# ENKRIPSI CITRA DIGITAL BERBASIS KOMBINASI *ARNOLD CAT MAP* TERMODIFIKASI DAN *DNA ENCODING*

**Thesa Adi Saputra Yusri [1], Deddy Rudhistiar [2]**
[1] Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Negeri Yogyakarta, Indonesia
[2] Program Studi Teknik Informatika, Fakultas Teknologi Industri,
Institut Teknologi Nasional Malang, Indonesia
*thesaadisaputrayusri@uny.ac.id*

**ABSTRAK**

Keberagaman data privat berupa citra atau video meningkatkan kebutuhan pengamanan data yang lebih *robust*. Pengamanan ini dibutuhkan karena adanya kemungkinan *fraud* yang membuat kerahasiaan data seseorang bisa bocor. Penelitian ini dikembangkan dengan tujuan meningkatkan metode enkripsi citra digital berbasis Arnold Cat Map termodifikasi dengan difusi DNA *encoding*. Fokus penelitian ini menganalisis performansi pengacakan citra dengan Arnold Cat Map termodifikasi yang didifusikan dengan DNA *encoding*. Hasil enkripsi diuji dengan 4 parameter numerik, yaitu entropi, Mean-squared error (MSE), peak signal-tonoise ratio (PSNR) dan koefisien korelasi. Citra pengujian dikhususkan pada citra persegi dengan variasi ukuran 128 x 128 hingga 512 x 512. Hasil menunjukkan signifikansi perubahan hasil enkripsi ketika dilihat dari kondisi histogram yang menyebar merata. Rata-rata nilai korelasi sebesar 0.017, rata-rata entropi sebesar 7.9964 dan PSNR sebesar 5.487 dB.

**Kata Kunci :** *citra digital, enkripsi. DNA encoding, arnold cat map termodifikasi*

## 1. PENDAHULUAN

Perkembangan industri 4.0 menuntut kebutuhan transfer data berbasis cloud semakin meningkat. Proses transfer data dan penyimpanannya menuntut kondisi pengamanan yang lebih baik pula [1]. Jumlah transaksional data berupa data *time-series* maupun data *binary large object* (BLOB) seperti citra semakin cepat dan rentan terhadap kondisi-kondisi *fraud*. Beragamnya pemanfaatan data citra termasuk dalam bidang kesehatan, militer, teknologi, teknik, fashion dan juga Pendidikan. Setiap bidang memiliki tingkat kredential yang beragam namun tidak kalah penting satu sama lain [2]. Kredential ini dapat berupa kerahasiaan (*confidentiality*) [3], keaslian (*authenticity*) [4] serta validitas citra (*image validity*) [5].

Keberadaan *fraud* ini bisa dihadapi dengan mengamankan data sebelum ditransmisikan. Upaya preventif ini menjaga agar walaupun data berhasil diambil alih oleh pihak tak berkepentingan, data tersebut tetap aman [6].

Teknik pengamanan yang mungkin dilakukan adalah pengenkripsian data. Enkripsi citra berbasis *chaotic map* menjadi pilihan yang cukup baik berdasarkan hasil yang ditunjukan dalam beberapa penelitian [7]–[9]. Salah satu Teknik yang cukup efisien adalah dengan melakukan pengacakan posisi piksel pada citra. Meskipun cukup baik, proses pengacakan ini cenderung akan Kembali ke posisi serupa dengan periode tertentu. Oleh karena itu, menjamin keamanan citra ini dapat dilakukan dengan mendifusikan hasil enkripsi tersebut [10]. Namun penelitian *cryptanalyst* menunjukan adanya kelemahan pada *cryptosystem* berbasis *chaotic map* [11]–[13] Penelitian oleh [14] menunjukan proses difusi yang sangat baik dengan proses DNA *encoding*.

Penelitian ini mengkonstruksi metode enkripsi berbasis pengacakan citra yang dikombinasikan dengan difusi nilai per piksel. Pengacakan citra akan memanfaatkan metode *Arnold cat map* yang diusulkan [10] dikombinasikan dengan DNA *encoding* yang diusulkan [15].

