PROTEKSI CITRA BIOMETRIK SIDIK JARI DENGAN PENDEKATAN KRIPTOGRAFI ROUTE CIPHER: STUDI EKSPERIMEN DAN ANALISIS KETAHANAN

Suhardi[1*], Muhammad Siddik Hasibuan[2]
[1,2]Imu Komputer, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara
suhardi@uinsu.ac.id[1], muhammadsiddik@uinsu.ac.id[2]

Submitted October 14, 2025; Revised November 27, 2025; Accepted December 1, 2025

Abstrak

Keamanan data biometrik kini menjadi sorotan tajam, terutama setelah munculnya berbagai insiden kebocoran data yang membuktikan bahwa data sidik jari rentan dicuri. Masalah utamanya jelas, tidak seperti kata sandi, sidik jari yang sudah terekspos tidak bisa diganti oleh pemiliknya. Berangkat dari urgensi tersebut, penelitian ini menguji efektivitas metode kriptografi klasik, *Route Cipher*, sebagai benteng perlindungan citra sidik jari. Idenya cukup sederhana namun teknis, yaitu memanfaatkan transposisi spiral untuk mengacak struktur visual data agar tidak bisa dikenali oleh pihak yang tidak berwenang. Eksperimen dilakukan terhadap 10 sampel citra sidik jari berformat BMP. Temuan kami menunjukkan hasil yang terbagi dua. Pada satu sisi, algoritma ini terbukti sangat ringan dan cepat, dengan waktu proses enkripsi rata-rata hanya 0,015 detik. Namun, dari aspek ketahanan sandi, analisis menggunakan parameter *Number of Pixels Change Rate* (NPCR) yang menghasilkan nilai 88,56% dan *Unified Average Changing Intensity* (UACI) sebesar 46,33% menunjukkan bahwa pengacakan ini belum sepenuhnya mencapai standar optimal. Kesimpulannya, *Route Cipher* menawarkan efisiensi waktu yang luar biasa, tetapi untuk perlindungan data yang sangat sensitif, metode ini sebaiknya tidak berdiri sendiri dan perlu dikombinasikan dengan lapisan keamanan tambahan.
Kata Kunci : Citra, Sidik Jari, *Route Cipher*, Kriptografi

Abstract

Biometric data security has come under intense scrutiny, particularly following a series of data breaches demonstrating that even fingerprints are vulnerable to theft. The core issue is undeniable: unlike passwords, once a fingerprint is compromised, it cannot be reset by the owner. Addressing this urgency, this study evaluates the effectiveness of the Route Cipher, a classic cryptographic method, as a defensive mechanism for fingerprint images. The concept is technically straightforward: it employs spiral transposition to scramble the data's visual structure, rendering it unrecognizable to unauthorized entities. Experiments were conducted using ten BMP-formatted fingerprint image samples. The findings reveal a dual outcome; on one hand, the algorithm proves to be exceptionally lightweight and fast, achieving an average encryption time of merely 0.015 seconds. However, in terms of cryptographic resilience, the analysis—yielding a Number of Pixels Change Rate (NPCR) of 88.56% and a Unified Average Changing Intensity (UACI) of 46.33%—indicates that the scrambling process has not yet fully met optimal security standards. In conclusion, while the Route Cipher offers remarkable time efficiency, it should not be relied upon as a standalone solution for highly sensitive data; rather, it is best implemented in conjunction with additional security layers.
Keywords: *Image, Fingerprint, Route Cipher, Cryptography*

1. PENDAHULUAN

Dalam era digital yang terus berkembang, teknologi telah mengubah banyak aspek kehidupan, termasuk bagaimana kita melindungi data. Sistem autentikasi berbasis biometrik, seperti sidik jari, menjadi semakin populer karena sifatnya yang unik dan sulit untuk dipalsukan. Sidik jari merupakan pola garis yang terpisah pada kulit jari tangan dan kaki yang mengandung pori-pori keringat [1]. Meningkatnya penggunaan teknologi menggunakan sidik jari, risiko kebocoran

data juga menjadi lebih tinggi. Salah satu situs berita daring menyatakan adanya dugaan terjadinya pembobolan data *Automatic Fingerprint Identification System* (Inafis) milik Kepolisian RI dan dijual di BreachForum. Sebuah akun bernama MoonzHaxor, yang dikenal memiliki keakuratan data yang tinggi, mengklaim memiliki data Inafis dan akan menjualnya dengan harga $1.000 [2]. Di Inggris, sebuah kebocoran data mengekspos jutaan catatan biometrik. Karena data biometrik digunakan oleh banyak orang, seperti penegak hukum, lembaga keuangan, kontraktor pertahanan, dan perusahaan, kebocoran data dianggap serius [3].

