Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.2024117666
Vol. 11, No. 6, Desember 2024,, hlm. 1233-1242 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

PENGAMANAN CITRA DIGITAL MENGGUNAKAN KRIPTOGRAFI DNA DAN MODIFIED LSB

Sabrina Adela Br Sibarani[*1], Andreas Munthe[2], Ronsen Purba[3], Ali Akbar Lubis[4]

[1,2,3,4] Universitas Mikroskil, Medan
Email: [1] sabrina.sibarani@mikroskil.ac.id, [2] 181112418@alumni.mikroskil.ac.id, [3] ronsen@mikroskil.ac.id, [4] ali.akbar@mikroskil.ac.id
[*]Penulis Korespondensi

(Naskah masuk: dd mmm 23 Agustus 2023, diterima untuk diterbitkan: 20 November 2024)

Abstrak

Enkripsi citra digital menggunakan Kriptografi DNA menggabungkan ilmu komputasi dengan prinsip biologis untuk memberikan keamanan ganda. Proses enkripsi terdiri dari dua lapisan. Lapisan pertama, sistem *chaos* seperti *Arnold's Cat Map* (ACM) digunakan untuk mengacak posisi piksel melalui beberapa iterasi, sementara *Logistic Map* (LM) membangkitkan *keystream* karena sensitivitasnya yang tinggi. Lapisan kedua melibatkan karakteristik DNA, yang memanfaatkan basa nukleotida (A, T, C, G) untuk mengenkripsi data citra pada tingkat molekuler, menghasilkan tingkat keacakan yang tinggi. Setelah enkripsi, *ciphertext* disembunyikan dalam citra sampul menggunakan teknik steganografi *Modified Least Significant Bit* (MLSB), yang mengoptimalkan penyisipan bit di saluran RGB dengan pemilihan piksel acak menggunakan generator modulo. Hasil pengujian menunjukkan kualitas enkripsi yang sangat baik, dengan nilai NPCR $\geqslant$ 98%, UACI $\geqslant$ 30%, koefisien korelasi $\simeq$ 0, entropi $\simeq$ 8, dan histogram yang datar (*flat*). Kualitas *stego-image* optimal dicapai dengan penyisipan satu bit pada saluran RGB, menghasilkan PSNR $\geqslant$ 50dB. Ketahanan stego-image terhadap *noise salt* & *pepper* bergantung pada ukuran citra sampul, persentase *noise*, dan jumlah bit sisip yang digunakan. Hasil tersebut menunjukkan bahwa kombinasi Kriptografi DNA, ACM, LM, dan MLSB memberikan keamanan yang tinggi dan sulit ditembus.

Kata kunci: *kriptografi DNA, arnold's cat map, logistic map, MLSB*

DIGITAL IMAGE SECURITY USING DNA CRYPTOGRAPHY AND MODIFIED LSB

Abstract

Digital image encryption using DNA Cryptography combines computational science with biological principles to provide dual security. The encryption process consists of two layers: first, a chaotic system like Arnold's Cat Map (ACM) is used to shuffle pixel positions through several iterations, while the Logistic Map (LM) generates a keystream due to its high sensitivity. The second layer involves DNA characteristics, utilizing nucleotide bases (A, T, C, G) to encrypt image data at the molecular level, resulting in higher randomness. After encryption, the ciphertext is hidden within a cover image using Modified Least Significant Bit (MLSB) steganography, which optimizes bit insertion in the RGB channels by selecting random pixels using a modulo generator. Experimental results show excellent encryption quality, with NPCR $\geqslant$ 98%, UACI $\geqslant$ 30%, correlation coefficient close to 0, entropy close to 8, and a flat histogram. Optimal stego-image quality is achieved with a single bit insertion in the RGB channels, resulting in PSNR $\geqslant$ 50dB. The resistance of the stego-image to salt & pepper noise depends on the cover image size, noise percentage, and the number of inserted bits. The results indicate that the combination of DNA Cryptography, ACM, LM, and MLSB provides high security and is difficult to breach.

Keywords: *DNA cryptography, arnold's cat map, logistic map, MLSB*

1. PENDAHULUAN

Kemajuan teknologi komunikasi telah menyebabkan perkembangan pesat dan luasnya penggunaan citra digital di berbagai bidang. Namun, keleluasaan ini membawa potensi masalah, seperti pencurian data dan penyalahgunaan akses (Radke et al., 2021). Untuk mencegah permasalahan tersebut, perlu adanya sistem pengamanan yang dapat melindungi kerahasiaan citra digital dengan memanfaatkan teknik kriptografi dan steganografi (Samiullah et al., 2020; Zheng & Hu, 2021).

Berbagai teknik kriptografi telah diterapkan untuk melindungi citra digital. *Advanced Encryption Standard* (AES) adalah salah satu algoritme kriptografi simetris yang paling umum, menawarkan keamanan yang kuat dengan enkripsi blok data menggunakan kunci yang sama untuk proses enkripsi dan dekripsi (Alsaffar et al., 2021; Kumar et al., 2022). Meskipun AES efektif, ia sering mengalami keterbatasan dalam kecepatan pemrosesan dan pengelolaan kunci pada citra berukuran besar. RSA, sebagai algoritme kriptografi asimetris, menggunakan pasangan kunci publik dan privat untuk enkripsi dan dekripsi (Gollagi et al., 2021), namun prosesnya lebih lambat dan memerlukan sumber daya komputasi lebih banyak, menjadikannya kurang efisien untuk aplikasi pada citra digital yang memerlukan pemrosesan cepat (Akkasaligar & Biradar, 2020).

Selain itu, terdapat algoritme kriptografi lain seperti *Elliptic Curve Cryptography* (ECC). Pada penelitian yang telah dilakukan (Ullah et al., 2023) ECC menawarkan keamanan tinggi dengan ukuran kunci yang lebih kecil dibandingkan RSA, namun dapat menjadi rumit dalam implementasinya untuk citra digital yang besar (Habek et al., 2022). Di sisi lain, algoritme seperti *Blowfish* dan *Twofish* juga digunakan dalam kriptografi simetris, menawarkan kecepatan dan fleksibilitas, namun kadang kala kesederhanaannya tidak selalu mencukupi untuk aplikasi yang memerlukan tingkat keamanan ekstrem (Assa-Agyei & Olajide, 2023).

