CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 9, No. 1, Mei 2026, hlm. 16-22

Implementasi Algoritma Hill Cipher Dan Arnold CAT MAP Dalam Pengamanan Data Citra Digital Pengguna Ujian Daring

Muhammad Khudzaifah[1], Muhammad Luqman Hakim[2], Hawzah Sa'adati [1]

[1]Universitas Islam Negeri Maulana Malik Ibrahim
[2]PT. GoTo Gojek Tokopedia
Email: [1]khudzaifah@uin-malang.ac.id, [2]luqmanhkm38@gmail.com , [3]hawzahsaadati@gmail.com

Abstrak

Penelitian enkripsi citra digital berbasis web terus berkembang untuk menutup *research gap* yang ada pada algoritma tunggal. Algoritma klasik seperti Hill Cipher rentan terhadap serangan *known-plaintext* karena sifat linier transformasi matriksnya, sedangkan Arnold Cat Map memiliki periode pendek sehingga ruang kunci efektifnya terbatas. Sebagai solusi, penelitian ini mengusulkan metodologi hibrid dengan memadukan Hill Cipher dan Arnold Cat Map. Citra digital diujikan pada berbagai variasi kunci integer dan iterasi, dengan pengukuran kualitas menggunakan *Structural Similarity Index* (SSIM). Hasil eksperimen menunjukkan bahwa integrasi kedua algoritma menghasilkan *cipher-image* yang sangat berbeda dari citra asli (nilai SSIM enkripsi terendah ≈ 0,0097, rata-rata ≈ 0,0112) dan proses dekripsi berhasil mengembalikan citra dengan sempurna (SSIM = 1). Waktu komputasi enkripsi pada iterasi pertama sekitar 2,151 detik dan meningkat menjadi 3,661 detik pada iterasi berikutnya. Implikasi teoretisnya, kombinasi transformasi matriks (Hill Cipher) dan permutasi piksel kaotik (Arnold Cat Map) memaksimalkan difusi dan konfusi sehingga sistem enkripsi menjadi lebih aman. Penelitian ini juga mengimplementasikan sistem pada aplikasi web berbasis Django untuk menguji kelayakan penerapan praktis.

Kata kunci: *Hill Cipher, Arnold Cat Map, Enkripsi Citra Digital, Keamanan Data, SSIM*

Implementation Of Hill Cipher And Arnold CAT MAP Algorithms For Securing Digital Image Data Of Online Exam Users

Abstract

Research on web-based digital image encryption continues to evolve to close the research gap that exists in single algorithms. Classic algorithms such as Hill Cipher are vulnerable to known-plaintext attacks due to the linear nature of their matrix transformations, while Arnold Cat Map has a short period, limiting its effective key space. As a solution, this study proposes a hybrid methodology by combining Hill Cipher and Arnold Cat Map. Digital images were tested on various integer key and iteration variations, with quality measured using the Structural Similarity Index (SSIM). The experimental results show that the integration of the two algorithms produces cipher-images that are very different from the original images (lowest encryption SSIM value ≈ 0.0097, average ≈ 0.0112) and the decryption process successfully restores the images perfectly (SSIM = 1). The encryption computation time in the first iteration was approximately 2.151 seconds and increased to 3.661 seconds in the next iteration. Theoretically, the combination of matrix transformation (Hill Cipher) and chaotic pixel permutation (Arnold Cat Map) maximizes diffusion and confusion, making the encryption system more secure. This research also implemented the system on a Django-based web application to test its practical applicability.

Keywords *Hill Cipher, Arnold Cat Map, Digital Image Encryption, Data Security, SSIM).*

1. PENDAHULUAN

Perkembangan layanan ujian daring memerlukan proteksi data yang kuat, khususnya citra digital sebagai bagian dari verifikasi identitas pengguna (Agustini, 2024). Kriptografi menjadi solusi dalam menjaga keamanan citra digital. Enkripsi dan dekripsi adalah dua fungsi yang ada dalam kriptografi. Enkripsi citra digital bertujuan menyandikan citra digital (*plain-image*) sehingga tidak dapat dikenali lagi (*cipher-image*) (Munir, 2012). Metode enkripsi citra digital yang sekarang ini banyak dikembangkan adalah fungsi Chaos (Zhang & Liu, 2023; Neamah, 2023).