Berdasarkan fakta yang terjadi maka dibutuhkan teknik untuk mengamankan data sidik jari. Salah satu cara untuk melindungi data adalah dengan menggunakan metode kriptografi. Kriptografi berasal dari bahasa Yunani, yaitu *crypto* dan *graphia. Crypto* merujuk pada rahasia dan graphia berarti tulisan. Kriptografi merupakan metode untuk menyandikan pesan sehingga pesan tersebut dapat dikirim dan diterima secara aman. Kriptografi memiliki tujuan untuk melindungi kerahasiaan informasi dan mencegah penyalahgunaan oleh pihak yang tidak berwenang[4]. Kriptografi terdiri dari dua tahap, yaitu enkripsi di pihak pengirim dan dekripsi di pihak penerima [5]. Enkripsi citra merupakan suatu proses pengkodean yang mengubah citra yang dapat dipahami (*plain image*) menjadi citra yang tidak dapat dipahami (*cipher image*). Dekripsi citra merupakan suatu proses pemulihan yang mengkonversi citra yang tidak dapat dipahami (*cipher image*) menjadi citra yang asli [5], [6].

Dalam dunia kriptografi, banyak teknik telah dikembangkan untuk melindungi informasi, salah satunya adalah metode *Route Cipher. Route cipher* adalah jenis kriptografi klasik yang memanfaatkan transposisi untuk melakukan enkripsi. *Plainteks* awalnya dituliskan dalam *grid* dengan dimensi yang ditentukan kemudian dibacakan pola yang ditentukan dalam kunci [7]. Pesan atau *plainteks* juga bisa dimasukkan ke dalam *array* lalu dibaca sesuai urutan yang ditetapkan oleh rute[8]. Meskipun awalnya dirancang untuk teks, metode ini memiliki potensi besar untuk digunakan pada citra digital, termasuk citra sidik jari. Dengan menyandikan data citra menggunakan pola tertentu, keamanan informasi dapat diperkuat.

Penelitian sebelumnya telah mengusulkan berbagai pendekatan untuk pengamanan citra digital. Misalnya, Zhang dan Liu [9] meneliti pengamanan citra biometrik menggunakan metode enkripsi berbasis transformasi chaos, yang terbukti efektif dalam melindungi data dari serangan. Jiang dan Yang [10] mengklaim bahwa pengacakan *spiral/chaotic maps* telah diterapkan dalam enkripsi citra modern memiliki ketahanan yang baik terhadap serangan *brute-force*, serangan statistik, dan serangan diferensial. Hendarto & Eko mengusulkan algoritma hibrida yang menggabungkan kriptografi dan steganografi untuk melindungi citra sidik jari, yang menunjukkan ketahanan terhadap analisis kriptografi [11]. Baru-baru ini, El-Rahmah dan Alluhaidan (2024) mengeksplorasi penggunaan *deep learning* untuk mendeteksi ancaman pada data biometrik, yang memberikan hasil menjanjikan dalam mengidentifikasi serangan[12].

Berbeda dengan penelitian-penelitian tersebut, eksplorasi terhadap metode klasik seperti *Route Cipher* di tengah gempuran algoritma modern sebenarnya didasari oleh kebutuhan akan efisiensi. Algoritma enkripsi citra yang sangat kompleks seringkali membebani kinerja sistem, terutama jika diterapkan pada perangkat pemindai sidik jari *portabel* yang memiliki sumber daya memori dan prosesor terbatas. Kriptografi modern berbasis *chaos* atau