Kriptografi DNA adalah salah satu algoritme yang digunakan untuk mengamankan citra digital. Algoritme ini menawarkan keamanan ganda dengan menggabungkan *cryptosystem* pada lapisan pertama dan karakteristik DNA (*Deoxyribonucleic Acid*) pada lapisan kedua (Biswas et al., 2017; Samiullah et al., 2020). Salah satu *cryptosystem* yang dapat diterapkan adalah metode *chaotic*, yang merupakan teknik enkripsi berbasis kekacauan dan efektif dalam menghadapi berbagai serangan seperti *brute-force attack* dan *cryptanalysis* (Liu & Liu, 2020; Luo et al., 2019; Xuejing & Zihui, 2020). *Chaotic system* memiliki sifat yang sensitif karena *cipher image* tidak akan kembali ke citra awal apabila kunci yang digunakan pada proses dekripsi berbeda dengan kunci sewaktu proses enkripsi dilakukan (Ibrahim et al., 2024; Singh et al., 2023). Contoh *chaotic system* antara lain *Arnold's Cat Map*, *Tent Map*, *Baker's Map*, *Circle Map*, *Logistic Map* dan lain sebagainya (Lan et al., 2018; Pourjabbar Kari et al., 2021; Qayyum et al., 2020).

Pada tahun 2016, Awdun dan Li melakukan penelitian mengenai gabungan DNA *Encoding* dan *Sine Chaos*. Teknik enkripsi yang digunakan melibatkan permutasi dan difusi dengan memisahkan citra menjadi komponen R, G, B, dan kemudian mengenkodasi berdasarkan operasi DNA serta mengacaknya menggunakan *Sine Chaos* (Awdun & Li, 2016). Namun, penerapan algoritme tersebut menyebabkan redundansi pada *pixel*, sehingga muncul celah untuk mendekripsi *cipher image*. Oleh karena itu, dalam penelitian ini, *chaotic system* yang akan digunakan adalah *Arnold's Cat Map* (ACM) dan *Logistic Map* (LM). Berdasarkan penelitian yang dilakukan oleh Farhan bersama tim pada tahun 2018, penggunaan ACM menjadi penting untuk mengacak susunan *pixel* melalui beberapa iterasi hingga membentuk pola yang tidak beraturan, sementara LM digunakan untuk menghasilkan *keystream* karena sensitivitasnya yang baik. Secara spesifik, algoritme ini memiliki periode berulang, tingkat keacakan, dan sensitivitas yang tinggi, hal ini didukung oleh hasil penelitian yang menunjukkan bahwa penggunaan ACM dan LM dalam proses enkripsi menghasilkan skor NPCR $\geq$ 98%, UACI $\geq$ 33,3%, dan *correlation coefficient* $\simeq$ 0 (Musanna et al., 2018; Raj et al., 2019; Zareai et al., 2021).

Penggunaan teknik kriptografi DNA, *Arnold's Cat Maps*, dan *Logistic Map* pada proses enkripsi akan menghasilkan citra acak yang tidak terbaca dan tidak dapat dikenali, dengan demikian akan menimbulkan kecurigaan dari pihak lain. Untuk mengatasi masalah ini, dilakukan penyembunyian pesan ke dalam media citra menggunakan teknik steganografi. Salah satu metode yang sering digunakan dalam steganografi adalah *Least Significant Bit* (LSB), di mana beberapa bit pesan disisipkan ke dalam bit-bit sampul untuk menghasilkan *stego-image*. Dalam penelitian sebelumnya, metode LSB telah terbukti efisien dan sederhana dalam menyisipkan dan mengekstraksi pesan, memiliki *imperceptibility* yang baik, dan citra yang membawa pesan tidak mengalami perubahan yang signifikan (Kumar et al., 2022; Nie et al., 2019; Panwar et al., 2020). Namun, kelemahan LSB terletak pada kurangnya pertimbangan terhadap bit-bit lain selain *Least Significant Bit*, serta penyisipan bit yang bersifat sekuensial dan tidak terdistribusi secara merata, yang menyebabkan *stego-image* dapat dengan mudah terdeteksi dan diserang (Poi Wong et al., 2019). Untuk mengatasi kelemahan tersebut, dilakukan modifikasi terhadap metode LSB dengan menambahkan proses penentuan jumlah bit yang akan disisipkan serta pemilihan saluran yang beragam. Selain itu, penentuan posisi penyisipan bit, dilakukan melalui proses seleksi *pixel* acak dengan generator modulo (Adha Oktarini Saputri & Epa Sari, 2023; Emad et al., 2018; Emam et al., 2016). Dengan cara ini, penyerang akan kesulitan menemukan bit-bit yang disisipkan karena hal ini bergantung pada ukuran sampul, jumlah bit yang disisipkan, dan saluran yang digunakan.

Berdasarkan uraian di atas, penelitian ini bertujuan untuk menghasilkan sistem pengamanan citra digital menggunakan kombinasi kriptografi DNA dan *Modified Least Significant Bit* (MLSB). Pengujian akan dilakukan untuk mengetahui kualitas hasil enkripsi, pengaruh parameter masukan jumlah bit yang disisipkan dan *channel* yang digunakan

terhadap kualitas *stego-image*, serta ketahanan *stego-image* terhadap serangan *noise*.

2. METODE PENELITIAN

Dalam penelitian ini, digunakan algoritma kriptografi DNA, *Arnold's Cat Map*, dan *Logistic Map* untuk pelaksanaan proses enkripsi dan dekripsi, serta metode *modified* LSB untuk proses penyisipan dan ekstraksi.

2.1. Kriptografi DNA

Kriptografi DNA merupakan pendekatan baru yang berkembang pesat dalam bidang kriptografi, dengan fokus pada urutan DNA. Konsep kriptografi DNA terinspirasi dari molekul DNA yang memiliki kemampuan untuk menyimpan, memproses, dan mengirimkan informasi (Alsaffar et al., 2021; Singh et al., 2023). DNA (*Deoxyribonucleic Acid*) atau Asam Deoksiribonukleat merupakan materi genetik yang kompleks berfungsi sebagai pembawa informasi genetik yang diwariskan oleh semua makhluk hidup, mulai dari virus yang sangat kecil hingga manusia. Struktur DNA terdiri dari dua untai heliks yang saling antiparallel (Hammad et al., 2020; Samiullah et al., 2020). DNA sendiri merupakan polimer panjang yang tersusun atas unit-unit kecil yang disebut nukleotida. Setiap nukleotida terdiri dari tiga komponen utama: basa nitrogen, gula lima karbon, dan gugus fosfat. Terdapat empat jenis nukleotida, yang dibedakan berdasarkan jenis basa nitrogen yang dikandungnya, yaitu Adenin (A), Sitosin (C), Timin (T), dan Guanin (G). Meskipun hanya terdiri dari empat basa nitrogen ini, DNA mampu menyimpan informasi genetik yang sangat kompleks dan dalam jumlah besar. Ikatan hidrogen terbentuk antara pasangan basa yang spesifik, yaitu antara Adenin (A) dengan Timin (T), dan Sitosin (C) dengan Guanin (G), yang menjaga stabilitas dua untai (Iliyasu et al., 2021).