Metode chaos-based encryption banyak dikembangkan karena memiliki sensitivitas tinggi

terhadap kondisi awal dan mampu menghasilkan pola acak yang kompleks (Hussain et al., 2022; Wang et al., 2022). Chaos digunakan didalam kriptografi karena tiga alasan: (1) sifat chaos yang sensitif terhadap nilai awal, (2) chaos berkelakuan acak, (3) Nilai-nilai chaos tidak mempunyai periode (Sharma, 2010), *Arnold Cat Map* adalah salah satu algoritma kriptografi yang menggunakan skema transposisi berbasis fungsi *Chaos* dalam melakukan enkripsi citra digital (Ratna et al., 2021).

Teknik ini memanfaatkan kunci iterasi dan matriks untuk menyandi citra digital, tetapi memiliki kelemahan jika hanya mengandalkan algoritma tunggal. Algoritma Hill Cipher, dengan sifat penyebaran informasi yang baik, dapat digunakan bersama Arnold Cat Map untuk meningkatkan keamanan (Pratama et al., 2021). Kombinasi ini menghasilkan sistem enkripsi yang lebih tahan terhadap serangan kriptanalis (Xi et al., 2024; Turan et al., 2024).

Penelitian ini akan mengembangkan aplikasi berbasis website dengan framework Django untuk implementasi enkripsi dan dekripsi data menggunakan algoritma Arnold Cat Map dan Hill Cipher. Django dipilih karena kemudahan pengembangannya, sementara library Python seperti Pillow akan digunakan untuk pemrosesan citra. Aplikasi ini bertujuan untuk mengamankan data pengguna, baik dalam bentuk teks maupun citra digital, dengan proses yang cepat dan efisien.

Meski berbagai metode kriptografi telah dikembangkan, terdapat research gap signifikan terkait efektivitas algoritma tunggal dalam menjaga keamanan citra digital. Penelitian-penelitian sebelumnya menunjukkan bahwa algoritma Hill Cipher, misalnya, hanya melakukan substitusi-permutasi berbasis matriks sehingga dikenal rentan terhadap known-plaintext attack apabila penyerang memiliki cukup pasangan plainteks sandi (Azza A. Abdo et al., 2020). Di sisi lain, Arnold Cat Map, meski efektif sebagai peta chaos untuk mengacak piksel, memiliki periode pendek ($\leq 3N$ untuk citra NxN) sehingga kembali ke bentuk semula setelah iterasi tertentu (Ratna et al., 2021). Periodisitas ini membatasi ruang kunci efektif dan meningkatkan kerentanan terhadap serangan brute force (Turan et al., 2024). Temuan literatur menunjukkan bahwa penggunaan salah satu algoritma saja tidak memadai untuk mengamankan citra digital secara handal (Qin et al., 2023 ; Zhang, 2023)..

Kebaruan penelitian ini terletak pada kombinasi dua pendekatan berbeda: transformasi linier matriks (Hill Cipher) dan permutasi kaotik piksel (Arnold Cat Map). Pendekatan hibrid ini diharapkan mengatasi keterbatasan masing-masing algoritma; Hill Cipher memperkuat difusi informasi, sementara Arnold Cat Map memperkuat konfusi dengan mengacak posisi piksel. Secara teoretis, integrasi kedua algoritma meningkatkan kekuatan kriptografi—memperluas ruang kunci dan menyulitkan analisis kriptanalisis. Penelitian ini bertujuan merancang dan menguji sistem enkripsi citra pada platform web berbasis framework Django, sekaligus menganalisis performa dan keamanan metode gabungan tersebut.

2. TINJAUAN PUSTAKA

Penelitian terkini mengenai enkripsi citra menunjukkan pergeseran menuju penggunaan peta chaos berganda dan kombinasi teknik matriks untuk meningkatkan difusi serta konfusi pada cipher-image (Li et al., 2023). Literatur lima tahun terakhir memperlihatkan bahwa penggabungan Hill Cipher dengan mekanisme modern atau variasi dinamis mulai banyak dikembangkan untuk mengatasi kelemahan linearitasnya (Xi et al., 2024).

Teknik Hill Cipher ini dirancang untuk mencegah analisis frekuensi dengan melakukan enkripsi berbasis perkalian matriks, bukan substitusi langsung antar huruf (Fitri dan Rahmadani, 2024). Dalam penerapannya pada citra digital, Hill Cipher menggunakan operasi perkalian matriks dan invers matriks untuk mengamankan data visual (Mafula, 2025).

