Terjemahan dari 10.22146/jnteti.v13i2.9623

Teknik Konfusi dan Difusi untuk Proses Enkripsi Citra Berbasis Sistem *Chaos*

Magfirawaty Magfirawaty[1], Ariska Allamanda[1], Malika Ayunasari[1], Muhamad Nadhif Zulfikar[1]

[1] Program Studi Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, Bogor, Jawa Barat 16120, Indonesia

[Diserahkan: 19 September 2023, Direvisi: 8 Desember 2023, Diterima: 20 Maret 2024]
Penulis Korespondensi: Magfirawaty Magfirawaty (email: magfirawaty@poltekssn.ac.id)

INTISARI — Pengenalan wajah menggunakan teknologi biometrik untuk mengidentifikasi manusia berdasarkan karakteristik wajah. Metode ini biasanya digunakan untuk membatasi kontrol akses informasi. Salah satu keuntungan dari sistem pengenalan wajah adalah kemudahan penggunaan dan keamanannya. Proses pengenalan wajah manusia terdiri atas deteksi wajah, pelacakan wajah, dan pengenalan wajah. Proses ini menggunakan beberapa algoritma: Viola-Jones untuk deteksi wajah, Kanade-Lucas-Tomasi (KLT) untuk pelacakan wajah, dan *principal component analysis* (PCA) untuk pencocokan wajah. Lebih lanjut, penelitian ini mengusulkan pengenalan wajah dengan proses enkripsi untuk melindungi data yang tersimpan di dalam basis data. Proses enkripsi terdiri atas dua proses utama: konfusi dan difusi. Proses konfusi adalah pengacakan posisi piksel gambar asli. Penelitian ini menggunakan *Arnold cat map* (ACM) untuk proses konfusi, sedangkan proses difusi dilakukan dengan menggunakan operasi XOR dengan kunci yang dibangkitkan dari sistem *chaos* 1D. Tiga sistem *chaos* 1D yang berbeda digunakan dalam penelitian ini, yaitu *logistic map*, *Bernoulli map*, dan *tent map*, untuk perbandingan sistem *chaos* terbaik dari hasil enkripsi. Pengujian dilakukan dengan membandingkan berbagai parameter pada ketiga sistem *chaos* 1D yang diusulkan, antara lain koefisien korelasi, analisis histogram, nilai entropi, *number of pixels change rate* (NPCR), dan *unified average changing intensity* (UACI). Berdasarkan pengujian terhadap hasil enkripsi citra, proses difusi dengan menggunakan *tent map* menghasilkan enkripsi citra yang paling baik dibandingkan dengan sistem *chaos* lainnya.

KATA KUNCI — Pengenalan Wajah, *Arnold Cat Map*, *Logistic Map*, *Bernoulli Map*, *Tent Map*.

I. PENDAHULUAN

Banyak perusahaan yang menggunakan teknologi dalam menjalankan perusahaannya dari waktu ke waktu. Aset berharga merupakan salah satu hal yang harus dilindungi dalam sebuah perusahaan. Aset-aset tersebut biasanya disimpan di dalam sebuah ruangan dan membutuhkan kontrol akses dengan autentikasi keamanan. Biasanya, *smart card* digunakan untuk proses autentikasi tersebut. Namun, sistem ini tidak efisien karena kartu dapat hilang akibat kesalahan manusia. Oleh karena itu, perlu dikembangkan proses autentikasi yang memanfaatkan teknologi, khususnya teknologi biometrik. Penggunaan biometrik makin meningkat, terutama pada aplikasi yang berhubungan dengan keamanan, seperti kontrol akses logika dan fisik, investigasi forensik, keamanan teknologi informasi (TI), perlindungan penipuan identitas, dan pencegahan atau deteksi terorisme [1]. Teknologi biometrik dapat diklasifikasikan berdasarkan jenis sinyal yang digunakan, yaitu sinyal fisiologis, perilaku, dan kognitif [2]. Biometrik fisiologis menggunakan karakteristik fisik seperti mata, sidik jari, dan wajah.