## 2. TINJAUAN PUSTAKA

### 2.1. Enkripsi berbasis *chaotic map*

Sistem kriptografi berbasis *chaos* telah mulai diteliti sejak tahun 1990. Properti utama dari fungsi chaos adalah sensitivitas yang bergantung pada keadaan / kontrol awal, yang berarti bahwa jika Anda memasukkan beberapa nilai awal dengan perbedaan yang sangat kecil, kunci yang dihasilkan akan memiliki perbedaan yang sangat besar, dan properti ini memenuhi persyaratan propagasi. cipher, menurut teori Shannon.

*Arnold cat map* yang berbasis permutasi. *Arnold cat map* (ACM) adalah suatu fungsi chaos reversible. Fungsi chaos diperkenalkan tahun 1960-an oleh Vladimir Arnold. Fungsi ACM mentransformasikan suatu titik koordinat $(x, y)$ pada citra yang berukuran $N \times N$ ke koordinat baru $(x', y')$. Persamaan iterasinya diformulasikan pada Persamaan (1).

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ N \qquad (1)$$

dengan p dan q sebarang bilangan bulat positif, $x_i$ dan $y_i$ menyatakan posisi piksel pada iterasi ke-i.

Sebagai syarat tambahan, nilai determinan matriks $\begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix}$ harus sama dengan 1 agar hasil transformasinya bersifat area-preseving. ACM merupakan pemetaan yang bersifat one-to-one karena setiap posisi piksel selalu ditransformasikan ke posisi lain secara unik. ACM diiterasikan sebanyak m kali dan setiap iterasi menhasilkan citra yang acak. Oleh karena itu, nilai p,q dan m merupakan kunci rahasia dalam kriptografi berbasis ACM [16].

### 2.2. *DNA Encoding*

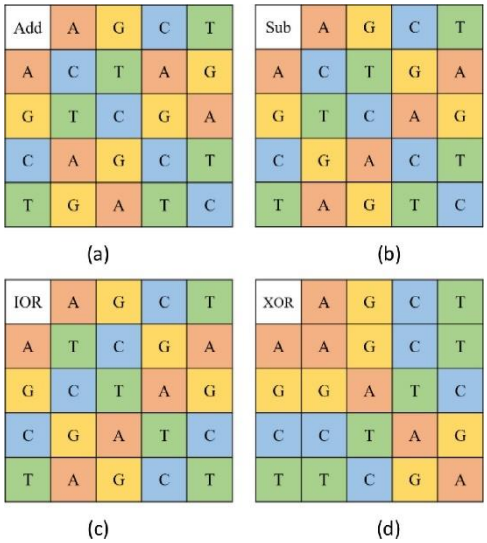
*Deoxyribonucleic Acid* (*DNA)* adalah suatu entitas yang menyimpan informasi dari semua jenis makhluk hidup. Terdapat empat *nucleic acid* yaitu A (*Adenine*), C (*Cytosine*), G (*Guanine*) dan T (*Thymine*) yang digunakan pada DNA *sequence*. Dalam *DNA sequence*, A merupakan komplemen dari T dan C merupakan komplemen dari G [15]. Keempat *nucleic acid* ini dapat direpresentasikan dalam bilangan biner, seperti pada Tabel 1.

Tabel 1. Aturan DNA encoding

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

Pada saat yang sama, berdasarkan operasi penjumlahan biner, pengurangan biner, operasi IOR dan XOR, operasi serupa antara basa DNA dapat diperoleh, seperti yang ditunjukkan pada Gambar. 2 (a) – (d). Sesuai dengan operasi antara basis DNA, kami akan melakukan enkripsi dan dekripsi pada suatu citra.

Sebagai contoh, jika diambil piksel dengan nilai intensitas 112 akan diperoleh nilai biner 01110000. Dengan menerapkan *rule* 5 akan diperoleh hasil pengkodean TGCC. Sebagai tambahan untuk meningkatkan keamanan dari *DNA Cryptography*, beberapa operasi aljabar berupa penjumlahan dan pengurangan antara *nucleic acid*, seperti yang diperllihatkan pada Tabel 1. Penjumlahan dan pengurangan untuk DNA dilakukan berdasarkan sistem penjumlahan dan pengurangan dalam $Z_2$. Sebagai contoh, 11 + 10 = 01, 01 – 11 = 10




Gambar 1. Operasi pada basis DNA. (a) DNA *addition*; (b) DNA *subtraction*; (c) DNA IOR; (d) DNA XOR