Diberikan citra digital asli (*plain-image)* $\boldsymbol{P}$ dan kunci matriks $\boldsymbol{K} = \begin{bmatrix} k_{11} k_{12} \\ k_{21} k_{22} \end{bmatrix}$, dengan kondisi $\boldsymbol{K}$ harus memiliki *invers* matriks atau dapat disebut *invertible.* Enkripsi citra digital berdasarkan *Hill Cipher* bergantung pada pembagian piksel citra digital $\boldsymbol{P}$ menjadi matriks berukuran sama, dan kemudian sandi *Hill Cipher* diterapkan pada masing-masing matriks tersebut. Berdasarkan matriks $\boldsymbol{P}$ dari dua piksel berturut-turut p_1, p_2 dari citra digital asli (*plain-image)* $\boldsymbol{P}$. Enkripsi dari matriks $\boldsymbol{P}$ adalah sama dengan matriks sandi $C = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$ berdasarkan persamaan berikut :

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} k_{11} k_{12} \\ k_{21} k_{22} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \ mod\ 256 \qquad (1)$$

Kemudian berdasarkan persamaan (1), citra digital sandi (*cipher-image*) dapat didefinisikan menjadi $\boldsymbol{C} = \boldsymbol{KP}\ mod\ 256$, di mana $\boldsymbol{C} = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$, $K = \begin{bmatrix} k_{11} k_{12} \\ k_{21} k_{22} \end{bmatrix}$, dan $\boldsymbol{P} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$. Sedangkan untuk mengembalikan hasil dari enkripsi citra digital yakni dekripsi citra digital dapat didefinisikan menjadi $\boldsymbol{P} = \boldsymbol{K^{-1}C}\ mod\ 256$, di mana $\boldsymbol{K^{-1}}$ adalah invers matriks dari $\boldsymbol{K}$(Azza A. Abdo et al., 2020).

Algoritma Arnold Cat Map pertama kali diperkenalkan pada tahun 1960 oleh Vladimir I. Arnold, seorang matematikawan asal Rusia, yang mendemonstrasikan algoritma ini menggunakan citra digital seekor kucing (Purba, 2014). Arnold Cat Map merupakan sistem *chaotic* dua dimensi yang mampu mengubah posisi piksel dalam citra digital tanpa menghilangkan informasi yang terkandung di dalamnya (Zhang dan Liu, 2022), di mana posisi

piksel citra digital dapat direpresentasikan dengan $S = \{(x, y) \mid x, y = 0, 1, 2 \ldots N - 1\}$.

Sehingga algoritma Arnold Cat Map dapat dituliskan dengan persamaan berikut :

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = [A] \begin{bmatrix} x \\ y \end{bmatrix} (mod\ N) \quad (2)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (mod\ N) \quad (3)$$

Di mana a dan b pada persamaan (3) adalah bilangan bulat positif sehingga determinan $[A] = 1$. (x', y') adalah posisi baru dari posisi piksel asli (x, y) ketika algoritma Arnold Cat Map dilakukan satu kali.

Setelah algoritma Arnold Cat Map diterapkan dengan jumlah iterasi tertentu d, hasilnya berupa citra digital acak yang tetap mempertahankan semua nilai piksel dari citra asli. Jumlah iterasi d yang diperlukan bergantung pada parameter $a, b,$ dan ukuran N dari citra asli (plain-image). Dengan demikian, algoritma Arnold Cat Map memiliki tiga parameter $a, b,$ dan jumlah iterasi d yang dapat digunakan sebagai kunci rahasia (Hariyanto, 2016).

Arnold Cat Map juga tetap menjadi metode permutasi piksel yang populer, dengan beragam pengembangan hybrid seperti pemrosesan sub-image maupun integrasinya dengan kriptografi asimetris atau teknologi blockchain (Turan et al, 2024; Inam et al., 2024). Pendekatan hybrid yang menggabungkan transformasi piksel dan substitusi matriks terbukti meningkatkan difusi dan konfusi pada cipher-image (Banu dan Amutha, 2021; Chai et al., 2020). Penggunaan chaotic maps modern juga mampu meningkatkan ketahanan terhadap statistical attack dan differential attack pada citra digital (Rhouma et al., 2021; Zhou et al., 2021).

Selain itu, kajian komprehensif terbaru mengungkap bahwa penggunaan berbagai chaotic maps atau penggabungan dengan algoritma kriptografi modern memberikan peningkatan signifikan terhadap keamanan dan ketahanan sistem enkripsi terhadap serangan diferensial maupun histogram (Zhang, 2023; Neamah, 2023).