Pengenalan wajah merupakan teknologi pengenalan biometrik berdasarkan fitur wajah manusia yang dapat dilakukan dengan masukan 2D dengan citra atau 3D dengan proses pelatihan [2]. Sistem pengenalan wajah pada umumnya terdiri atas deteksi wajah, pelacakan wajah, dan pengenalan wajah [3], [4]. Pada setiap proses tersebut, diimplementasikan algoritma pemrosesan untuk mendapatkan keluaran.

Ada banyak jenis algoritma yang digunakan dalam proses pengenalan wajah. Penelitian ini membuat sistem pengenalan wajah dengan menggunakan algoritma Viola-Jones untuk deteksi wajah, algoritma Kanade-Lucas-Tomasi (KLT) untuk pelacakan wajah, dan algoritma *principal component analysis* (PCA) untuk pengenalan wajah berdasarkan penelitian sebelumnya [5]-[7]. Referensi [5] menerapkan algoritma Viola-Jones serta membandingkan penggunaan algoritma PCA dan *linear discriminant analysis* (LDA). Hasilnya menunjukkan bahwa PCA lebih baik daripada LDA pada jumlah citra basis data yang sedikit.

Berdasarkan sistem pengenalan wajah yang dibuat, pengamanan data citra yang tersimpan dalam basis data selama proses pelatihan sangat diperlukan. Pengamanan bertujuan untuk mencegah penyalahgunaan citra wajah, sehingga citra tersimpan ditampilkan bukan sebagai citra asli. Proses yang diterapkan dalam pengamanan tersebut adalah enkripsi pada saat penyimpanan citra dan proses dekripsi untuk proses pencocokan pada saat pengenalan wajah. Referensi [8] melakukan pengenalan wajah dengan skema enkripsi citra yang menggunakan operasi XOR dan permutasi piksel dengan metode pengacakan, sedangkan algoritma pengenalan wajahnya menggunakan LDA. Penelitian ini menunjukkan bahwa sistem yang diusulkan hanya mencapai akurasi sebesar 8,75%.

Pengamanan data citra dengan menerapkan algoritma enkripsi citra pada sistem pengenalan wajah dapat memanfaatkan XOR dan kunci yang dihasilkan melalui pengacakan [9]. Penelitian ini menggunakan citra *red-green-blue* (RGB) dalam pengolahan citra, yaitu pada sistem pengenalan wajah dan proses enkripsi citra. Model RGB merepresentasikan sebuah citra dengan warna primer: merah, hijau, dan biru, yang diwakili oleh nilai vektor warna piksel [10]. Pemrosesan citra RGB cenderung memakan waktu lebih lama; konversi citra dari RGB ke citra skala abu-abu akan mempermudah dan mempercepat perhitungan untuk

pemrosesan citra [11], [12]. Selain itu, tidak ada proses pengacakan piksel sebelum nilai piksel diubah.

Enkripsi citra memiliki dua proses, yaitu konfusi dan difusi [13]. Konfusi adalah proses untuk melakukan operasi permutasi atau pengacakan piksel-piksel pada citra, sedangkan difusi adalah proses substitusi nilai piksel citra. Enkripsi citra yang hanya memanfaatkan proses konfusi dirasa belum cukup aman karena penyerang masih dapat mengatur ulang piksel-piksel tersebut untuk mendapatkan citra yang asli. Oleh karena itu, perlu ditambahkan proses difusi untuk mengubah nilai piksel citra [13], [14].

Beberapa penelitian telah menggabungkan proses konfusi sistem *chaos* 2D dan difusi yang memanfaatkan sistem *chaos* 1D dalam enkripsi citra. Referensi [14] telah menggunakan sistem *chaos Arnold cat map* (ACM) untuk proses konfusi. Pada proses difusi, digunakan sistem *chaos* 1D *logistic map* untuk menghasilkan *keystream* [14]. Selain *logistic map*, sistem *chaos* 1D yang dapat menghasilkan *keystream* adalah *tent map* dan *Bernoulli map* [13], [15].