deep learning memang menawarkan keamanan tinggi, namun seringkali lambat dalam eksekusi. Di sinilah letak relevansi penelitian ini: mencari titik keseimbangan di mana citra dapat diamankan dengan cepat tanpa membebani sistem. Penerapan metode *Route Cipher* sebagai metode klasik yang belum banyak digunakan untuk pengamanan citra sidik jari. Keunggulan utama metode ini adalah kesederhanaannya, yang memungkinkan proses enkripsi lebih efisien tanpa mengorbankan keamanan. Penelitian ini juga akan mengevaluasi bagaimana metode *Route Cipher* dapat diadaptasi untuk menangani karakteristik unik dari citra digital, yang memiliki struktur data lebih kompleks dibandingkan teks. Dengan pendekatan ini, penelitian ini tidak hanya berkontribusi pada pengembangan metode pengamanan citra tetapi juga membuka jalan untuk mengeksplorasi penerapan teknik kriptografi klasik di masa kini.

2. METODE PENELITIAN

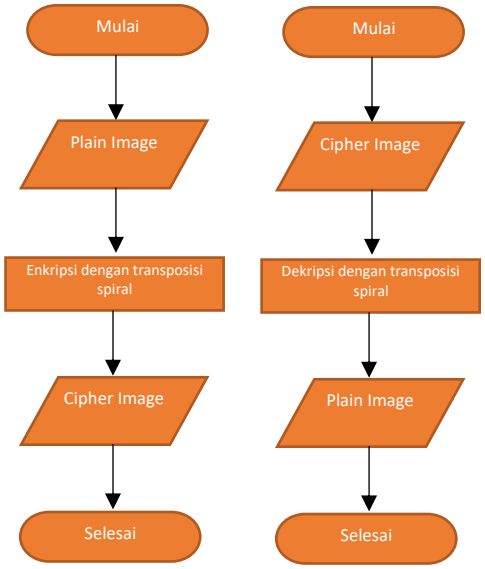
Pada penelitian ini menggunakan metode kualitatif dengan empat langkah utama yang dilakukan yaitu: pembelajaran literatur, pengumpulan data, analisis dan perancangan, implementasi dan pengujian, seperti yang ditunjukkan pada gambar 1

Gambar 1. Langkah Penelitian

a. Pembelajaran Literatur
Pada fase ini dilakukan pengumpulan data yang diperlukan untuk proses desain sistem. Studi literatur ini mencakup pemahaman tentang konsep-konsep tersebut, di antaranya: kriptografi, serta pemahaman mengenai metode algoritma *Route Cipher.*

b. Pengumpulan Data
Dalam fase ini, dilakukan pengumpulan data yang diperlukan untuk pembuatan aplikasi. Pengumpulan data ini bisa didapatkan dari artikel, jurnal, buku, serta dari internet yang berkaitan dengan perancangan aplikasi. Untuk data citra sidik jari akan diambil 10 sampel citra BMP yang didapatkan dari situs kaggle.com.

c. Analisis dan Perancangan
Tahap perancangan sistem dalam penelitian adalah langkah yang diambil peneliti setelah mengumpulkan seluruh kebutuhan sistem yang akan dibuat. Proses enkripsi dan dekripsi dapat dilihat pada gambar 2.

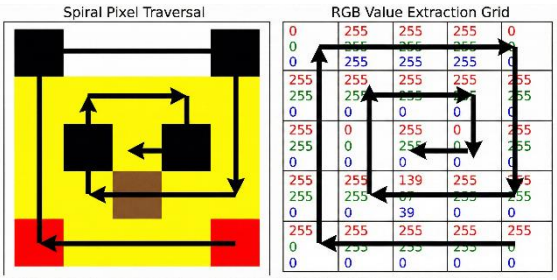


Gambar 2. Flowchart Enkripsi dan Dekripsi *Route Cipher*

Diagram alir di atas sebenarnya memetakan dua proses bagaimana sebuah citra diamankan, dan

bagaimana ia dikembalikan lagi ke bentuk aslinya.