1) DNA encoding

Rangkaian DNA terdiri dari empat basa asam nukleat, yaitu A (*adenin*), C (*sitosin*), G (*guanin*), dan T (*timin*), di mana pasangan A dan T serta G dan C saling berpasangan. Seperti dalam sistem biner di mana 0 dan 1 saling berpasangan, begitu pula 00 dan 11, serta 01 dan 10 berpasangan. Dengan menggunakan empat basis A, C, G, dan T untuk menyandikan 00, 01, 10, dan 11. Dari keempat asam nukleat dasar tersebut, terdapat 24 kombinasi yang mungkin, tetapi hanya 8 kombinasi yang sesuai dengan aturan pasangan seperti yang ditunjukkan pada Tabel 1 di bawah ini (Xuejing & Zihui, 2020).

Tabel 1. Aturan *complementary* DNA *encoding*

Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
00-A	00-A	00-C	00-C	00-G	00-G	00-T	00-T
01-C	01-G	01-A	01-T	01-A	01-T	01-C	01-G
10-G	10-C	10-T	10-A	10-T	10-A	10-G	10-C
11-T	11-T	11-G	11-G	11-C	11-C	11-A	11-A

Dalam proses pengkodean DNA, setiap *nukleotida* biasanya direpresentasikan dengan nomor biner yang mengikuti aturan pasangan, contohnya: A - 00; C - 01; G - 10; T - 11. Sebagai hasilnya, nilai desimal 177 (10 11 00 01) akan diwakili sebagai urutan DNA CTAG. Nilai piksel 8-bit dari gambar diubah menjadi empat urutan DNA 2-bit.

2) DNA *addition* dan *substraction*

Proses *addition* dan *substraction* pada urutan DNA memiliki kemiripan dengan perhitungan aljabar tradisional. Penjumlahan dan pengurangan dijalankan pada modulo 4 dengan menambahkan angka pada DNA. Tujuan dari penjumlahan dan pengurangan adalah untuk mengubah dan mengembalikan nilai *pixel* pada citra. *Addition* dan *substraction* memiliki aturan tersendiri, mirip dengan proses *encoding*. Rincian mengenai aturan tersebut dapat ditemukan pada tabel 2 berikut ini.(Xuejing & Zihui, 2020).

Tabel 2. Aturan *addition* dan *substraction* pada DNA

DNA addition rule					DNA *substraction rule*				
(+)	A	T	C	G	(-)	A	T	C	G
G	G	C	T	A	G	G	T	C	A
C	C	A	G	T	C	C	G	A	T
T	T	G	A	C	T	T	A	G	C
A	A	T	C	G	A	A	C	T	G

Langkah dalam DNA *addition* dan DNA *subtraction operation*:

a. *Plain-image* dipecah menjadi tiga bagian R (M, N), G (M, N), B (M, N) seperti berikut:

$$\begin{aligned} R &= \{r_1, r_2, \dots r_{M\times N}\} \\ G &= \{g_1, g_2, \dots g_{M\times N}\} \\ B &= \{b_1, b_2, \dots b_{M\times N}\} \end{aligned} \quad (1)$$

b. Konversi matriks R, G, B yang sudah dipecah dari matriks desimal ke matriks biner seperti R_b (M, N x 4), G_b (M, N x 4) dan B_b (M, N x 4).

c. Terapkan pengkodean DNA dengan menggunakan *rule* pada tabel 2 untuk menghasilkan tiga matriks DNA R_c (M, N x 4), G_c (M, N x 4) dan B_c (M, N x 4). Kemudian *encoding* matriks tadi dengan operasi DNA *addition* pada tabel 2 (bagian kiri) untuk menghasilkan tiga matriks pengkodean sebagai berikut:

$$\left.\begin{aligned} R_e &= R_c + G_c \\ G_e &= G_c + B_c \\ B_e &= B_c + G_e \end{aligned}\right\} \quad (2)$$

Sedangkan untuk proses DNA *subtraction* menggunakan tabel 2 (bagian kanan) untuk mendapatkan DNA matriks pengkodean R_c, G_c, dan B_c dengan pengkodean sebagai berikut:

$$\left.\begin{aligned} B_c &= B_e - G_e \\ G_c &= G_e - B_c \\ R_c &= R_e - G_c \end{aligned}\right\} \quad (3)$$

3) DNA decoding

DNA *decoding* adalah proses untuk mengonversi nilai DNA menjadi nilai desimal atau biner, dengan tujuan agar nilai tersebut dapat digunakan selanjutnya. Proses *decoding* harus sesuai dengan *rule encoding* yang telah diterapkan sebelumnya. (Xuejing & Zihui, 2020). Berikut proses *decoding* dapat dilihat pada Tabel 3

Tabel 3. Aturan *complementary* DNA *decoding*

Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
A-00	A-00	C-00	C-00	G-00	G-00	T-00	T–00
C-01	G-01	A-01	T-01	A-01	T-01	C-01	G–01
G-10	C-01	T-10	A-10	T-10	A-10	G-10	C–10
T-11	T-11	G-11	G-11	C-11	C-11	A-11	A–11

2.2. *Arnold's Cat Map* (ACM)

ACM merupakan perkembangan dari fungsi *chaos* yang awalnya ditemukan oleh Vladimir Arnold (1960), dan kata "*cat*" digunakan karena penggunaan citra seekor kucing dalam eksperimen tersebut (Raj et al., 2019). Perhitungan ACM menggunakan rumus yang dapat dilihat pada persamaan (4) di bawah ini:

$$\begin{bmatrix} X_{i+1} \\ Y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} X_i \\ Y_i \end{bmatrix} mod\ (N) \quad (4)$$

Keterangan :

X_i, Y_i = Posisi *pixel* dalam citra berukuran N x N

X_{i+1}, Y_{i+1} = Posisi *pixel* yang baru setelah transformasi

b dan c = bilangan bulat sembarang

Persamaan dekripsi *Arnold's Cat Map* yaitu:

$$\begin{bmatrix} X_i \\ Y_i \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix}^{-1} \begin{bmatrix} X_{i+1} \\ Y_{i+1} \end{bmatrix} mod\ (N) \quad (5)$$

2.3. *Logistic Map* (LM)

Logistic map merupakan sistem *chaos* sederhana yang dinyatakan sebagai persamaan iteratif berikut:

$$X_{i+1} = \lambda X_i(1 - X_i) \quad (6)$$

Keterangan:

X_i = Interval angka antara 0 dan 1. Parameter x disebut juga sebagai nilai *chaos* ($0 \leq x \leq 1$)

λ = Parameter fungsi yang menyatakan laju pertumbuhan dengan nilai antara [0,4]

Nilai X_i antara $0 \leq X_i \leq 1$, dan μ merupakan parameter fungsi yang menyatakan laju pertumbuhan bernilai $0 \leq \lambda \leq 4$. LM bersifat *chaos* jika bernilai $3.5699456 \leq \lambda \leq 4$ (Luo et al., 2019). Setelah proses pembangkitan *keystream*, *cipher–image* akan disubstitusi XOR menggunakan skema *cipher block chaining* dengan persamaan:

$$C_i = (P_i\ XOR\ C_{i-1})\ XOR\ K_i \quad (7)$$

2.4. *Modified Least Significant Bit* (MLSB)

Modifikasi yang diterapkan pada metode LSB melibatkan penambahan langkah-langkah untuk menentukan jumlah bit yang akan disisipkan dan memilih saluran yang beragam. Selain itu, untuk menentukan posisi penyisipan, digunakan proses seleksi *pixel* secara acak dengan bantuan generator modulo.

1) *Greatest Common Divisor* (GCD)

Greatest Common Divisor (GCD) atau Faktor Persekutuan Terbesar (FPB) digunakan untuk menguji apakah sebuah bilangan yang lebih kecil dari m merupakan bilangan yang relatif prima. Dua bilangan dapat disebut relatif prima apabila GCD (m,a)=1. Untuk mencari dua bilangan bulat yang relative prima dapat menggunakan algoritme *euclidean* karena algoritme ini didasarkan pada asumsi bahwa terdapat dua bilangan bulat positif, yaitu m dan n, dengan m≥n. Berikut adalah tahapan dalam algoritme *Euclidean*:

a. Apabila n = 0 maka m merupakan $FPB(m,n)$; stop. Namun jika n ≠ 0, maka lanjutkan ke langkah 2.

b. Bagi nilai m dengan n dan misalkan sisanya adalah r; ganti nilai m dengan nilai n dan nilai n dengan nilai r, kemudian ulangi ke langkah a kembali.

2) Order Modulo

Bilangan asli z disebut sebagai order dari bilangan asli a dalam modulo bilangan asli m jika a dan m adalah relative prima, $a\ z \equiv 1 \pmod m$, dan z adalah bilangan asli terkecil yang memiliki sifat ini. karakteristik menarik yang terkait dengan order modulo, yaitu jika $a\ k \equiv 1 \pmod m$ dan z adalah order dari a modulo m maka z akan membagi k. Dengan demikian, z adalah bilangan asli terkecil yang memenuhi $a^k \equiv \pmod m$ sehingga k harus < dari z. Bilangan k dapat dituliskan dalam bentuk $k=qz+r$ dengan q adalah bilangan asli dan r adalah bilangan cacah r yang memenuhi $0 \leq r < z$.

$$\begin{aligned} .a^k &\equiv 1 \pmod m\ a \\ a^{qz+r} &\equiv 1 \pmod m \\ (a^z)^q\ .\ a^r &\equiv 1\ (mod\ m) \\ a^r &\equiv 1\ (mod\ m) \end{aligned} \quad (8)$$

3) Fungsi phi *euler* (∅)

Fungsi phi *euler* (∅) didefinisikan sebagai jumlah bilangan bulat positif yang lebih kecil dari bilangan bulat tertentu dan relatif prima terhadap bilangan bulat tersebut. Misalnya, jika kita memiliki bilangan bulat positif n, maka ∅(n) akan memberikan banyaknya bilangan bulat positif yang lebih kecil dari n dan relatif prima terhadap n. Meskipun disebut "phi," fungsi ini sama sekali tidak terkait dengan nilai phi (∅) yang dikenal sebagai bilangan emas 1,61803399. Penggunaan simbol phi (∅) di sini hanya untuk sebuah 'fungsi'. Jika n merupakan bilangan prima, maka

$$\emptyset\ (n) = n - 1 \quad (9)$$

4) Bilangan Prima

Bilangan prima merupakan bilangan bulat positif yang lebih besar dari 1 dan memiliki dua faktor pembagi yang berbeda, yaitu 1 dan dirinya sendiri. Dengan kata lain, bilangan prima adalah bilangan bulat positif, kecuali 0 dan 1, yang tidak dapat dipecah menjadi faktor-faktor bilangan lain selain 1 dan bilangan itu sendiri. Bilangan untuk ini misalnya 2, 3, 5, 7 , 11, 13, 17 … dan seterusnya. Cara paling mudah untuk mendapatkan bilangan prima dengan bilangan yang kecil adalah dengan menggunakan metode *Sieve Eratosthenes*. Metode ini membuat daftar bilangan dari 1 hingga n, dan mencoret bilangan kelipatan dari daftar. Algoritme sebagai berikut:

a. Membuat daftar bilangan 1 – n.
b. Menandai bahwa bilangan 1 adalah Prima (dalam beberapa pendapat menyatakan bahwa bilangan 1 bukanlah prima).
c. Menandai bilangan 2 adalah prima, kemudian mencoret semua bilangan kelipatan dari 2. Karena kelipatan 2 bukanlah bilangan prima.
d. Menandai bilangan 3 adalah prima serta mencoret semua kelipatan 3 sebagai bukan prima.
e. Mengulangi proses pada b dan seterusnya sampai kemudian semua bilangan yang bukan prima telah habis tercoret.
f. Bilangan yang tidak dicoret adalah daftar bilangan prima.

5) Fast Exponential

Fast Exponential digunakan untuk melakukan operasi pemangkatan dengan cepat pada bilangan bulat modulo. Dalam metode ini, ekspansi biner dari eksponen dimanfaatkan. Misalkan kita memiliki himpunan G, dan g ϵ G, sedangkan z adalah bilangan bulat positif. Untuk menghitung g^z menggunakan metode *fast exponentiation*, langkah-langkahnya adalah sebagai berikut:

a. Hitung $g^{2^i}, 0 \leq 1 < k$
b. Nilai g^z adalah hasil perkalian darix nilai-nilai g^{2^i}, dengan a_1=1. Diperoleh bahwa

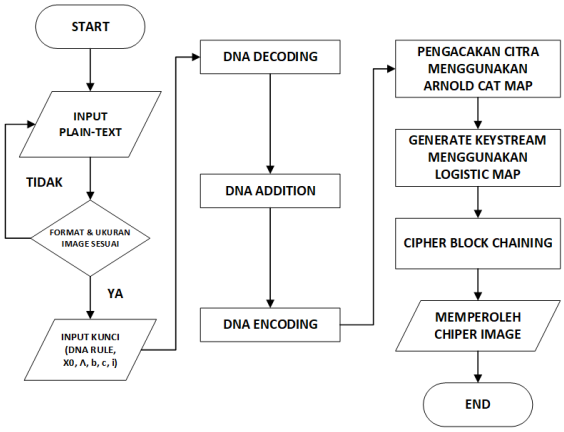
$$g^{2^{i+1}} = \left(g^{2^i}\right)^2 \qquad (10)$$

2.5. Analisis Proses

Dalam analisis proses, akan diuraikan langkah-langkah penyelesaian masalah pada sistem yang dibangun, yang mencakup analisis proses enkripsi, penyisipan, ekstraksi, dan dekripsi terhadap citra.