Dari permasalahan yang ada, penelitian ini mengimplementasikan skema enkripsi citra berdasarkan proses konfusi dan difusi untuk mengamankan basis data pengenalan wajah. Skema ini menggunakan sistem *chaos* ACM 2D dalam proses konfusi. Namun, proses difusi akan membandingkan tiga sistem *chaos*, yaitu *logistic map*, *Bernoulli map*, dan *tent map*. Semua pemrosesan citra dilakukan dalam format skala abu-abu untuk memudahkan komputasi. Penelitian ini akan menghasilkan sistem pengenalan wajah dengan data citra terenkripsi yang tersimpan di dalam basis data.

Makalah ini terdiri atas empat bagian. Bagian I menjelaskan pengantar penelitian dan metode yang diusulkan. Pada Bagian II, dijelaskan penelitian terkait yang mendukung penyusunan penelitian ini. Kemudian, pada Bagian III, dijelaskan metodologi yang digunakan. Selanjutnya, pada Bagian IV, dipaparkan pengujian dan analisis hasil pengujian. Kesimpulan dijelaskan pada Bagian V.

II. TREN ENKRIPSI PENGENALAN WAJAH

Beberapa penelitian telah dilakukan pada skema enkripsi data untuk sistem pengenalan wajah. Sebagian besar metode yang diusulkan menggunakan sistem *chaos* dan permutasi piksel. Penelitian tentang mekanisme pengawasan yang aman dan enkripsi rangka kunci citra probabilistik ringan telah dilakukan [16]. Penelitian tersebut menggunakan *cosine transform-based chaotic sequence* (CTC) untuk menghasilkan *pseudorandom number generator* (PRNG) dan operasi konfusi-difusi untuk enkripsi rangka kunci citra.

Permutasi juga telah dilakukan pada penelitian sebelumnya [17], [18]. Referensi [17] menggunakan ACM yang dikombinasikan dengan deret Fibonacci. Penelitian ini menggunakan ACM untuk mengacak citra asli dan memodifikasi difusi medan selama periode penggunaan. Referensi [18] menggunakan dua nilai abu-abu acak semu dari *generalized ACM* dan *generalized Bernoulli shift map* untuk meningkatkan ketahanan terhadap serangan statistik, diferensial, dan serangan teks asli. Penelitian menunjukkan bahwa metode yang diusulkan memiliki ruang kunci yang cukup untuk mencegah serangan *brute force*.

Terdapat penelitian tentang enkripsi citra yang menggunakan lebih dari satu sistem *chaos*, yang disebut dengan *hybrid chaos* [19]. Sistem *chaos* tersebut adalah sistem *chaos* 2D dengan *Hénon map*, sistem dinamis waktu diskrit, peta *chaos* 2D untuk permutasi piksel, dan peta *chaos* yang diusulkan oleh para peneliti dengan menggunakan fungsi iterasi. Dari penelitian yang diusulkan, peta *chaos* terbukti memiliki keacakan yang sangat baik dengan ruang parameter yang relatif besar, sehingga cocok digunakan untuk enkripsi citra.

Salah satu metode enkripsi citra yang banyak digunakan adalah XOR [20]-[23]. Referensi [20] mengusulkan skema enkripsi pengacakan piksel menggunakan *Josephus traversing* dan difusi piksel untuk meningkatkan keandalan sistem enkripsi. Proses permutasi dan difusi piksel menggunakan operasi XOR. Selanjutnya, hasil simulasi dan analisis keamanan menunjukkan bahwa skema tersebut terbukti dapat diandalkan.