Secara keseluruhan, pendekatan hibrida yang memadukan Hill Cipher dan Arnold Cat Map sejalan dengan arah riset mutakhir, meskipun evaluasi ketahanan formal terhadap berbagai jenis serangan serta pengujian pada beragam ukuran dan format citra masih sangat diperlukan.

3. METODOLOGI

Penelitian ini menggunakan metode eksperimen, yang merupakan pendekatan penelitian kuantitatif paling lengkap karena memenuhi kriteria untuk menguji hubungan sebab-akibat, data yang digunakan dalam penelitian ini terdiri dari citra digital uji.

Metode penelitian meliputi implementasi algoritma Hill Cipher dan Arnold Cat Map pada citra digital berwarna, serta pengembangan aplikasi berbasis Django untuk proses enkripsi–dekripsi. Citra diuji pada beberapa kombinasi ukuran kunci matriks Hill dan jumlah iterasi Arnold. Kualitas hasil enkripsi dievaluasi dengan *Structural Similarity Index* (SSIM), yang mengukur kesamaan persepsi antara citra asli dan hasil enkripsi. SSIM dekat dengan 0 menunjukkan perbedaan tinggi (ciphering efektif), sementara SSIM=1 menandakan gambar identik. Selain itu, waktu komputasi enkripsi dan dekripsi dicatat sebagai indikator efisiensi.

Tahapan Penelitian terdiri dari Proses enkripsi dan dekripsi menggunakan algoritma Hill Cipher dan Arnold Cat Map dilakukan melalui langkah-langkah berikut:

1. Proses enkripsi dengan algoritma *Hill Cipher* dan *Arnold Cat Map* pada citra digital.
   a. Menentukan tiga bilangan bulat (a, b, d) yang akan digunakan sebagai kunci.
   b. Menyiapkan *plain-image* dalam bentuk citra digital berukuran $N \times N$ dengan N merupakan bilangan genap positif.
   c. Mengubah plain-image ke dalam bentuk matriks plain-image yang mana setiap entri matriks tersebut terdiri dari nilai tingkat keabuan warna R (Red), G (Green) dan B (Blue) di setiap piksel pada plain-image.
   d. Membuat kunci dalam bentuk matriks berukuran 2×2 dengan mensubstitusikan dua bilangan bulat (a, b) ke dalam formula matriks yang telah ditentukan.
   e. Mengoperasikan matriks kunci dengan tiap dua entri pada matriks plain-image menggunakan operasi perkalian matriks. Kemudian, hasil dari setiap perkalian tersebut dimodulokan dengan 256 sehingga setiap entri pada matriks hasil enkripsi tetap berada pada interval nilai tingkat keabuan warna R (Red), G (Green) dan B (Blue).
   f. Diperoleh matriks cipher-image (HC) atau matriks citra digital hasil enkripsi menggunakan algoritma Hill Cipher.
   g. Mensubstitusikan dua bilangan bulat (a, b) yang telah ditentukan dan panjang matriks cipher-image (HC) (N) ke dalam persamaan Arnold Cat Map.
   h. Mentransformasikan posisi tiap entri matriks cipher-image (HC) ke titik lain menggunakan persamaan Arnold Cat Map dengan perulangan sebanyak bilangan bulat (d) kali.
   i. Diperoleh matriks cipher-image (HC-ACM) atau matriks citra digital hasil enkripsi menggunakan algoritma Hill Cipher dan Arnold Cat Map.
   j. Mengembalikan matriks cipher-image (HC-ACM) ke dalam bentuk citra digital.
   k. Diperoleh citra digital hasil enkripsi menggunakan algoritma Hill Cipher dan Arnold Cat Map atau cipher-image (HC-ACM).