Proses Enkripsi

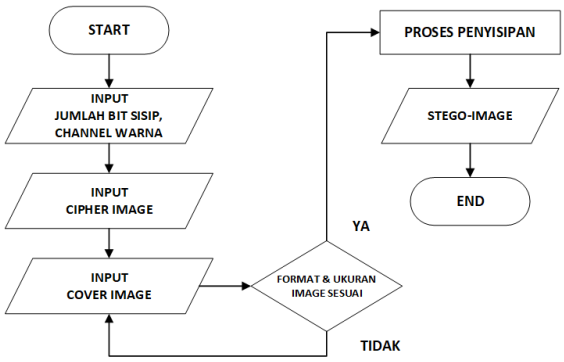
Proses enkripsi meliputi pengacakan *plain image* dengan mengubah posisi RGB menggunakan pengkodean DNA, algoritme *Arnold's Cat Map* dan pembangkit *keystream* dengan algoritme *Logistic Map*. *Flowchart* proses enkripsi dapat dilihat pada Gambar 1.



Gambar 1. *Flowchart* proses enkripsi

Proses Penyisipan

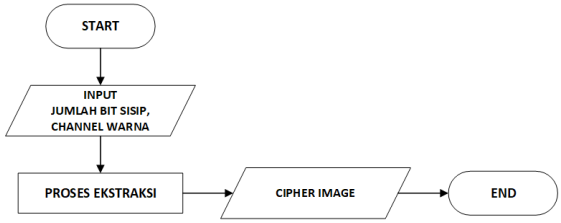
Proses penyisipan ke dalam citra sampul menggunakan MLSB *(Modified Least Significant Bit*) seleksi *pixel* acak dengan generator modulo. *Flowchart* proses penyisipan dapat dilihat pada Gambar 2.



Gambar 2. *Flowchart* proses penyisipan

Proses Ekstraksi

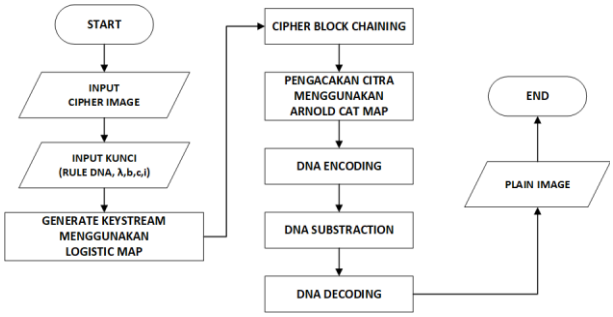
Proses ekstraksi merupakan kebalikan dari proses penyisipan karena pada tahap ini citra sampul yang sudah disisipkan pesan akan diekstrak. *Flowchart* proses ekstraksi dapat dilihat pada Gambar 3.



Gambar 3. *Flowchart* proses ekstraksi

Proses Dekripsi

Proses dekripsi adalah kebalikan proses enkripsi. Proses dekripsi dilakukan dengan mengubah citra terenkripsi atau *cipher-image* menjadi citra asli atau *plain image*. *Flowchart* proses dekripsi dapat dilihat pada Gambar 4.



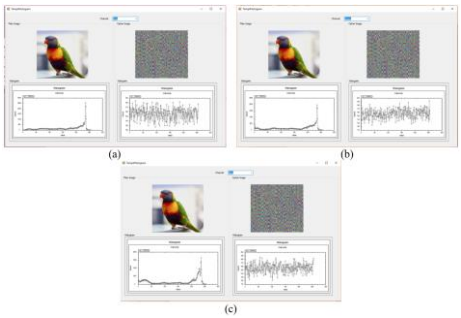
Gambar 4. *Flowchart* proses dekripsi

3. HASIL DAN PENGUJIAN

Hasil didapatkan dari pengujian yang telah dilakukan yaitu pengujian kualitas enkripsi, kualitas *stego-image*, dan ketahanan *stego-image.*

3.1.1 Kualitas Enkripsi

Pengujian kualitas enkripsi dilakukan dengan melihat tampilan histogram serta menghitung nilai NPCR, UACI, entropi, dan *correlation coefficient* pada citra berukuran 200x200px dengan aturan DNA yang digunakan adalah 1 dan 8, serta aturan *Arnold's Cat Map* dan *Logistic Map* kunci yang digunakan: b = 1, c = 1, i = 10, X0 = 0,0000001, λ = 3,5699456. Gambar 5, Tabel 4 dan Gambar 7 menunjukkan hasil pengujian kualitas enkripsi.



Gambar 5. Tampilan histogram (a)*layer red*, (b)*layer green*, (c)*layer blue*

Berdasarkan data hasil pengujian pada Tabel 4 dan Tabel 5, proses enkripsi menggunakan algoritme kriptografi DNA menghasilkan nilai NPCR > 98%, UACI > 30%, *correlation coefficient*≃0, serta nilai entropi≃8 dan histogram pada Gambar 5 terlihat datar (*flat*). Hal tersebut membuktikan bahwa kulitas pengacakan menggunakan algoritme tersebut sangat baik.

3.1.2 Kualitas Stego-image

Pengujian ini dilakukan untuk mengetahui *imperceptibility stego-image* terhadap perubahan parameter jumlah bit sisip dan saluran, *cipher image* serta ukuran sampul yang digunakan. Pengujian ini menggunakan citra hasil enkripsi yang akan disisip ke dalam sampul dengan jumlah bit sisip antara 1, 2 dan 4 sedangkan saluran yang dapat digunakan yaitu R, G, B, RG, RB, BG dan RGB. Kemudian dari hasil pengujian yang dilakukan akan mendapatkan nilai MSE dan PSNR. Tabel 6 dan Tabel 7 akan menunjukkan tampilan dan hasil pengujian kualitas *stego–image*.