Penelitian lainnya menggunakan ACM untuk melakukan pengacakan dengan mengimplementasikan permutasi piksel citra sebelum enkripsi [21], [22]. Setelah pengacakan, proses enkripsi dilanjutkan dengan menggunakan operasi XOR dengan nilai *pseudorandom* yang dihasilkan dari *Hénon map*. Sementara itu, sebuah penelitian membandingkan nilai *peak noise-to-signal ratio* (PNSR) dari empat metode, yaitu ACM, *Hénon map*, ACM + *Hénon map*, dan *Hénon map* + ACM. Hasil pengujian menemukan bahwa nilai PNSR terbaik adalah metode dengan ACM + *Hénon map* [21]. Hal ini menunjukkan bahwa ACM mampu melakukan proses *tampering* yang baik dalam proses enkripsi citra.

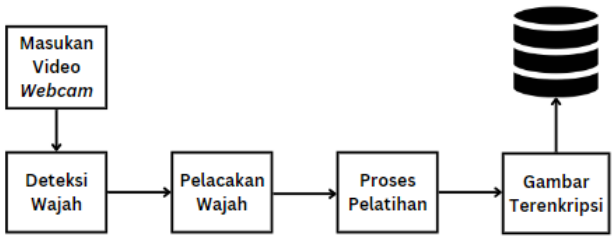
Metode XOR umumnya digunakan untuk enkripsi kriptografi simetris dengan keamanan yang lebih baik jika menggunakan kunci acak yang panjang untuk menghindari serangan *brute force* [23]. Oleh karena itu, pada penelitian ini, operasi XOR diterapkan untuk mengenkripsi citra yang telah dikenai proses permutasi menggunakan ACM. Proses XOR pada enkripsi dan dekripsi dioperasikan dengan kunci atau *keystream* yang dibangkitkan dari *chaos map* seperti *tent map*.

Penelitian sebelumnya telah menggunakan *tent map* untuk membuat kunci rahasia [24], [25]. *Tent map* digunakan untuk menghasilkan angka acak untuk kunci kedua dalam enkripsi citra [24], yang kemudian dikenai operasi XOR dengan citra yang sebelumnya telah mengalami permutasi menggunakan *Hénon Map*, dan kunci tersebut dihasilkan dengan menggunakan metode matriks ortogonal. Pada penelitian lain, *tent map* dikombinasikan dengan *Bernoulli map* untuk menghasilkan kunci kedua, sedangkan kunci pertama dihasilkan dari *logistic sine map* 2D dan *linear congruential generator* (LCG) [25].

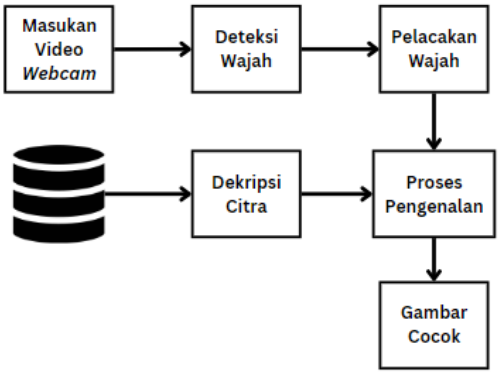
III. METODOLOGI

Enkripsi data citra sistem pengenalan wajah menggunakan proses konfusi dan difusi merupakan fokus utama dari penelitian ini. Sistem pengenalan wajah menggunakan algoritma Viola-Jones, KLT, dan PCA. Proses utama dari sistem ini adalah pelatihan dan proses pengenalan. Enkripsi data citra melibatkan pengaburan menggunakan ACM untuk permutasi piksel. Proses lainnya adalah difusi menggunakan operasi XOR pada piksel, yang dimungkinkan dengan menggunakan *keystream* yang dihasilkan oleh sistem *chaos* 1D. Selanjutnya, penelitian ini membandingkan hasil enkripsi dengan tiga sistem *chaos* 1D yang berbeda dalam proses difusi.