## 3. METODE PENELITIAN

Pengacakan posisi piksel dengan Arnold Cat Map sederhana menunjukkan kekurangan berupa kendala pada koefisien yang dimodifikasi telah diatur dalam nilai tertentu yang punya kaitan dengan obyek yang dienkripsi. Penelitian ini mengombinasikan Arnold Cat Map termodifikasi yang dirancang pada [10] dengan DNA encoding yang diusulkan pada [15]. Persamaan Arnold Cat Map termodifikasi ditunjukkan pada persamaan (2). Pemilihan nilai di matriks A dibatasi dengan pemenuhan kondisi persamaan (3) serta pemilihan koefisien K merupakan nilai terbesar dari multak setiap elemen matriks A sesuai dengan persamaan (4).

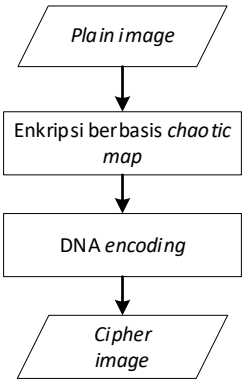
$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + K \begin{pmatrix} N \\ N \end{pmatrix} mod\ N \quad (2)$$

$$a_{00} \times a_{11} - a_{01} \times a_{10} = \pm 1 \quad (3)$$

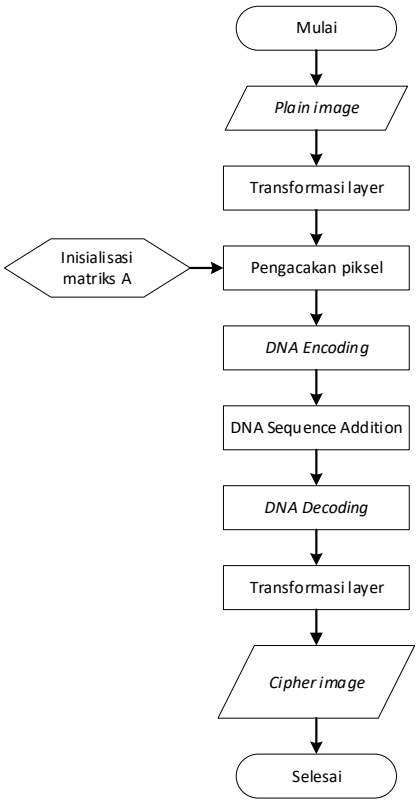
$$K = \max(|a_{00}|, |a_{01}|, |a_{10}|, |a_{11}|) \quad (4)$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}^{-1} \begin{pmatrix} x' \\ y' \end{pmatrix} + K \begin{pmatrix} N \\ N \end{pmatrix} mod\ N \quad (5)$$

Proses enkripsi diproses dengan bahasa pemrograman Python dengan bantuan package OpenCV untuk pengolahan citra. Gambar 1 menunjukkan proses enkripsi keseluruhan yang diusulkan. Secara lebih detail dalam diagram alir, Gambar 2 menunjukan framework enkripsi secara lebih rinci.




Gambar 1. Framework enkripsi citra




Gambar 2. Diagram alir enkripsi citra

Hasil enkripsi citra dievaluasi performansi keamanan dengan beberapa pengujian. Pengujian secara visual dilihat dari histogram persebaran nilai citra dan hasil enkripsinya. Pengujian keseragaman piksel diperhitungkan dengan Mean-squared error (MSE) dan peak signal-tonoise ratio (PSNR) serta analisis statistikal dengan uji korelasi.

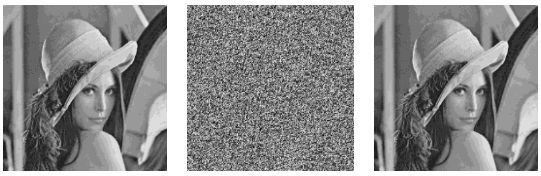
## 4. HASIL DAN PEMBAHASAN

Penyelidikan rinci dari pendekatan yang diusulkan dibahas dalam segmen ini. Perincian hasil ditunjukan dalam analisis meliputi inspeksi visual, analisis kualitas, dan deskripsi hasil metrik sistem. Kualitas skema enkripsi yang dinilai, meliputi analisis histogram, MSE, PSNR puncak, dan koefisien analisis korelasi. Informasi terkait citra yang diuji ditampilkan pada Tabel 2.

