati 0 maka dua piksel yang berdekatan memiliki korelasi warna yang rendah atau kedua piksel diacak dengan baik.

Persamaan (6) sebagai rumus korelasi, dimana A dan B adalah citra yang sebangun mewakili dua piksel yang berdekatan secara horizontal, vertikal, dan diagonal. Variabel dan masing-masing merupakan nilai rata-rata dari semua piksel pada citra A dan B.


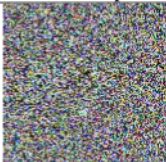
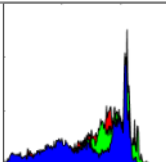
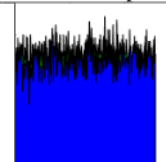
$$r = \frac{\sum_x^M \sum_y^N (A_{xy} - \bar{A})(B_{xy} - \bar{B})}{\sqrt{(\sum_x^M \sum_y^N (A_{xy} - \bar{A})^2)(\sum_x^M \sum_y^N (B_{xy} - \bar{B})^2)}} \quad (6)$$

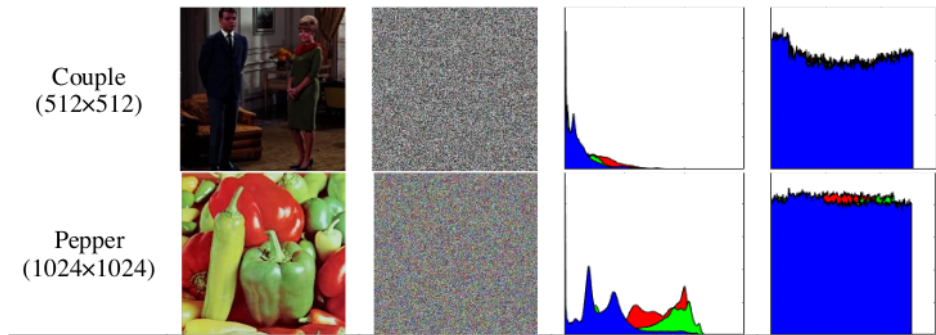
Pada tabel 2, kolom 5, 6, dan 7 menunjukkan korelasi nilai absolut citra terenkripsi antara 0.00024 dan 0,1.269. Nilai korelasi citra terenkripsi lebih kecil dari citra asli pada kolom 2, 3 dan 4. Hal ini mengindikasikan algoritma yang diusulkan dapat mengacak semua informasi yang terdapat pada citra terenkripsi sehingga informasi tersebut tidak dapat terbaca.

Pada kolom 2, 3, dan 4 terlihat garis kurva dari citra asli bergerak dalam ruang diagonal yang menunjukkan dua piksel yang berdekatan pada citra asli berkorelasi tinggi. Namun pada kolom 5, 6 dan 7 terlihat garis kurva citra terenkripsi bergerak secara acak dalam ruang kurva dua dimensi yang menunjukkan dua piksel yang berdekatan pada citra terenkripsi memiliki korelasi warna yang rendah.

Berdasarkan hasil nilai korelasi dan kurva korelasi pada Tabel 2 menunjukkan algoritma enkripsi citra yang diusulkan dapat mengacak posisi dan intensitas warna semua piksel sehingga pesan yang terkandung dalam citra terenkripsi sulit untuk dibajak.

Tabel 1. Analisis Histogram

Nama	Citra		Histogram	
	Asli	Terenkripsi	Asli	Terenkripsi
House (300x300)				



Tabel 2. Analisis Korelasi

Name	Korelasi Citra Asli			Korelasi Citra Terenkripsi		
	Horizontal	Vertikal	Diagonal	Horizontal	Vertikal	Diagonal
House (300 ×300)	 0.90081	 0.91792	 0.84436	 -0.10032	 -0.00345	 -0.00645
Couple (512×512)	 0.98370	 0.98836	 0.96388	 0.08367	 0.00022	 -0.00440
Pepper (1024 ×1024)	 0.98120	 0.99490	 0.98953	 -0.00132	 -0.00015	 -0.00142

### C. Analisis NPCR dan UACI

NPCR (Number of Pixel Change Rate) adalah parameter untuk mengukur sensitivitas piksel yang berbeda pada citra asli yang mempengaruhi hasil citra terenkripsinya [10]. UACI adalah parameter untuk mengukur rata-rata persentase perubahan piksel pada citra terenkripsi. Nilai NPCR dan UACI menunjukkan tingkat keamanan algoritma yang tahan terhadap serangan diferensial [11].