Berdasarkan data hasil pengujian pada Tabel 6 dan Tabel 7 dengan ukuran dan jenis *cipher-image* yang sama, dapat dilihat bahwa jumlah bit sisip dan jenis saluran mempengaruhi nilai PSNR. Pengujian yang telah dilakukan menunjukkan kualitas *stego–image* yang baik diperoleh jika jumlah bit sisipnya satu pada saluran RGB dengan nilai PSNR di atas 50dB.

3.1.3 Ketahanan *Stego-image*

Pada penelitian ini, pengujian ketahanan *stego-image* dilakukan untuk mengetahui ketahanan *stego-image* terhadap serangan menggunakan *noise salt & pepper* dengan menghitung nilai *recovery rate*. Tampilan dan hasil pengujian ketahanan *stego–image* dapat dilihat pada Gambar 9, Tabel 8 dan Tabel 9.

Tabel 4. Hasil pengujian 1 kualitas enkripsi

No.	b	c	i	X0	λ	NPCR	UACI	Entropy	CCRed	CCGreen	CCBlue
1	1	1	10	0,0000001	3,5699456	98,8850	30,7334	7,9654	0,6556	0,8126	0,7937
2	1	4	10	0,0000001	3,5699456	98,8225	30,8508	7,9627	-0,8392	-0,7904	0,5944
3	1	7	10	0,0000001	3,5699456	98,8175	30,8657	7,9656	-0,6219	0,6624	0,8872
4	1	10	10	0,0000001	3,5699456	98,8600	30,7864	7,9644	-0,8862	0,9496	-0,0167
5	4	1	10	0,0000001	3,5699456	98,8625	30,8404	7,9637	-0,3509	-0,0316	0,3519
6	4	4	10	0,0000001	3,5699456	98,8025	30,9841	7,9637	0,6374	-0,9366	0,0219
7	4	7	10	0,0000001	3,5699456	98,8000	30,8434	7,9614	0,7297	-0,8955	0,2999
8	4	10	10	0,0000001	3,5699456	98,8750	30,9342	7,9669	-0,9431	-0,9592	0,3376
9	7	1	10	0,0000001	3,5699456	98,9550	30,8322	7,9659	0,9228	-0,2543	0,7474
10	7	4	10	0,0000001	3,5699456	98,8800	30,8801	7,9643	-0,8211	-0,6273	0,5642
11	7	7	10	0,0000001	3,5699456	98,7425	30,8585	7,9646	0,8080	0,1286	-0,8451
12	7	10	10	0,0000001	3,5699456	98,7425	30,7463	7,9642	-0,6313	0,4554	0,8901
13	10	1	10	0,0000001	3,5699456	98,7925	30,8156	7,9658	0,6856	-0,2509	0,9609
14	10	4	10	0,0000001	3,5699456	98,7925	30,8501	7,9631	0,4120	0,8084	-0,9360

No.	b	c	i	X0	λ	NPCR	UACI	Entropy	CCRed	CCGreen	CCBlue
15	10	7	10	0,0000001	3,5699456	98,8100	30,9929	7,9651	0,4548	0,9046	-0,8476
16	10	10	10	0,0000001	3,5699456	98,9025	31,0093	7,9627	-0,6792	0,8097	-0,6814

	RATA-RATA	MINIMUM	MAKSIMUM
NPCR	98,8497	98,7050	98,9600
UACI	30,8278	30,6003	31,0182
ENTROPY	7,9641	7,96120	7,9669

Tabel 5. Hasil pengujian 2 kualitas enkripsi

No.	b	c	i	X0	λ	NPCR	UACI	Entropy	CCRed	CCGreen	CCBlue
1	1	1	10	0,0000001	3,5699456	98,8350	30,8037	7,9643	0,6554	-0,8653	0,7648
2	1	4	10	0,0000001	3,5699456	98,8325	31,1394	7,9634	-0,9498	-0,6104	-0,5308
3	1	7	10	0,0000001	3,5699456	98,8500	30,7322	7,9650	0,9055	0,9588	0,8805
4	1	10	10	0,0000001	3,5699456	98,8800	30,9902	7,9640	-0,1136	0,5849	0,6763
5	4	1	10	0,0000001	3,5699456	98,9225	30,8350	7,9662	-0,1873	-0,8771	0,1849
6	4	4	10	0,0000001	3,5699456	98,9725	30,9355	7,9640	0,3400	-0,2137	0,4556
7	4	7	10	0,0000001	3,5699456	98,7475	30,7715	7,9637	0,5371	0,1642	0,9086
8	4	10	10	0,0000001	3,5699456	98,8700	31,0736	7,9645	0,6316	-0,8890	-0,3992
9	7	1	10	0,0000001	3,5699456	98,8150	30,8265	7,9651	-0,9383	0,1031	0,7189
10	7	4	10	0,0000001	3,5699456	98,7950	30,8451	7,9663	0,8995	-0,5866	0,9534
11	7	7	10	0,0000001	3,5699456	98,8050	30,8404	7,9639	0,3124	-0,7359	0,2037
12	7	10	10	0,0000001	3,5699456	98,9100	30,8311	7,9629	-0,6753	-0,8529	-0,2950
13	10	1	10	0,0000001	3,5699456	98,7200	30,8858	7,9634	0,8871	-0,7531	0,9059
14	10	4	10	0,0000001	3,5699456	98,7800	30,9245	7,9663	-0,7985	-0,4942	-0,9661
15	10	7	10	0,0000001	3,5699456	98,8550	30,8893	7,9650	-0,9023	0,8686	-0,9424
16	10	10	10	0,0000001	3,5699456	98,8950	30,9018	7,9645	0,1793	0,7879	-0,7210

	RATA-RATA	MINIMUM	MAKSIMUM
NPCR	98,8330	98,7025	98,9725
UACI	30,8804	30,6759	31,1394
ENTROPY	7,9645	7,9623	7,9671

Tabel 6. Data hasil pengujian 1 kualitas *stego - image*

No.	Jumlah Bit Sisip	Channel	Mse	Psnr (dB)
1	1	RG	0,12989	56,75329
2	1	RB	0,12956	56,76427
3	1	BG	0,12917	56,81223
4	1	R	0,17534	55,45013
5	1	G	0,17749	55,39741
6	1	B	0,17493	55,46028
7	1	RGB	0,10764	57,56919
8	2	RGB	0,1655	55,77083
9	2	R	0,2078	54,71258
10	2	G	0,21016	54,66359
11	2	B	0,20705	54,76327
12	2	RG	0,17818	55,31017
13	2	RB	0,17423	55,44283
14	2	BG	0,17856	55,4062
15	4	G	1,2171	47,07071
16	4	B	1,05899	47,67505
17	4	R	1,20753	47,13982
18	4	RGB	1,13684	47,50543
19	4	RG	1,14594	47,36717
20	4	RB	1,14861	47,39175
21	4	BG	1,11756	47,4761