Gambar 1 menunjukkan skema ketika sistem pengenalan wajah melakukan pelatihan atau mengumpulkan citra wajah dari masukan video *webcam*. Proses pelatihan akan mendapatkan beberapa citra wajah setelah melewati tahap deteksi wajah dan pelacakan wajah. Sistem akan mengenkripsi kumpulan citra wajah tersebut dan menyimpannya di dalam basis data sebagai *datasheet* untuk pengenalan wajah.



Gambar 1. Proses pelatihan wajah.



Gambar 2. Proses pengenalan wajah.

Gambar 2 menyajikan skema ketika sistem pengenalan wajah melakukan proses pengenalan. Proses pengenalan memiliki tahapan yang sama dengan proses pelatihan, yaitu deteksi wajah dan pelacakan wajah. Tahapan-tahapan ini akan mendapatkan citra wajah dari masukan video *webcam*, yang akan dicocokkan dengan *datasheet* yang ada di basis data. Selanjutnya, proses pengenalan akan mendekripsi citra wajah dari basis data untuk mendapatkan *datasheet* citra wajah asli. *Datasheet* citra wajah asli ini dibandingkan dengan citra dari masukan video *webcam*. Selanjutnya, proses pencocokan wajah akan menentukan cocok atau tidaknya kedua citra tersebut. Jika kedua citra cocok, proses pengenalan berhasil. Tahapan sistem meliputi deteksi wajah, pelacakan wajah, proses pelatihan, konversi RGB ke skala abu-abu, enkripsi citra, dan pengenalan wajah.

A. DETEKSI WAJAH

Pada penelitian ini, tahap deteksi wajah menggunakan algoritma Viola-Jones. Algoritma ini mengambil bagian wajah yang ditandai dengan kotak kuning. Dengan algoritma ini, sistem akan mendeteksi keberadaan wajah dari video *webcam* yang menjadi masukan.

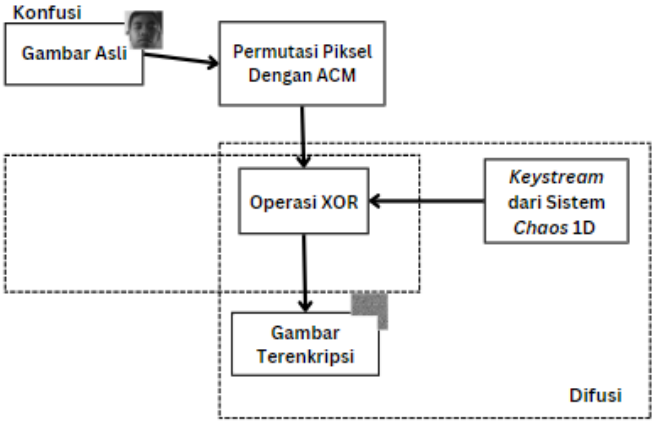
Viola Jones merupakan algoritma yang didasarkan pada fitur Haar. Paul Viola dan Michael Jones, pencipta algoritma ini, menuangkan hasil penelitiannya ke dalam sebuah makalah. Kontribusinya adalah mengusulkan metode deteksi wajah dengan fitur Haar, *integral image*, AdaBoost, dan *cascade* [26]. Dengan menggunakan algoritma ini, proses pendeteksian wajah menjadi lebih singkat.

B. PELACAKAN WAJAH

Pelacakan wajah adalah tahap untuk mengekstraksi fitur wajah yang unik dan melacak objek seperti alis, mata, mulut, dan garis wajah. Berikut adalah beberapa tahapan dalam algoritma KLT [27].

1. Menangkap urutan video dari *file* masukan.
2. Mengekstrak fitur-fitur dari *region of interest* untuk deteksi wajah.
3. Melacak citra wajah saat ini dari citra wajah sebelumnya.

Gambar 3. Proses pelatihan basis data.



Gambar 4. Skema proses enkripsi.