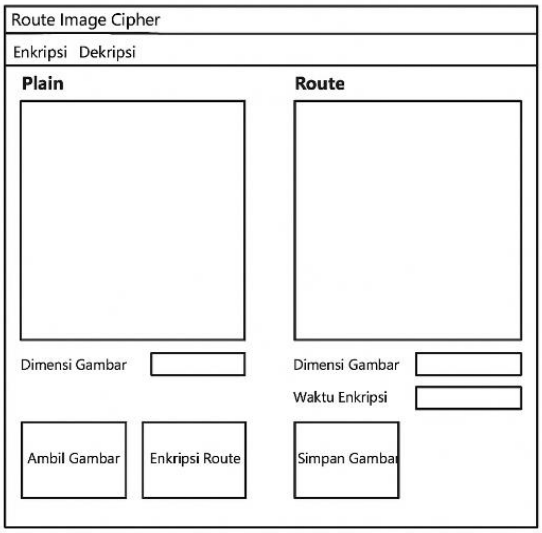
Pada sisi kiri, alurnya berfokus pada enkripsi. Semuanya berawal dari Plain Image (BMP), yaitu data mentah sidik jari yang masih utuh dan bisa dibaca oleh siapa saja. Agar data ini aman, sistem tidak membiarkannya terbuka, melainkan langsung memprosesnya menggunakan teknik transposisi spiral.



Gambar 3. Pola Spiral *Route Cipher*

Mekanisme transposisi spiral yang diadopsi dalam penelitian ini sebenarnya menawarkan pendekatan yang unik dalam memecah korelasi antar piksel. Berbeda dengan pembacaan teks biasa yang umumnya linear (kiri ke kanan), transposisi spiral bekerja dengan cara memanipulasi koordinat pembacaan matriks citra. Idenya sederhana namun efektif, susunan piksel diacak mengikuti jalur melingkar. Algoritma diprogram untuk menelusuri piksel mulai dari sudut terluar, kemudian bergerak memutar ke arah dalam menyerupai cangkang siput atau obat nyamuk bakar hingga mencapai titik tengah matriks. Teknik ini dipilih untuk mengacaukan struktur visual citra. Dengan mengubah rute pembacaan ini, pola garis sidik jari yang tadinya bersambung menjadi terputus dan tersebar secara acak di lokasi yang tidak semestinya sehingga hasil akhirnya yang kita sebut *Cipher Image* hanya tampak seperti gangguan visual (*noise*) yang tidak bermakna bagi mata manusia.

Sementara itu, diagram di sisi kanan menunjukkan alur atau proses dekripsi. Tahapan ini krusial karena data yang aman tidak akan berguna jika tidak bisa dibaca kembali oleh pemiliknya. Ketika sistem menerima masukan berupa *Cipher Image*, ia akan membalikkan logika pengacakan tadi. Karena pola rutenya sama (spiral), sistem tinggal menyusun ulang *piksel-piksel* yang berantakan tersebut ke koordinat aslinya. Sistem harus mengetahui dimensi *grid* awal untuk dapat mengembalikan *piksel-piksel* yang berserakan tersebut ke koordinat aslinya. Tanpa kunci rute yang tepat, merekonstruksi citra sidik jari hanyalah upaya menyusun *puzzle* tanpa gambar panduan. Begitu proses ini tuntas, *Plain Image* pun kembali muncul dalam kondisi sempurna, siap untuk diverifikasi.



Gambar 4. Rancangan Route Image Cipher

d. Implementasi dan Pengujian

Pada tahap implementasi ini dibuatlah sistem berdasarkan rancangan yang telah dibuat sebelumnya. Sistem ini nantinya digunakan untuk mengimplementasikan proses enkripsi yang menghasilkan *cipher image* dan dekripsi yang menghasilkan *plain*

image algoritma *route cipher*. Kemudian pada tahap ini proses pengujian ketahanan citra hasil enkripsi adalah menggunakan teknik pengukuran *differential attack value* yaitu *Unified Average Changing Intensity* (UACI). Nilai NPCR dan UACI digunakan untuk menilai sensitivitas sistem enkripsi terhadap perubahan 1-*bit* / 1-*pixel* pada *plaintext/plain image* [13][14]. Metrik ini masih digunakan untuk evaluasi citra hasil teknik enkripsi modern [15]. UACI adalah ukuran standar rata-rata perbedaan intensitas antara dua gambar yang telah dienkripsi. Nilai optimal untuk UACI berada dalam rentang 33,25% hingga 33,48% [5], [16], [17] dan penghitungan dapat dilakukan menggunakan rumus