Tabel 2. Informasi citra yang diuji

| Nama | Ukuran piksel |
|---|---|
| Cameraman.tif | 256 x 256 |
| | 512 x 512 |
| Lena.jpg | 128 x 128 |
| | 256 x 256 |
| | 512 x 512 |
| Peppers.tif | 512 x 512 |
| Madril.tif | 512 x 512 |
| Aerial.png | 256 x 256 |
| Circuit.jpg | 256 x 256 |
| House.tif | 512 x 512 |
| Jetplane.tif | 512 x 512 |
| Lake.tif | 512 x 512 |

Penyidikan visual yang dicontohkan dalam segmen ini akan menggunakan citra Lena dengan format JPG berukuran 256 x 256 piksel dan citra Cameraman dengan format tif berukuran 512 x 512 piksel. Hasil enkripsi dan dekripsi ditunjukan pada Gambar 3 dan Gambar 4.



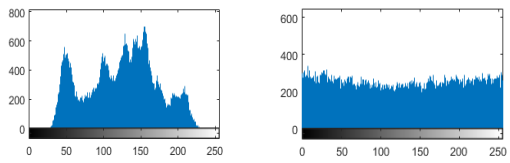
(a) (b) (c)

Gambar 3. Hasil analisis visual citra Lena.jpg (a) citra asli ; (b) citra terenkripsi; (c) citra hasil dekripsi

(a) (b) (c)

Gambar 4. Hasil analisis visual citra Cameraman.tif (a) citra asli ; (b) citra terenkripsi; (c) citra hasil dekripsi

Secara visual Gambar 3 (b) dapat terlihat bahwa citra teracak dan terdifusi sempurna serta berhasil terdekripsi dengan baik seperti pada Gambar 3(c). Histogram pada analisis visual pada citra merepresentasikan intensitas kemunculan suatu nilai suatu piksel pada setiap layer citra [17]. Diagram histogram pada Gambar 5 memperlihatkan frekuensi kemunculan dari setiap nilai piksel pada citra Lena.JPG.



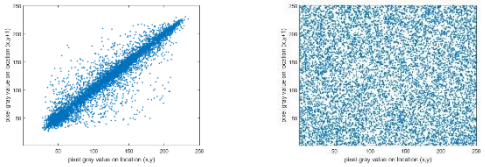

(a) (b)

Gambar 5. Histogram (a) citra asli ; (b) citra terenkripsi

Gambar 5 menunjukan bahwa distribusi nilai piksel pada citra asli pada Gambar 5 (a) tidak menyebar secara merata. Terdapat penumpukan nilai piksel pada rentang nilai tertentu. Secara umum, hasil enkripsi skema yang diusulkan memberikan hasil penyebaran warna yang sangat baik, terlihat dari frekuensi derajat keabuan yang telah menyebar merata sebagaimana yang diperlihatkan pada Gambar 5 (b).

Tabel 3. Korelasi piksel bertetangga

| Arah | Citra asli | Citra terenkripsi |
|---|---|---|
| Horizontal | 0.9203 | 0.0097 |
| Vertikal | 0.9575 | - 0.0140 |
| Diagonal | 0.9148 | 0.0332 |



(a) (b)

Gambar 6. Sebaran nilai piksel (a) citra asli; (b) citra terenkripsi

Tabel 3 menunjukan bahwa nilai korelasi dari citra asli sangat kuat. Nilai korelasi dari masing-masing citra sangat dekat dengan $\pm 1$, baik secara horizontal, veifrtikal maupun diagonal. Setelah citra terenkripsi terlihat bahwa ada perubahan drastis pada nilai korelasinya. nilai korelasinya mendekati nol, yang mengindikasikan piksel-piksel yang bertetangga tidak lagi berkorelasi. Untuk melihat lebih jelas korelasi antara piksel-piksel bertetangga, maka Gambar 6 memperlihatkan distribusi korelasi piksel-piksel yang bertetangga. Kolom sebelah kiri adalah distribusi korelasi pada plain image dan kolom kanan adalah distribusi korelasi pada cipher image. Pada plain image dapat dilihat bahwa piksel-piksel yang bertetangga nilai-nilainya berada di sekitar garis diagonal $45^0$, yang mengindikasikan korelasi yang kuat antara piksel-piksel tersebut. Sebaliknya, pada cipher-image nilai-nilai piksel tersebar merata di seluruh area bidang datar, yang mengindikasikan piksel-piksel di dalamnya tidak lagi berkorelasi. Namun pada skema enkripsi kedua masih terlihat sejumlah piksel yang terkumpul pada suatu titik tertentu