Persamaan (7) dan (8) sebagai rumus NPCR dan UACI dimana C1 dan C2 adalah dua buah citra terenkripsi. Koefisien  $D_{xy}$  adalah nilai kesamaan piksel dalam koordinat yang sama dari citra C1 dan C2.  $C1_{xy}$  dan  $C2_{xy}$  adalah nilai intensitas warna dari C1 dan C2 pada posisi (x,y).

$$NPCR = \frac{1}{M \times N} \sum_x^M \sum_y^N D_{xy} \times 100\% \quad (7)$$



$$UACI = \frac{1}{M \times N} \sum_x^M \sum_y^N \frac{|C1_{xy} - C2_{xy}|}{255} \times 100\% \quad (8)$$

Tabel 3 menunjukkan nilai NPCR terbesar adalah 99.65210% dan nilai UACI terbesar adalah 34.13334%. Kedua nilai tersebut berada di atas standar 99.6% dari nilai NPCR dan 33.4% dari nilai UACI yang menunjukkan bahwa algoritma yang diusulkan tahan terhadap serangan diferensial [7] dan memiliki kepekaan terhadap perubahan piksel pada citra asli masukan yang berpengaruh terhadap hasil citra terenkripsi.

#### D. Analisis Entropi

Entropi adalah parameter untuk mengukur rata-rata minimum jumlah bit yang diperlukan untuk mendekodekan suatu simbol dalam rangkaian bit. Nilai entropi menunjukkan kinerja tingkat keamanan dalam algoritma yang tahan terhadap serangan entropi dan tingkat keacakan dalam citra terenkripsi [12]. Persamaan (9) sebagai rumus entropi dimana  $P_i$  adalah probabilitas kemunculan suatu piksel dengan nilai  $i$ . Nilai maksimum entropi adalah 8 [7].

$$H = \sum_{i=0}^{255} P_i \log_2 \left( \frac{1}{P_i} \right) \quad (12)$$

Tabel 3 menunjukkan nilai entropi terbesar adalah 7.99976. Hal ini menunjukkan bahwa algoritma yang diusulkan tahan terhadap serangan entropi dan mampu mengacak koordinat piksel dan memodifikasi nilai intensitas warna piksel pada citra terenkripsi [9].

Tabel 3. NPCR, UACI, dan Entropi Citra Terenkripsi

Name	NPCR (%)	UACI (%)	Entropi
House	99.65210	33.34663	7.99637
Couple	99.60620	34.13334	7.99665
Pepper	99.60715	33.39355	7.99976

#### E. Analisis Kualitas Citra Terdekripsi

Kualitas citra hasil dekripsi diukur dengan PSNR (Peak Signal to Noise Ratio) dan MSE (Mean Square Error). Persamaan (10) sebagai formula PSNR yang dihitung mengacu pada nilai MSE antara citra asli dan citra dekripsi [13] menggunakan persamaan (11).

$$PSNR = 20 \log_{10} \frac{255}{MSE} \quad (9)$$

$$MSE = \frac{1}{M \times N} \sum_x^M \sum_y^N (I(x, y) - \hat{I}(x, y))^2 \quad (10)$$







Secara visual pada Tabel 4 kolom 1 dan 2 direpresentasikan sebagai citra asli dan citra dekripsi dimana tidak ada perbedaan antara kedua citra atau kualitas citra dekripsi sama dengan citra aslinya. Kolom 4 dan 5 adalah nilai  $MSE = 0$  dan  $PSNR = \infty$  pada semua citra yang didekripsi. Hal ini menandakan bahwa informasi pada citra hasil dekripsi sama dengan citra aslinya [14].

F. Analisis Ruang Kunci

Algoritma yang diusulkan adalah komposisi transposisi Cat Map dan substitusi Logistic Map. Parameter kunci yang digunakan adalah  $p, q, g_0$ , dan  $r$ . Rentang nilai  $p, q \in \mathbb{Z}^+$ . Rentang nilai  $r$  dan  $g_0$  adalah  $3.5699 < r \leq 4$  dan  $0 < g_0 < 1$  dimana  $g_0, r \in \mathbb{R}^+$  [7]. Rentang nilai bilangan bulat pada Matlab adalah  $1,8 \times 10^{19}$  dan nilai matissa adalah  $10^{15}$  [13].

Pada Tabel 5, ruang kunci algoritma yang diusulkan lebih besar dari Cat Map dan Logistic Map. Hal ini menunjukkan algoritma yang diusulkan lebih tahan terhadap serangan brute force [14].