$$UACI = \frac{\sum_{(i,j)} E(i,j) - E\prime(i,j)}{255 \times W \times H} \times 100 \quad (1)$$

di mana $E(i,j)$ dan $E'(i,j)$ adalah gambar terenkripsi dari gambar asli dan gambar yang dimodifikasi.
Sedangkan *Number of Pixels Change Rate* (NPCR) untuk menentukan perbandingan pada setiap piksel antara dua gambar yang terenkripsi dari gambar asli yang relevan jika terjadi perubahan pada kunci sebesar 1 bit. Nilai optimal untuk NPCR harus lebih dari 99.6% [5], [16], [17] dan penghitungan dapat dilakukan menggunakan rumus:

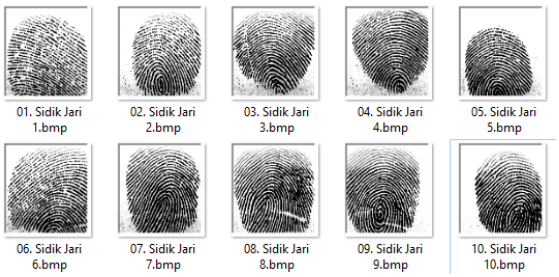
$$NPCR = \frac{\sum_{(i,j)} D(i,j)}{W \times H} \times 100 \quad (2)$$

$$D(i,j) = \begin{cases} 0 \; if \; E(i,j) = E'(i,j) \\ 1 \; if \; E(i,j) \neq E'(i,j) \end{cases} \quad (3)$$

$E(i,j)$ dan $E'(i,j)$ masing-masing adalah citra terenkripsi dari citra asli dan citra yang dimodifikasi. Sementara $D(i,j)$ menunjukkan perbedaan antara piksel citra asli terenkripsi dan citra yang dimodifikasi. W dan H masing-masing mewakili lebar dan tinggi citra.

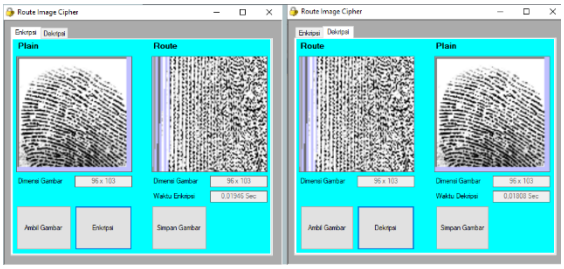
3. HASIL DAN PEMBAHASAN

Penelitian ini dimulai dengan menyiapkan 10 citra sidik jari yang memiliki dimensi 96 x 103 *piksel.*



Gambar 5. Citra Sidik Jari

Citra sidik jari kemudian dienkripsi dan didekripsi kembali dengan kriptografi *route cipher* melalui transposisi spiral menggunakan sistem keamanan citra sidik jari yang telah dirancang sebelumnya. Setiap proses enkripsi dan dekripsi yang dilakukan pada citra-citra tersebut akan dilihat waktu prosesnya.



Gambar 6. Proses Enkripsi dan Dekripsi

Setelah proses enkripsi selesai maka citra yang telah dienkripsi akan dihitung waktu prosesnya. Kemudian sisi ketahanannya akan dianalisis dengan UACI dan NPCR sehingga menghasilkan data seperti pada tabel 1.

Tabel 1. Analisis Ketahanan *Cipher Image* dan Waktu Enkripsi

No	Nama Citra	NPCR (%)	UACI(%)	Waktu (detik)
1	Sidik Jari 1	87,6517%	44,1556%	0,0154
2	Sidik Jari 2	86,1549%	44,7292%	0,0136
3	Sidik Jari 3	92,5061%	45,3162%	0,0158
4	Sidik Jari 4	92,4353%	45,1715%	0,0139
5	Sidik Jari 5	83,2828%	47,6140%	0,0128

6	Sidik Jari 6	90,6553%	45,6352%	0,0182
7	Sidik Jari 7	90,1800%	48,1224%	0,0187
8	Sidik Jari 8	91,4037%	46,3580%	0,0182
9	Sidik Jari 9	90,5845%	48,7421%	0,0152
10	Sidik Jari 10	80,7848%	47,4649%	0,0126
	Rata-Rata	**88,5639%**	**46,3309%**	**0,0154**