2. Proses dekripsi dengan algoritma *Hill Cipher* dan *Arnold Cat Map* pada citra digital.
   a. Menentukan tiga bilangan bulat (a, b, d) yang sama dengan bilangan yang digunakan sebagai kunci pada proses enkripsi.
   b. Menyiapkan *cipher-image* (HC-ACM) atau citra digital hasil enkripsi menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map* berukuran $N \times N$ dengan N merupakan bilangan genap positif.
   c. Mengubah *cipher-image* (HC-ACM) ke dalam bentuk matriks *cipher-image* (HC-ACM) yang mana setiap entri matriks tersebut terdiri dari nilai tingkat keabuan warna R (*Red*), G (*Green*) dan B (*Blue*) di setiap piksel pada *cipher-image (*HC-ACM*)*.
   d. Mensubstitusikan dua bilangan bulat (a, b) dan panjang citra digital (N) dari *cipher-image* $(\mathrm{HC-ACM})$ ke dalam persamaan *Arnold Cat Map.*
   e. Mengembalikan posisi tiap entri matriks *cipher-image* (HC-ACM) ke posisi semula pada *cipher-image* (HC) dengan melakukan transformasi titik menggunakan persamaan *Arnold Cat Map* dengan perulangan sebanyak bilangan bulat (d) kali.
   f. Diperoleh matriks *cipher-image* (HC) atau matriks citra digital hasil enkripsi menggunakan algoritma *Hill Cipher.*
   g. Membuat kunci dalam bentuk matriks berukuran 2×2 dengan mensubstitusikan dua bilangan bulat (a, b) ke dalam formula matriks yang telah ditentukan dan melakukan operasi *invers* matriks pada matriks kunci tersebut.
   h. Mengoperasikan matriks kunci yang telah di-*invers* dengan tiap dua entri pada matriks *cipher-image* (HC) menggunakan operasi perkalian matriks. Kemudian, hasil dari setiap perkalian tersebut dimodulokan dengan 256 sehingga setiap entri pada matriks hasil dekripsi tetap berada pada interval nilai tingkat keabuan dari R (*Red*), G (*Green*) dan B (*Blue*).
   i. Diperoleh matriks *plain-image* atau matriks citra digital hasil dekripsi menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map.*
   j. Mengembalikan matriks *plain-image* ke dalam bentuk citra digital.

4. HASIL DAN PEMBAHASAN

Pengujian didalam penelitian ini hanya menggunakan satu jenis citra digital (file *leni.jpg*). sehingga hasilnya belum dapat digeneralisasi ke berbagai tipe citra dengan ukuran, format, atau karakteristik visual yang berbeda. Hal ini membatasi ruang lingkup validitas eksternal dari temuan penelitian.

Penelitian ini membandingkan performa tiga metode Hill Cipher, Arnold Cat Map, dan kombinasi keduanya. Analisis komparatif tersebut masih terbatas pada indikator SSIM dan waktu proses. Evaluasi belum mencakup pengujian terhadap metrik keamanan lain seperti entropy, histogram uniformity, NPCR, dan UACI yang umum digunakan untuk menilai kekuatan enkripsi terhadap berbagai jenis serangan.

Berikut pengujian menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map* serta kombinasi keduanya terhadap citra digital uji. Hasil pengujian dapat dilihat pada Tabel 4.1.

Tabel 1. Hasil Pengujian Enkripsi dan Dekripsi

No	Citra Digital Awal	Metode	Nilai SSIM Enkripsi	Hasil Enkripsi	Nilai SSIM Dekripsi	Hasil Dekripsi
1		Hill Cipher	0,041		1	
2		Arnold Cat Map	0,102		1	
3		Hill Cipher + Arnold Cat Map 1 Iterasi	0,0112		1	
4		Hill Cipher + Arnold Cat Map 2 Iterasi	0,0097		1	

Dapat dilihat pada Tabel 4.1, pengujian dilakukan dengan metode yang berbeda. Nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan dari proses enkripsi menggunakan citra digital yang sama tetapi dengan metode *Hill Cipher* saja dengan $a = 2$ dan $b = 3$ yang digunakan sebagai kunci maka nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan pada pengujian ini adalah $0{,}041$. Kemudian, untuk nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan dari proses dekripsi menggunakan citra digital hasil enkripsi menghasilkan nilai 1 untuk semua pengujian.

Kemudian pengujian menggunakan algoritma *Arnold Cat Map* terhadap citra digital uji, untuk nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan dari proses enkripsi menggunakan citra digital yang sama dengan nilai kunci $a = 2$ dan $b = 3$ yang digunakan sebagai kunci maka dapat nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan pada pengujian ini adalah $0{,}102$. Kemudian, untuk nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan dari proses dekripsi

menggunakan citra digital hasil enkripsi menghasilkan nilai 1 untuk semua pengujian.