Tabel 4. Analisis Kualitas Citra Terdekripsi

Citra Asli	Citra Terdekripsi	MSE	PSNR
		0	$\infty$
		0	$\infty$
		0	$\infty$

Tabel 5. Ruang Kunci

Fungsi	Parameter Kunci	Ruang Kunci
Cat Map	$p, q \in \mathbb{Z}^+$	$3.24 \times 10^{38}$
Logistic Map	$g_0 \in [0, 1]; r \in [3.5699, 4]$	$10^{30}$
Usulan	$p, q \in \mathbb{Z}^+;$	$3.24 \times 10^{68}$
Algoritma	$g_0 \in [0, 1]; r \in [3.5699, 4]$	

G. Analisis Waktu Proses

Waktu proses enkripsi dan dekripsi menunjukkan rata-rata waktu yang dibutuhkan oleh algoritma untuk melakukan proses enkripsi dan dekripsi. Tabel 6 menunjukkan perbandingan waktu proses enkripsi dan dekripsi. Proses waktu algoritma yang diusulkan lebih cepat dibandingkan algoritma kombinasi Cat dan Logistik secara berurutan atau sekuensial.

H. Perbandingan

Perbandingan algoritma didasarkan pada prinsip *chaos comparative* menurut aspek NPCR, UACI, dan Entropy [9]. Tabel 7 menunjukkan algoritma yang diusulkan mendapatkan hasil terbaik dibandingkan dengan referensi lain berdasarkan NPCR, UACI, dan Entropy.

Tabel 6. Waktu Enkripsi dan Dekripsi (s)

Nama	Ukuran	Enkripsi		Dekripsi	
		Cat & Logistic Map Sekuensial	Usulan Algorithm	Cat & Logistic Map Sekuensial	Usulan Algoritma
House	300×300	0.06	0.04	0.06	0.03
Couple	512×512	0.96	0.56	0.96	0.55
Pepper	1024×1024	3.92	2.29	3.87	2.22

Tabel 6. Waktu Enkripsi dan Dekripsi (s)

Referensi	NPCR (%)	UACI (%)	Entropi
[7]	99.43080	33.52930	7.99720
[15]	99.61000	33.46000	7.99920
[16]	99.61720	33.45160	7.99750
[17]	99.64000	33.51000	7.99700
Usulan Algoritma	99.65210	34.13334	7.99976

## KESIMPULAN DAN SARAN

Algoritma yang diusulkan dapat mengubah koordinat piksel dengan transposisi Cat Map dan memodifikasi intensitas warna piksel dengan substitusi Logistic Map secara acak dan simultan yang ditunjukkan dalam kurva histogram dan korelasi citra terenkripsi. Analisis NPCR, UACI dan entropi menunjukkan algoritma yang diusulkan tahan terhadap serangan entropi dan serangan diferensial. Ruang kunci algoritma yang diusulkan dapat diperbesar, dan proses waktu lebih cepat daripada kombinasi algoritma Cat Map dan Logistic Map secara berurutan atau sekuensial. Algoritma yang diusulkan memiliki hasil terbaik dari prinsip *chaos comparative* yang dibandingkan dengan algoritma lainnya.

## DAFTAR PUSTAKA

- [1] M. R. Joshi and R. A. Karkade, "Network Security with Cryptography," *Int. J. Comput. Sci. Mob. Comput.*, 2015.
- [2] Y. P. K. Nkandeu and A. Tiedeu, "An image encryption algorithm based on substitution technique and chaos mixing," *Multimed. Tools Appl.*, vol. 78, no. 8, pp. 10013–10034, 2019, doi: 10.1007/s11042-018-6612-2.
- [3] R. D. Syah and R. J. Suhatri, "Digital Image Cryptography Using Combination of Arnold's Cat Map and Bernoulli Map Based on Chaos Theory," *Int. Res. J. Adv. Eng. Sci.*, vol. 4, no. 2, pp. 258–262, 2019, doi: 10.5281/zenodo.3153337.
- [4] B. J. Saha, K. K. Kabi, and C. Pradhan, "A new approach on color image encryption using arnold 4D cat map," *Adv. Intell. Syst. Comput.*, vol. 410, pp. 131–138, 2016, doi: 10.1007/978-81-322-2734-2\_14.
- [5] R. D. Syah, S. Madenda, R. J. Suhatri, and S. Harmanto, "Hybrid Digital Image Cryptography Using Composition of Henon Map Transposition and Logistic Map Substitution," in *2022 IEEE International Conference of Computer Science and Information Technology (ICOSNIKOM)*, 2022, pp. 1–6, doi:

- 10.1109/ICOSNIKOM56551.2022.10034926.
- [6] S. Madenda, *Pengolahan Citra dan Video Digital: Teori, Aplikasi, dan Pemrograman Menggunakan MATLAB*. Erlangga, 2015.
  - [7] P. N. Lone, D. Singh, and U. H. Mir, "A novel image encryption using random matrix affine cipher and the chaotic maps," *J. Mod. Opt.*, vol. 68, no. 10, pp. 507–521, 2021, doi: 10.1080/09500340.2021.1924885.
  - [8] E. Sukirman, S. MT, and M. A. Mubarak, "The Implementation of Henon Map Algorithm for Digital Image Encryption," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 12, no. 3, p. 651, 2014, doi: 10.12928/telkomnika.v12i3.83.
  - [9] A. Benlashram, M. Al-ghamdi, R. Altalhi, and P. Kaouther, "A novel approach of image encryption using pixel shuffling and 3D chaotic map A novel approach of image encryption using pixel shuffling and 3D chaotic map," in *Journal of Physics: Conference Series*, 2020, vol. 1447, doi: 10.1088/1742-6596/1447/1/012009.
  - [10] Y. Liu and Y. C. Ko, "Image Processing Method Based on Chaotic Encryption and Wavelet Transform for Planar Design," *Adv. Math. Phys.*, vol. 2021, pp. 1–12, 2021, doi: 10.1155/2021/7511245.
  - [11] P. Ping, F. Xu, Y. Mao, and Z. Wang, "Designing permutation substitution image encryption networks with Henon map," *Neurocomputing*, vol. 283, pp. 53–63, 2018, doi: 10.1016/j.neucom.2017.12.048.
  - [12] L. Zhang, L. Zhang, and L. Zhang, "Application Research of Digital Media Image Processing Technology Based on Wavelet Transform," *J Image Video Proc*, vol. 138, no. 2018, 2018, doi: 10.1186/s13640-018-0383-6.
  - [13] A. M. Eskiciouglu and P. S. Fisher, "Image Quality: Measures and Visual Performance," *IEEE Trans. Commun.*, vol. 43, no. 12, pp. 70–90, 1995, doi: 10.1007/978-94-011-7062-8\_4.
  - [14] S. B. Kembaren, S. Suryadi, and T. Triswanto, "Implementasi Algoritma Enkripsi Citra Digital Berbasis Chaos Menggunakan Fungsi Komposisi Logistic Dan Gauss," in *Seminar Nasional Edusintek*, 2018, pp. 263–272.
  - [15] S. Kanwal *et al.*, "An Effective Color Image Encryption Based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices," *Sensors*, vol. 22, no. 12, p. 4359, 2022, doi: 10.3390/s22124359.
  - [16] Y. Chen, S. Xie, and J. Zhang, "A Hybrid Domain Image Encryption Algorithm Based on Improved Henon Map," *Entropy*, vol. 24, no. 2, pp. 1–28, 2022, doi: 10.3390/e24020287.
  - [17] N. Munir, M. Khan, A. Al Karim Haj Ismail, and I. Hussain, "Cryptanalysis and Improvement of Novel Image Encryption Technique Using Hybrid Method of Discrete Dynamical Chaotic Maps and Brownian Motion," *Multimed. Tools Appl.*, vol. 81, no. 5, pp. 6571–6584, 2022, doi: 10.1007/s11042-021-11810-2.

# Rama Paper

---

## ORIGINALITY REPORT

---

12%

SIMILARITY INDEX

6%

INTERNET SOURCES

10%

PUBLICATIONS

4%

STUDENT PAPERS

---

## PRIMARY SOURCES

---

- 1** Rama Dian Syah, Sarifuddin Madenda, Ruddy J Suhatri, Suryadi Harmanto. "Hybrid Digital Image Cryptography Using Composition of Henon Map Transposition and Logistic Map Substitution", 2022 IEEE International Conference of Computer Science and Information Technology (ICOSNIKOM), 2022  
Publication 7%
  - 2** Submitted to Universitas Gunadarma  
Student Paper 1%
  - 3** I Nyoman Purnama. "IMPLEMENTASI ALGORITMA ENKRIPSI RC5 UNTUK MENGAMANKAN GAMBAR PADA PERANGKAT ANDROID", Jurnal Informatika dan Rekayasa Elektronik, 2019  
Publication <1%
  - 4** [www.mdpi.com](http://www.mdpi.com)  
Internet Source <1%
  - 5** [www.science.gov](http://www.science.gov)  
Internet Source <1%
-

6	Makmun Makmun. "HASIL ANALISIS STATISTIK, DIFERENSIAL, DAN KUALITAS CITRA TERHADAP KOMPOSISI LOGISTIC CIRCLE MAP", Jurnal Ilmiah Teknik, 2023 Publication	<1 %
7	ml.scribd.com Internet Source	<1 %
8	repository.uksw.edu Internet Source	<1 %
9	O. Egger. "High-performance compression of visual information-a tutorial review. I. Still pictures", Proceedings of the IEEE, 6/1999 Publication	<1 %
10	ejournals.umn.ac.id Internet Source	<1 %
11	pt.scribd.com Internet Source	<1 %
12	journal.ugm.ac.id Internet Source	<1 %

Exclude quotes Off

Exclude matches Off

Exclude bibliography On