Data yang tersaji dalam Tabel 1 memberikan gambaran menarik mengenai trade-off atau kompromi antara kecepatan dan keamanan dalam algoritma klasik ini. Nilai rata-rata NPCR 88,5639% mengindikasikan bahwa sekitar 88% piksel telah berubah posisi atau nilai dibandingkan citra aslinya. Hal ini juga menunjukkan bahwa perubahan pada citra sidik jari asli dengan *route cipher* akan menyebabkan perubahan yang tidak begitu besar pada citra sidik jari terenkripsi. Meskipun secara visual gambar sudah terlihat rusak (seperti *noise*), dalam standar kriptografi ketat, angka ini masih menyisakan celah. Standar optimal yang diharapkan untuk menahan serangan diferensial biasanya berada di atas 99,6%. Artinya, masih ada sekitar 11-12% korelasi piksel yang mungkin belum teracak dengan sempurna. Sedangkan nilai rata-rata UACI 46,3309% yang mana sedikit melenceng dari rentang ideal teoritis 33,48%. Anomali statistik ini menunjukkan bahwa meskipun *Route Cipher* dengan metode spiral sukses menyembunyikan bentuk visual sidik jari dari pandangan mata manusia, pola distribusi intensitas warnanya masih memiliki jejak yang bisa dideteksi oleh analisis komputer canggih. Hal ini wajar mengingat *Route Cipher* hanya melakukan transposisi (pemindahan letak) tanpa melakukan substitusi (pengubahan nilai) piksel secara mendasar. Oleh karena itu, hasil ini menegaskan bahwa metode ini sangat efisien sebagai lapisan pengamanan pertama yang ringan, namun membutuhkan modifikasi tambahan, seperti kombinasi dengan fungsi chaos atau substitusi sederhana jika ingin digunakan untuk data yang sangat sensitif

Berdasarkan hasil analisis yang telah dilakukan bahwa nilai NPCR dan UACI belum mencapai nilai optimal. Untuk waktu rata-rata yang dibutuhkan untuk enkripsi adalah 0,0154 detik. Sedangkan proses dekripsi dari *cipher image* menjadi *plain image* berjalan dengan baik dan dapat mengembalikan bentuk citra aslinya yang membutuhkan waktu rata-rata 0,0154 detik. Angka ini sangat impresif untuk kebutuhan sistem real-time atau perangkat dengan daya rendah, karena beban komputasinya sangat minim dibandingkan algoritma modern yang kompleks.

4. SIMPULAN

Hasil penelitian ini dapat disimpulkan bahwa kriptografi *route cipher* dapat diimplementasikan pada citra sidik jari dengan baik menggunakan transposisi spiral yang membutuhkan waktu untuk enkripsi dan dekripsi rata-rata 0,015 detik. Analis ketahanan *cipher image* menggunakan teknik pengukuran *differential attack value* yaitu *Unified Average Changing Intensity* (UACI) dan *Number of Pixels Change Rate* (NPCR). Nilai NPCR menunjukkan rata-rata 88,5639% dan nilai UACI menunjukkan rata-rata 46,3309%. menunjukkan bahwa pengacakan ini belum sepenuhnya mencapai standar optimal. *Route Cipher* menawarkan efisiensi waktu yang luar biasa, tetapi untuk perlindungan data yang sangat sensitif, metode ini sebaiknya tidak berdiri sendiri dan perlu dikombinasikan dengan lapisan keamanan tambahan.

DAFTAR PUSTAKA

[1] A. Alfadila, N. Arianti, and F. Faizin, “Sidik Jari dalam Al-Qur’an (Kajian Tafsir Ilmi),” *Ikhtisar J. Pengetah. Islam*, vol. 2, no. 2, p. 162, 2022, doi: 10.55062//ijpi.2022.v2i2.122.

[2] Bloomberg Technoz, “Data Inafis Diduga Bocor & Ada Sidik Jari, Bisa Bobol Rekening?,” 2024. https://www.bloombergtechnoz.com/detail-news/53897/data-inafis-

diduga-bocor-ada-sidik-jari-bisa-bobol-rekening (accessed Jul. 27, 2025).