Tabel 2. Pengujian Waktu Komputasi Enkripsi dan Dekripsi

Metode	Waktu Enkripsi (s)	Waktu Dekripsi (s)
Hill Cipher	±1,234	±1,100
Arnold Cat Map	±1,876	±1,456
Kombinasi Hill Cipher dan Arnold Cat Map	2,151 (1 iterasi); 3,661 (2 iterasi)	2,347 (1 iterasi); 4,050 (2 iterasi)

Kemudian pengujian menggunakan kombinasi algoritma *Hill Cipher* dan *Arnold Cat Map* terhadap citra digital uji. Hasil pengujian dapat dilihat pada Tabel 4.2, pengujian dilakukan kunci yang sama dengan $a = 2$ dan $b = 3$ tetapi dengan jumlah iterasi yang berbeda. Untuk proses enkripsi dengan kombinasi algoritma *Hill Cipher* dan *Arnold Cat Map* 1 iterasi membutuhkan waktu enkripsi yang relatif cepat yaitu 2,151 detik . Sedangkan untuk proses enkripsi dengan kombinasi algoritma *Hill Cipher* dan *Arnold Cat Map* 2 iterasi membutuhkan waktu yang lebih lama yaitu 3,661 detik. Kasus yang sama terjadi juga pada proses dekripsi citra digital.

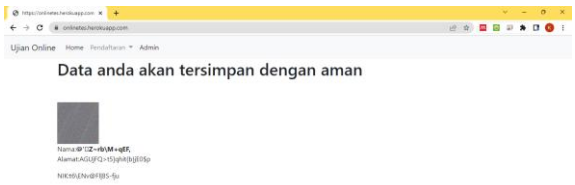
Selanjutnya, untuk nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan dari proses enkripsi menggunakan citra digital yang sama dan 1 iterasi yang dilakukan maka nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan adalah 0,0112. Dalam pengujian ini juga untuk 2 iterasi dapat menghasilkan nilai *Structural Similarity Index Metrics* (SSIM) yang lebih kecil, yaitu 0,0097. Hal tersebut menunjukkan bahwa semakin banyak iterasi yang dilakukan maka didapatkan nilai SSIM semakin kecil.

Kemudian, untuk nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan dari proses dekripsi menggunakan citra digital hasil enkripsi menghasilkan nilai 1 untuk semua pengujian. Hal tersebut menunjukkan bahwa citra digital yang dihasilkan identik atau sama dengan citra digital awal.

Selanjutnya, untuk implementasinya pada website, Data pengguna yang di inputkan melalui website pendaftaran peserta ujian online akan di enkripsi terlebih dahulu menggunakan algoritma *Hill cipher* dan *Arnold Cat Map*, Lalu data pengguna dalam bentuk *cipher text* dan data citra pengguna dalam bentuk *cipher image* disimpan ke database seperti pada gambar 4.1

Gambar 1. Tampilan web admin Django

Tujuan dari disimpannya data pengguna dalam bentuk *cipher text* dan data citra pengguna dalam bentuk *cipher image* adalah jika terjadi kebocoran database maka data teks maupun data citra tetap tidak terbaca karena tersimpan dalam bentuk *cipher text* dan *cipher image* seperti pada gambar 4.2



Gambar 2. Tampilan Antarmuka Halaman Website Data Pengguna yang telah terenkripsi

Pengguna dapat kembali melihat data semula yang didapat dari proses dekripsi data dari database setelah login menggunakan nama dan password.

4.2 Analisa Hasil Pengujian

Pengujian pada penelitian ini dilakukan secara terpisah untuk tiap algoritma sebelum dianalisis secara komparatif. Pada enkripsi Hill Cipher saja, SSIM rata-rata masih relatif tinggi (menunjukkan kesamaan tertentu dengan citra asli), sementara Arnold Cat Map menunjukkan SSIM lebih rendah karena efektivitas permutasi piksel. Namun, kombinasi keduanya menghasilkan *cipher-image* dengan SSIM sangat rendah (rata-rata ≈0,0112, terendah 0,0097), menandakan perbedaan yang signifikan dari citra asli. Seluruh metode berhasil dikembalikan sempurna melalui proses dekripsi (SSIM = 1). Dari sisi performa, Hill Cipher memiliki waktu enkripsi pendek (sekitar 1,2 detik) karena hanya operasi matriks, sedangkan Arnold Cat Map lebih lama (~1,9 detik) tergantung iterasi. Kombinasi kedua algoritma memperpanjang waktu komputasi (sekitar 2,151 detik pada iterasi pertama dan 3,661 detik pada iterasi kedua) sebagai konsekuensi dua tahap proses.