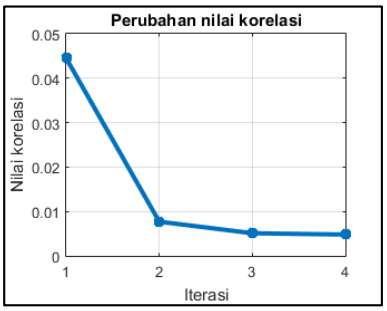
Pengujian selanjutnya melihat pengaruh jumlah iterasi dengan hasil enkripsi. Hasil pengujian tersebut diperlihatkan dalam Tabel 4.

Tabel 4. Pengaruh jumlah iterasi

| iterasi | Waktu proses (detik) | Nilai korelasi | | |
|---|---|---|---|---|
| | | Horizontal | Vertikal | Diagonal |
| 1 | 0.5979 | - 0,0311 | 0,0977 | - 0,0046 |
| 2 | 1,2268 | - 0,0093 | 0,0118 | 0,0019 |
| 3 | 1,8112 | 0,0033 | 0,0113 | 0,0006 |
| 4 | 2,0465 | 0,0023 | - 0,0064 | 0,0056 |

Berdasarkan Tabel 4 terlihat bahwa jumlah iterasi berpengaruh terhadap hasil enkripsi. Iterasi pertama hanya mengacak piksel sekali, hal ini menyebabkan hasil enkripsinya masih memiliki hubungan antar piksel yang cukup besar. Semakin bertambahnya iterasi semakin melemahkan hubungan antar piksel pada citra hasil enkripsi. Hal ini berbanding terbalik untuk waktu pemrosesannya, bertambahnya iterasi akan menambah waktu proses yang diperlukan.

Gambar 7 memunjukkan perubahan nilai korelasi untuk setiap iterasinya. Terlihat bahwa semakin bertambahnya iterasi, nilai korelasinya semakin menuju nol. Hal ini berarti Pertambahan jumlah korelasi akan meningkatkan kualitas enkripsi. Kemudian Gambar 8 menunjukan perubahan waktu pemrosesan untuk setiap iterasi. Berbanding terbalik dengan nilai korelasi, waktu pemrosesan enkripsi akan bertambah seiring pertambahan jumlah iterasi.




Gambar 7. Perubahan nilai korelasi


Gambar 8. Perubahan waktu proses

## 5. KESIMPULAN DAN SARAN

Berdasarkan penelitian dan eksperimen yang telah dilakukan dapat diambil kesimpulan bahwa skema enkripsi yang diusulkan berhasil disusun dan tetap bersifat inversible. Citra yang telah dienkripsi dapat didekripsi dengan sempurna. Hasil pengujian

menunjukan skema enkripsi cukup baik untuk dikombinasikan dengan DNA encoding. Hal ini dibuktikan dengan hasil pengujian histogram, nilai korelasi dan PSNR.

Saran dalam penelitian ini, agar kriptosistem pada citra dapat berlangsung lebih cepat, maka enkripsi citra dapat dilakukan secara selektif. Enkripsi selektif berarti proses enkripsi dilakukan hanya pada sebagian elemen citra namun tetap memberi efek menyeluruh

**DAFTAR PUSTAKA**


[1] B. A. Nathaniel, "Methodology for Image Cryptosystem Based on a Gray Code Number System," *Comput. Inf. Syst.*, vol. 23, no. 2, 2019, [Online]. Available: https://go.gale.com/ps/i.do?p=AONE&u=googlescholar&id=GALE%7CA565970156&v=2.1&it=r&sid=googleScholar&asid=8223a4e2.

[2] D. Rudhistiar, "IMPLEMENTASI PENGAMANAN CITRA DIGITAL BERBASIS ENKRIPSI 2D LOGISTIC MAP DAN DNA ENCODING DENGAN PENYISIPAN LSB DAN DWT," *J. Mnemon.*, vol. 5, no. 1, pp. 45–50, Jan. 2022, doi: 10.36040/mnemonic.v5i1.4436.