[3] Cyberthreat.id, "Puluhan Juta Data Biometrik Bocor, Terbanyak Sidik Jari," 2019. https://cyberthreat.id/read/2185/Puluhan-Juta-Data-Biometrik-Bocor-Terbanyak-Sidik-Jari (accessed Jul. 27, 2025).

[4] S. Suhardi, "Use of QRCode and Digital Signature Using The DSA Method to Authenticate Student Academic," *J. Comput. Networks , Archit. High Perform. Comput.*, vol. 6, no. 4, pp. 1913–1921, 2024, doi: 10.47709/cnahpc.v6i4.4765.

[5] C. Irawan and E. H. Rachmawanto, "Implementasi Kriptografi dengan Menggunakan Algoritma Arnold's Cat Map dan Henon Map," *J. Masy. Inform.*, vol. 13, no. 1, pp. 15–32, 2022, doi: 10.14710/jmasif.13.1.43312.

[6] S. Murphy and R. Player, *Understanding cryptography*. 2025. doi: 10.1093/actrade/9780192882233.003.0002.

[7] M. S. Bangun, "Implementasi Algoritma Route Cipher Dalam Pengamanan File Pdf," *Build. Informatics, Technol. Sci.*, vol. 1, no. 1, pp. 1–6, 2019.

[8] S. BAHRI, F. Jihan, and B. RUDIANTO, "Implementasi Algoritma Super Enkripsi Vigenere Cipher Dan Route Cipher Pada Penyandian Pesan Teks," *J. Mat. UNAND*, vol. 12, no. 2, pp. 168–175, 2024, doi: 10.25077/jmua.12.2.168-175.2023.

[9] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," *Mathematics*, vol. 11, no. 11, 2023, doi: 10.3390/math11112585.

[10] M. Jiang and H. Yang, "Image Encryption Using a New Hybrid Chaotic Map and Spiral Transformation," *Entropy*, vol. 25, no. 11, p. 1516, Nov. 2023, doi: 10.3390/E25111516.

[11] J. Hendarto and E. Eko Wahyudi, "Pengamanan Citra Sidik Jari Menggunakan Kriptografi Dan Steganografi Fraktal," *J. Mnemon.*, vol. 6, no. 2, pp. 89–95, 2023, doi: 10.36040/mnemonic.v6i2.5784.

[12] S. A. El-Rahman and A. S. Alluhaidan, "Enhanced multimodal biometric recognition systems based on deep learning and traditional methods in smart environments," *PLoS One*, vol. 19, no. 2 February, pp. 1–24, 2024, doi: 10.1371/journal.pone.0291084.

[13] M. A. Elmenyawi, N. M. Abdel Aziem, and A. M. Bahaa-Eldin, "Efficient and Secure Color Image Encryption System with Enhanced Speed and Robustness Based on Binary Tree," *Egypt. Informatics J.*, vol. 27, p. 100487, Sep. 2024, doi: 10.1016/J.EIJ.2024.100487.

[14] R. Saidi, N. Cherrid, T. Bentahar, H. Mayache, and A. Bentahar, "Number of pixel change rate and unified average changing intensity for sensitivity analysis of encrypted inSAR interferogram," *Ing. des Syst. d'Information*, vol. 25, no. 5, pp. 601–607, Nov. 2020, doi: 10.18280/ISI.250507.

[15] A. Abba, N. Ahmed, and H. A. Sulaimon, "Experimental Evaluation of Various Chaos-based Image Encryption Schemes," *J. Comput. Theor. Appl.*, vol. 3, no. 1, pp. 91–103, 2025, doi: 10.62411/jcta.13483.

[16] U. Zia *et al.*, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *Int. J. Inf. Secur.*, vol. 21, no. 4, pp. 917–935, 2022, doi: 10.1007/s10207-022-

00588-5.

[17] A. İhsan and N. Doğan, "An innovative image encryption algorithm enhanced with the Pan-Tompkins Algorithm for optimal security," *Multimed. Tools Appl. 2024 8335*, vol. 83, no. 35, pp. 82589–82619, Mar. 2024, doi: 10.1007/S11042-024-18722-X.