4. Memperkirakan skala, rotasi, serta translasi antara titik terakhir dan titik baru.

C. KONVERSI RGB MENJADI SKALA ABU-ABU

Citra skala abu-abu adalah citra monokrom atau citra satu warna yang hanya berisi informasi kecerahan dan tidak ada informasi warna. Representasi intensitas nilai pikselnya dalam kisaran antara 0 dan 1 (minimum dan maksimum) dan di antara berbagai rentang abu-abu yang berkisar antara 0 dan 255 [10]. Tahap awal dari proses konversi RGB ke skala abu-abu adalah mendapatkan tiga nilai warna primer (merah, hijau, dan biru) dan kemudian mengodekannya menggunakan ekspansi *gamma* dengan rumus sebagai berikut [10].

$$C_{linier} = \begin{cases} \frac{C_{rgb}}{12{,}92} & C_{rgb} \leq 0{,}04045 \\ \frac{(C_{rgb}+0{,}065)}{1{,}065} & C_{rgb} > 0{,}04045 \end{cases} \quad (1)$$

dengan C_{rgb} adalah primer RGB dalam rentang 0 hingga 1 dan C_{linier} adalah nilai intensitas pada bidang 0 hingga 1 dengan konversi yang diperoleh menggunakan fungsi $f(x)$. Fungsi $f(x)$ mengubah nilai RGB menjadi nilai skala abu-abu dengan menjumlahkan komponen R, G, dan B [10].

$$y = f(x) \quad (2)$$

$$f(x) = 0{,}2989 * R + 0{,}5870 * G + 0{,}1140 * B. \quad (3)$$

D. PROSES PELATIHAN

Pada tahap ini, sistem mengambil beberapa citra dan menyimpannya dalam basis data. Proses pelatihan mendaftarkan citra wajah sebagai *datasheet* pencocokan pengenalan wajah. Sistem akan mengambil 20 citra dalam setiap proses pelatihan dan menyimpannya dalam satu *folder*. Gambar 3 menunjukkan citra terenkripsi yang disimpan di dalam basis data.

E. PROSES ENKRIPSI

Dalam penelitian ini, proses enkripsi dilakukan pada citra wajah selama pelatihan. Skema enkripsi citra terdiri atas proses konfusi dan proses difusi. Gambar 4 menunjukkan skema enkripsi citra wajah.

1) KONFUSI

Proses pengaburan diterapkan dengan menggunakan ACM. Pada proses pengaburan citra menggunakan ACM, citra baru yang dihasilkan merupakan hasil dari permutasi setiap posisi piksel pada citra yang melibatkan transformasi permutasi ACM. Sebelum dilakukan permutasi, citra terlebih dahulu diubah ukurannya menjadi 90×90 piksel karena ACM hanya dapat dioperasikan pada citra dengan ukuran $N \times N$. Ukuran citra yang baru akan disimpan dalam variabel dimensi baris dan kolom. Inisialisasi menentukan jumlah iterasi dan parameter a dan b yang akan digunakan dalam rumus ACM. Pada program, jumlah iterasi ditentukan sebanyak 5, dengan nilai a = 34 dan b = 35. Nilai a dan b dalam matriks $\begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix}$ harus menghasilkan determinan yang sama dengan 1 agar hasil transformasi tetap mempertahankan area, yang artinya tetap berada di area citra yang sama [14]. Persamaan ACM untuk melakukan permutasi piksel dengan menggunakan koordinat piksel masukan (X, Y) adalah sebagai berikut [14].

$$\begin{pmatrix} X_{i+1} \\ Y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} X_i \\ Y_i \end{pmatrix} mod\ (N) \quad (4)$$

dengan (X_i, Y_i) adalah posisi piksel dalam citra, (X_{i+1}, Y_{i+1}) adalah posisi piksel baru setelah iterasi ke-i, serta a dan b adalah sembarang bilangan bulat positif. Berdasarkan rumus di atas, iterasi terjadi untuk setiap piksel citra dan perhitungan koordinat baru terjadi pada setiap iterasi.