Tabel 7. Data hasil pengujian 2 kualitas *stego – image*

No.	Jumlah bit Sisip	Channel	Mse	Psnr (dB)
1	1	RG	0,12777	57,06638
2	1	RB	0,12693	57,09518
3	1	BG	0,12632	57,11593
4	1	R	0,17014	55,82262
5	1	G	0,16903	55,85126
6	1	B	0,17029	55,81895
7	1	RGB	0,10605	57,87571
8	2	RGB	0,16821	55,8722
9	2	R	0,20824	54,94509
10	2	G	0,20812	54,94768
11	2	B	0,21	54,90863
12	2	RG	0,17798	55,62709
13	2	RB	0,17646	55,66442
14	2	BG	0,17927	55,5958
15	4	RGB	1,27	47,09278
16	4	RG	1,26895	47,09635
17	4	RB	1,27193	47,08617
18	4	BG	1,24763	47,16996
19	4	R	1,39894	46,67281
20	4	G	1,22866	47,23648
21	4	B	1,20108	47,33509

Tabel 8. Data hasil pengujian 1 ketahanan stego-image

No.	Nama File	Ukuran Plain-image	Ukuran Stego-image	Bit Sisip	Channel	Persentase Noise (%)	Recovery Rate
1	stegoimage-Cipher-image	80 x 80 px	200 x 200 px	4	RGB	0,005	100%
2	stegoimage-Cipher-image	80 x 80 px	200 x 200 px	4	RGB	0,006	100%
3	stegoimage-Cipher-image	80 x 80 px	200 x 200 px	4	RGB	0,007	99,97%

Tabel 9. Data hasil pengujian 2 ketahanan stego-image

No.	Nama File	Ukuran Plain-image	Ukuran Stego-image	Bit Sisip	Channel	Persentase Noise (%)	Recovery Rate
1	stegoimage-Cipher-image_500	80 x 80 px	500 x 500 px	4	RGB	0,005	100%
2	stegoimage-Cipher-image_500	80 x 80 px	500 x 500 px	4	RGB	0,006	100%
3	stegoimage-Cipher-image_500	80 x 80 px	500 x 500 px	4	RGB	0,007	100%
4	stegoimage-Cipher-image_500	80 x 80 px	500 x 500 px	4	RGB	0,008	100%
5	stegoimage-Cipher-image_500	80 x 80 px	500 x 500 px	4	RGB	0,009	100%
6	stegoimage-Cipher-image_500	80 x 80 px	500 x 500 px	4	RGB	0,01	100%
7	stegoimage-Cipher-image_500	80 x 80 px	500 x 500 px	4	RGB	0,011	100%
8	stegoimage-Cipher-image_500	80 x 80 px	500 x 500 px	4	RGB	0,012	99,97%

Hasil pengujian data pada Tabel 8 dan Tabel 9 menunjukkan bahwa ketahanan *stego-image* terhadap *noise salt* & *pepper* beragam, tergantung ukuran citra sampul yang digunakan, persentase *noise* yang diberikan, dan jumlah bit sisip saat proses *embedding*.

4. KESIMPULAN

Berdasarkan pengujian yang telah dilakukan, algoritme Kriptografi DNA menunjukkan hasil yang sangat baik dengan nilai NPCR $\geqslant$ 98%, UACI $\geqslant$ 30%, *correlation coefficient* mendekati 0, entropi $\simeq$ 8, serta histogram yang terlihat *flat*. Hal ini membuktikan bahwa teknik pengacakan yang diterapkan sangat efektif dalam menghasilkan *cipher-image* yang sulit dianalisis. Selain itu, penggunaan *Arnold's Cat Map* (ACM) dan *Logistic Map* (LM) memberikan kontribusi signifikan dalam menciptakan *keystream* yang sensitif dan aman, menjamin kerahasiaan citra yang terenkripsi. Pada teknik steganografi, metode *Modified Least Significant Bit* (MLSB) menunjukkan hasil optimal dengan penyisipan satu bit pada saluran RGB, menghasilkan *stego-image* dengan kualitas tinggi, di mana nilai PSNR $\geqslant$ 50dB. Namun, ketahanan *stego-image* terhadap *noise* juga dipengaruhi oleh ukuran citra sampul dan tingkat *noise* yang ditambahkan. Dengan demikian, kombinasi teknik Kriptografi DNA, ACM, LM, dan MLSB membuktikan bahwa metode yang diusulkan tidak hanya menghasilkan kualitas enkripsi yang kuat tetapi juga mampu mempertahankan kualitas steganografi secara optimal.

DAFTAR PUSTAKA

ADHA OKTARINI SAPUTRI, N., & EPA SARI, N. 2023. Information Security Analysis and Solution using LSB Steganography and AES Cryptographic Algorithm. In *JOURNAL OF DATA SCIENCE* | (Vol. 2023).

AKKASALIGAR, P. T., & BIRADAR, S. 2020. Selective medical image encryption using DNA cryptography. In *Information Security Journal* (Vol. 29, Issue 2, pp. 91–101). Taylor and Francis Inc. https://doi.org/10.1080/19393555.2020.1718248

ALSAFFAR, Q. S., MOHAISEN, H. N., & ALMASHHDINI, F. N. 2021. An encryption based on DNA and AES algorithms for hiding a compressed text in colored Image. *IOP Conference Series: Materials Science and Engineering*, *1058*(1), 012048. https://doi.org/10.1088/1757-899x/1058/1/012048

ASSA-AGYEI, K., & OLAJIDE, F. 2023. A Comparative Study of Twofish, Blowfish, and Advanced Encryption Standard for Secured Data Transmission. *International Journal of Advanced Computer Science and Applications*, *14*(3), 393–398. https://doi.org/10.14569/IJACSA.2023.0140344

AWDUN, B., & LI, G. 2016. *The Color Image Encryption Technology Based on DNA Encoding & Sine Chaos*. https://doi.org/10.1109/ICSCSE.2016.33

BISWAS, MD. R., ALAM, K. MD. R., AKBER, A., & MORIMOTO, Y. 2017. *A DNA*

Cryptographic Technique Based on Dynamic DNA Encoding and Asymmetric Cryptosystem.