[3] D. Puthal, X. Wu, N. Surya, R. Ranjan, and J. Chen, "SEEN: A Selective Encryption Method to Ensure Confidentiality for Big Sensing Data Streams," *IEEE Trans. Big Data*, vol. 5, no. 3, pp. 379–392, Sep. 2019, doi: 10.1109/TBDATA.2017.2702172.

[4] I. Kim, W. Susilo, J. Baek, and J. Kim, "Harnessing Policy Authenticity for Hidden Ciphertext Policy Attribute-Based Encryption," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 3, pp. 1856–1870, May 2022, doi: 10.1109/TDSC.2020.3040712.

[5] E. Zhang, Y. Hou, and G. Li, "A lattice-based searchable encryption scheme with the validity period control of files," *Multimed. Tools Appl.*, vol. 80, no. 3, pp. 4655–4672, Jan. 2021, doi: 10.1007/s11042-020-09898-z.

[6] A. N. Babatunde, A. A. Oke, A. A. Oloyede, and A. O. Bello, "Enhanced image security using residue number system and new Arnold transform," *J. Teknol. dan Sist. Komput.*, vol. 9, no. 4, pp. 205–210, Oct. 2021, doi: 10.14710/jtsiskom.2021.14038.

[7] P. Kiran and B. . Parameshachari, "Resource Optimized Selective Image Encryption of Medical Images Using Multiple Chaotic Systems," *Microprocess. Microsyst.*, vol. 91, p. 104546, Jun. 2022, doi: 10.1016/j.micpro.2022.104546.

[8] A. Belazi *et al.*, "Improved Sine-Tangent chaotic map with application in medical images encryption," *J. Inf. Secur. Appl.*, vol. 66, p. 103131, May 2022, doi: 10.1016/j.jisa.2022.103131.

[9] Y. Zhang, R. Zhao, Y. Zhang, R. Lan, and X. Chai, "High-efficiency and visual-usability image encryption based on thumbnail preserving and chaotic system," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 6, pp. 2993–3010, Jun. 2022, doi: 10.1016/j.jksuci.2022.04.001.

[10] M. Ding and F. Jing, "Digital Image Encryption Algorithm Based on Improved Arnold Transform," in *2010 International Forum on Information Technology and Applications*, Jul. 2010, pp. 174–176, doi: 10.1109/IFITA.2010.17.

[11] N. Munir, M. Khan, I. Hussain, and A. S. Alanazi, "Cryptanalysis of Encryption Scheme Based on Compound Coupled Logistic Map and Anti-Codifying Technique for Secure Data Transmission," *Optik (Stuttg).*, Jul. 2022, doi: 10.1016/j.ijleo.2022.169628.

[12] Y. Ma, C. Li, and B. Ou, "Cryptanalysis of an image block encryption algorithm based on chaotic maps," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, doi: 10.1016/j.jisa.2020.102566.

[13] J. Wu, X. Liao, and B. Yang, "Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation," *Signal Processing*, vol. 142, pp. 292–300, Jan. 2018, doi: 10.1016/j.sigpro.2017.06.014.

[14] C. Zou, X. Wang, C. Zhou, S. Xu, and C. Huang, "A novel image encryption algorithm based on DNA strand exchange and diffusion," *Appl. Math. Comput.*, vol. 430, p. 127291, Oct. 2022, doi: 10.1016/j.amc.2022.127291.

[15] A. Jain and N. Rajpal, "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps," *Multimed. Tools Appl.*, vol. 75, no. 10, pp. 5455–5472, May 2016, doi: 10.1007/s11042-015-2515-7.

[16] E. Hariyanto and R. Rahim, "Arnold's Cat Map Algorithm in Digital Image Encryption," *Int. J. Sci. Res.*, vol. 5, no. 10, pp. 1363–1365, Oct. 2016, doi: 10.21275/ART20162488.

[17] A. A. Arab, M. J. B. Rostami, and B. Ghavami, "An image encryption algorithm using the combination of chaotic maps," *Optik (Stuttg).*, vol. 261, no. January, p. 169122, 2022, doi: 10.1016/j.ijleo.2022.169122.