Secara komparatif, analisis keamanan menunjukkan bahwa Hill Cipher rentan terhadap serangan yang mengandalkan polanya, sedangkan Arnold Cat Map sendirian memiliki ruang kunci terbatas akibat periodisitas pendek. Kombinasi keduanya mengatasi kekurangan ini: Hill Cipher menyebarkan informasi ke seluruh citra (difusi), sedangkan Arnold Cat Map menciptakan *confusion* melalui pengacakan intensif piksel. Temuan ini sejalan dengan literatur yang menyatakan bahwa penggabungan teknik kriptografi meningkatkan kekuatan sistem (misalnya, algoritma kombinasi menunjukkan ruang kunci lebih besar dan tahan serangan lebih tinggi). Perbedaan mendasar pada nilai SSIM dan pengaruh waktu komputasi juga memperlihatkan trade-off efektivitas vs performa. Tabel 4.1 dan 4.2 menegaskan bahwa metode gabungan memberikan tingkat keamanan (SSIM

terendah) terbaik, meski memerlukan waktu komputasi lebih besar.

4.2 Limitasi Penelitian

Penelitian ini memiliki beberapa keterbatasan yang perlu diakui secara eksplisit sebagai bagian dari transparansi ilmiah. Pertama, pengujian dilakukan hanya pada satu jenis citra digital.

Kedua, proses enkripsi dan dekripsi belum dioptimalkan dari sisi komputasi. Implementasi saat ini belum memanfaatkan pemrosesan paralel atau akselerasi GPU, sehingga performa waktu proses berpotensi tidak efisien jika diterapkan pada citra berukuran besar atau dalam sistem berskala besar.

Ketiga, sistem belum diuji terhadap berbagai bentuk serangan kriptanalisis seperti known-plaintext attack, chosen-plaintext attack, atau brute-force, yang sangat penting untuk menilai ketahanan algoritma secara komprehensif dalam konteks keamanan dunia nyata.

5. KESIMPULAN DAN SARAN

Penelitian ini berhasil mencapai tujuan awal dengan mengimplementasikan enkripsi citra digital menggunakan Hill Cipher dan Arnold Cat Map dalam satu sistem web berbasis Django. Kombinasi kedua algoritma menghasilkan *cipher-image* yang sangat berbeda dari citra asli (SSIM enkripsi terendah ≈0,0097) serta dekripsi sempurna (SSIM=1). Dari segi performa, waktu enkripsi meningkat dengan bertambahnya iterasi Arnold Cat Map, namun masih dalam batas wajar untuk aplikasi web. Implikasi teoretisnya, integrasi algoritma linier dan chaos memperkuat difusi serta konfusi, sesuai dengan prinsip Shannon, sehingga sistem menjadi lebih tahan terhadap analisis kriptografi. Keberhasilan implementasi pada platform Django menunjukkan kelayakan penerapan metode ini dalam lingkungan nyata. Hasil ini memperkuat hipotesis bahwa kombinasi Hill Cipher dan Arnold Cat Map layak digunakan pada sistem keamanan data berbasis web.

Untuk penelitian selanjutnya, beberapa rekomendasi yang lebih spesifik meliputi eksplorasi algoritma chaos lain, Menerapkan peta chaos tambahan, misalnya Logistic Map atau peta chaos dimensi tinggi untuk meningkatkan kompleksitas enkripsi dan memperpanjang periode kunci.

Selain itu, disarankan untuk mengimplementasikan teknik percepatan komputasi, misalnya pemrosesan paralel/GPU agar enkripsi-dekripsi dapat berlangsung lebih cepat tanpa mengurangi keamanan. Dengan saran-saran tersebut, diharapkan penelitian berikutnya dapat memperkuat dan memperluas kontribusi yang telah dicapai, sesuai dengan perkembangan riset enkripsi citra digital saat ini.

DAFTAR PUSTAKA

Abdo, Azza A., Hanaa F. Morse dan Maissa A. El-Mageed. 2020. An Efficient Color Image Encryption Scheme Based On Combination Of Hill Cipher And Cellular Neural Network. Indian Journal of Computer Science and Engineering (IJCSE) Vol. 11 No. 2.

Agustini., 2024. Penerapan pengolahan citra untuk pengenalan wajah: studi literatur. East Asian Journal of Multidisciplinary Research, 6(3).

Banu, S. dan Amutha, R., 2021. Secure image encryption approach using chaotic maps and matrix transformation. Multimedia Tools and Applications, 80(18), pp.27811–27832.

Chai, X., Fu, X. dan Gan, Z., 2020. Color image cryptosystem based on dynamic chaos and DNA encoding. Signal Processing, 176, p.107684.

Fitri, R. dan Rahmadani, S., 2024. Implementasi Algoritma Hill Cipher dengan Matriks Kunci pada Sistem Keamanan Data. Jurnal Nasional Komputasi dan Teknologi Informasi Vol. 7 No. 4.