EMAD, E., SAFEY, A., REFAAT, A., OSAMA, Z., SAYED, E., & MOHAMED, E. 2018. A secure image steganography algorithm based on least significant bit and integer wavelet transform. *Journal of Systems Engineering and Electronics*, *29*(3), 639–649. https://doi.org/10.21629/JSEE.2018.03.21

EMAM, M. M., ALY, A. A., & OMARA, F. A. 2016. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 7, Issue 3). www.ijacsa.thesai.org

GOLLAGI, S. G., SRIVIDYA, R., SANTHOSH KUMAR, G., & PAREEK, P. K. 2021. A New Method of Secure Image Encryption by Using Enhanced RSA Algorithm. *2021 International Conference on Forensics, Analytics, Big Data, Security, FABS 2021*. https://doi.org/10.1109/FABS52071.2021.9702550

HABEK, M., GENC, Y., AYTAS, N., AKKOC, A., AFACAN, E., & YAZGAN, E. 2022. Digital Image Encryption Using Elliptic Curve Cryptography: A Review. *HORA 2022 - 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings*. https://doi.org/10.1109/HORA55278.2022.9800074

HAMMAD, B. T., SAGHEER, A. M., AHMED, I. T., & JAMIL, N. 2020. A comparative review on symmetric and asymmetric dna-based cryptography. *Bulletin of Electrical Engineering and Informatics*, *9*(6), 2484–2491. https://doi.org/10.11591/eei.v9i6.2470

IBRAHIM, L. J., BUSH IDOKO, J., & ALWHELAT, A. M. 2024. Robust Chaos Image Encryption System using Modification Logistic Map, Gingerbread Man and Arnold Cat Map Robust Chaos Image Encryption System. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 15, Issue 6). www.ijacsa.thesai.org

ILIYASU, M. A., ABISOYE, O. A., BASHIR, S. A., & OJENIYI, J. A. 2021. A review of DNA cryptograhic approaches. *Proceedings of the 2020 IEEE 2nd International Conference on Cyberspace, CYBER NIGERIA 2020*, 66–72. https://doi.org/10.1109/CYBERNIGERIA51635.2021.9428855

KUMAR, M., SONI, A., SHEKHAWAT, A. R. S., & RAWAT, A. 2022. Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique. *Proceedings of the 2nd International Conference on Artificial Intelligence and Smart Energy, ICAIS 2022*, 1453–1457. https://doi.org/10.1109/ICAIS53314.2022.9742942

LAN, R., HE, J., WANG, S., GU, T., & LUO, X. 2018. Integrated chaotic systems for image encryption. *Signal Processing*, *147*, 133–145. https://doi.org/10.1016/j.sigpro.2018.01.026

LIU, Q., & LIU, L. 2020. Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System. *IEEE Access*, *8*, 83596–83610. https://doi.org/10.1109/ACCESS.2020.2991420

LUO, Y., YU, J., LAI, W., & LIU, L. 2019. A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimedia Tools and Applications*, *78*(15), 22023–22043. https://doi.org/10.1007/s11042-019-7453-3

MUSANNA, F., RANI, A., & KUMAR, S. 2018. Image encryption using chaotic 3-D Arnold's cat map and logistic map. *Advances in Intelligent Systems and Computing*, *704*, 365–378. https://doi.org/10.1007/978-981-10-7898-9_30

NIE, S. A., SULONG, G., ALI, R., & ABEL, A. 2019. The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image. *International Journal of Electrical and Computer Engineering*, *9*(6), 5218–5226. https://doi.org/10.11591/ijece.v9i6.pp5218-5226

PANWAR, S., KUMAR, M., & SHARMA, S. 2020. *Digital Image Steganography Using Modified LSB and AES Cryptography* (N. Nain & S. K. Vipparthi, Eds.; Vol. 1122). Springer International Publishing. https://doi.org/10.1007/978-3-030-39875-0

POI WONG, N., HARDY, MEGAWAN, S., & ANDRI. 2019. *Steganography using Mode-Based Least Significant Bit (MBLSB) Method*. https://doi.org/10.1109/ICIC47613.2019.8985693

POURJABBAR KARI, A., HABIBIZAD NAVIN, A., BIDGOLI, A. M., & MIRNIA, M. 2021. A new image encryption scheme based on hybrid chaotic maps. *Multimedia Tools and Applications*, *80*(2), 2753–2772. https://doi.org/10.1007/s11042-020-09648-1

QAYYUM, A., AHMAD, J., BOULILA, W., RUBAIEE, S., ARSHAD, MASOOD, F., KHAN, F., & BUCHANAN, W. J. 2020. Chaos-Based Confusion and Diffusion of Image Pixels Using Dynamic Substitution. *IEEE Access*, *8*, 140876–140895. https://doi.org/10.1109/ACCESS.2020.3012912

RADKE, S. S., SCHOLAR, R., & MISHRA, D. S. 2021. *Review of Image Security approaches: Concepts, Issues, Challenges and Applications*.

RAJ, B., JANI ANBARASI, L., NARENDRA, M., & SUBASHINI, V. J. 2019. A New Transformation of 3D Models Using Chaotic Encryption Based on Arnold Cat Map. In *Lecture Notes on Data Engineering and Communications Technologies* (Vol. 29, pp. 322–332). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-12839-5_29

SAMIULLAH, M., ASLAM, W., NAZIR, H., LALI, M. I., SHAHZAD, B., MUFTI, M. R., & AFZAL, H. 2020. An Image Encryption Scheme Based on DNA Computing and Multiple Chaotic Systems. *IEEE Access*, *8*, 25650–25663. https://doi.org/10.1109/ACCESS.2020.2970981

SINGH, A. K., CHATTERJEE, K., & SINGH, A. 2023. An Image Security Model Based on Chaos and DNA Cryptography for IIoT Images. *IEEE Transactions on Industrial Informatics*, *19*(2), 1957–1964. https://doi.org/10.1109/TII.2022.3176054

ULLAH, S., ZHENG, J., DIN, N., HUSSAIN, M. T., ULLAH, F., & YOUSAF, M. 2023. Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. In *Computer Science Review* (Vol. 47). Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2022.100530

XUEJING, K., & ZIHUI, G. 2020. A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. *Signal Processing: Image Communication*, *80*. https://doi.org/10.1016/j.image.2019.115670

ZAREAI, D., BALAFAR, M., & FEIZI DERAKHSHI, M. R. 2021. A new Grayscale image encryption algorithm composed of logistic mapping, Arnold cat, and image blocking. *Multimedia Tools and Applications*, *80*(12), 18317–18344. https://doi.org/10.1007/s11042-021-10576-x

ZHENG, J., & HU, H. 2021. A symmetric image encryption scheme based on hybrid analog-digital chaotic system and parameter selection mechanism. *Multimedia Tools and Applications*, *80*(14), 20883–20905. https://doi.org/10.1007/s11042-021-10751-0