Hariyanto, Eko dan Robbi Rahim. 2016. Arnold's Cat Map Algorithm in Digital Image Encryption. International Journal of Science and Research (IJSR) Volume 5 Issue 10.

Hussain, I., Shah, T. dan Mahmood, H., 2022. A robust chaos-based image encryption scheme resistant to statistical and differential attacks. Journal of Information Security and Applications, 65, p.103104.

Inam, S., Kanwal, S., Firdous, R., & Hajjej, F. 2024. Blockchain-based medical image encryption using Arnold's cat map in a cloud environment. Scientific Reports, 14, Article 5678.

Li, H., Zhou, Q. dan Chen, X., 2023. Hybrid Chaos-Based Image Encryption Using Dynamic Matrix Diffusion. IEEE Access, 11, pp.55421–55435.

Mafula, V.Y., 2025. Hill Cipher-Based Visual Cryptography for Copyright Protection of Digital Images. *Journal of Software and Computer Engineering*, 2(1), pp.1–9.

Munir, Rinaldi. 2012. Algoritma Enkripsi Citra Digital Berbasis Chaos dengan Penggabungan Teknik Permutasi dan Teknik Substitusi Menggunakan Arnold Cat Map dan Logistic Map. ISSN : 2087-2658.

Neamah, A. A. 2023. An image encryption scheme based on a seven-dimensional hyperchaotic

system and Pascal's matrix. Journal of King Saud University – Computer and Information Sciences, 35(3), 238–248.

Pratama, R., Sari, D. dan Nugroho, A., 2021. *Implementasi Hill Cipher dan Arnold Cat Map pada Enkripsi Citra Digital*. Jurnal Teknologi Informasi dan Ilmu Komputer, 8(4), pp.721–728.

Purba, R. Arwin Halim dan Indra Syahputra. 2014. Enkripsi Citra Digital Menggunakan Arnold's Cat Map dan Nonlinear Chaotic Algorithm. ISSN : 1412-0100.

Qin, Y., Luo, Y., Wang, X. dan Zhang, H., 2023. Privacy-Preserving Biometrics Image Encryption and Digital Signature Technique Using Arnold and ElGamal. Applied Sciences, 13(14), p.8117

Ratna, A.A.P., Mahendra, I.G.A.P. dan Arthawan, K.G., 2021. Chaos-Based Image Encryption Using Arnold's Cat Map Confusion and Henon Map Diffusion. Advances in Science, Technology and Engineering Systems Journal, 6(1), pp.316–326.

Rhouma, R., Belghith, S. dan Solak, E., 2021. Cryptanalysis and improvement of chaos-based image encryption schemes. *Nonlinear Dynamics*, 105(1), pp.875–892.

Sharma, M. 2010. Image Encryption Techniques Using Chaotic Schemes: A Review. International Journal of Engineering Science and Technology 2(6), pp. 2359-2363.

Turan, M., Gökçay, E., & Tora, H. 2024. An unrestricted Arnold's cat map transformation. Multimedia Tools and Applications, 83, 70921–70935.

Wang, X., Liu, L. dan Zhang, Y., 2022. A Novel Hybrid Chaotic Image Encryption Algorithm Based on Matrix Transformation and Dynamic Permutation. Entropy, 24(9), pp.1–18.

Wang, X., Ünal, Ç. dan Kocamaz, U.E., 2022. Novel hyperchaotic image encryption algorithm with strong diffusion and confusion properties. *Chaos, Solitons and Fractals*, 157, p.111987.

Xi, L., Chen, Y. dan Zhao, H., 2024. Hybrid Chaotic Image Encryption Scheme Based on Matrix Transformation and Dynamic Diffusion. Security and Communication Networks, 2024(1), pp.1–15.

Xi, Y., Ning, Y., Jin, J., & Yu, F. 2024. A dynamic Hill cipher with Arnold scrambling technique for medical images encryption. Mathematics, 12(24), 3948.

Zhang, Y., 2023. A Review of Chaos-Based Image Encryption Techniques and Their Security Applications. Journal of Information Security and Applications, 72(1), pp.103–118.

Zhang, Y. dan Liu, H., 2022. Image Encryption Scheme Based on Arnold Cat Map and Chaotic Systems. International Journal of Network Security, 24(3), pp.456–464.

Zhou, N., Pan, S. dan Cheng, S., 2021. Image encryption scheme using coupled chaotic map lattices and dynamic S-boxes. Information Sciences, 579, pp.639–653.