2) DIFUSI

Hasil permutasi menggunakan ACM kemudian mengalami proses difusi dengan substitusi piksel. Hasilnya berupa gambar yang berbeda dengan gambar awal dengan nilai piksel $(p_1, p_2, \ldots, p_{NxN})$. Nilai-nilai ini akan dikenai operasi XOR dengan *keystream* yang dihasilkan oleh sistem *chaos* 1D. Tiga sistem *chaos* 1D akan dibandingkan untuk hasil enkripsi *logistic map* (5), *Bernoulli map* (6), dan *tent map* (7). Ketiganya dapat digunakan untuk menghasilkan *keystream* (k),

$$k_{i+1} = rk_i\,(1 - k_i) \quad (5)$$

$$k_{i+1} = \begin{cases} sk_i, & 0 \le k_i < 0{,}5 \\ sk_i - 1, & 0{,}5 < k_i \le 1 \end{cases} \quad (6)$$

$$k_{i+1} = \begin{cases} tk_i, & 0 \le k_i \le \frac{1}{t} \\ \frac{t}{t-1}(1 - k_i), & \frac{1}{t} < k_i \le 1 \end{cases} \quad (7)$$

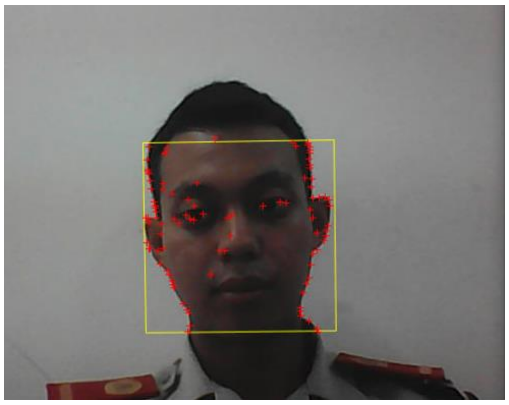
dengan r, s, dan t adalah parameter dalam bilangan real positif. Nilai k_0 ditentukan sebagai nilai inisialisasi untuk pembangkitan *keystream*, $r = 3{,}999$, $s = t = 1{,}99$. Persamaan umum untuk proses difusi dengan substitusi adalah sebagai berikut.

$$c_j = (p_j \oplus c_{j-1}) \oplus k_j \quad (8)$$

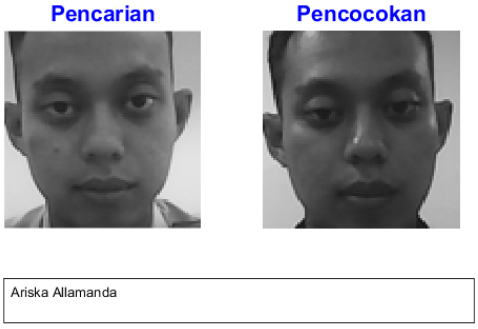
dengan vektor inisialisasi, c_0, adalah piksel pertama yang diperlukan $(IV = 0)$. Bilangan acak yang dihasilkan perlu diubah menjadi bilangan bulat antara 0 dan 255. Nilai piksel dan *keystream* pada indeks ke-j, yang dinyatakan sebagai bilangan bulat, akan dikenai operasi XOR dengan gambar terenkripsi dari piksel-piksel yang teracak dan tersebar. Bagian IV menjelaskan hasil pengujian yang diperoleh.

IV. HASIL DAN DISKUSI

Sistem ini dibuat dengan menggunakan aplikasi pemrograman matematis MATLAB dengan mengintegrasikan *webcam* pada perangkat. Hasil dari sistem ini meliputi hasil dari proses pengenalan wajah dan hasil enkripsi citra dari skema yang diusulkan. Selanjutnya, pengujian pada sistem ini meliputi pengenalan wajah dan enkripsi citra, dengan mengambil beberapa parameter uji, seperti histogram, grafik korelasi, entropi, *number of pixel rate changes* (NPCR), dan *unified average change intensity* (UACI).



Gambar 5. Masukan video *webcam*.



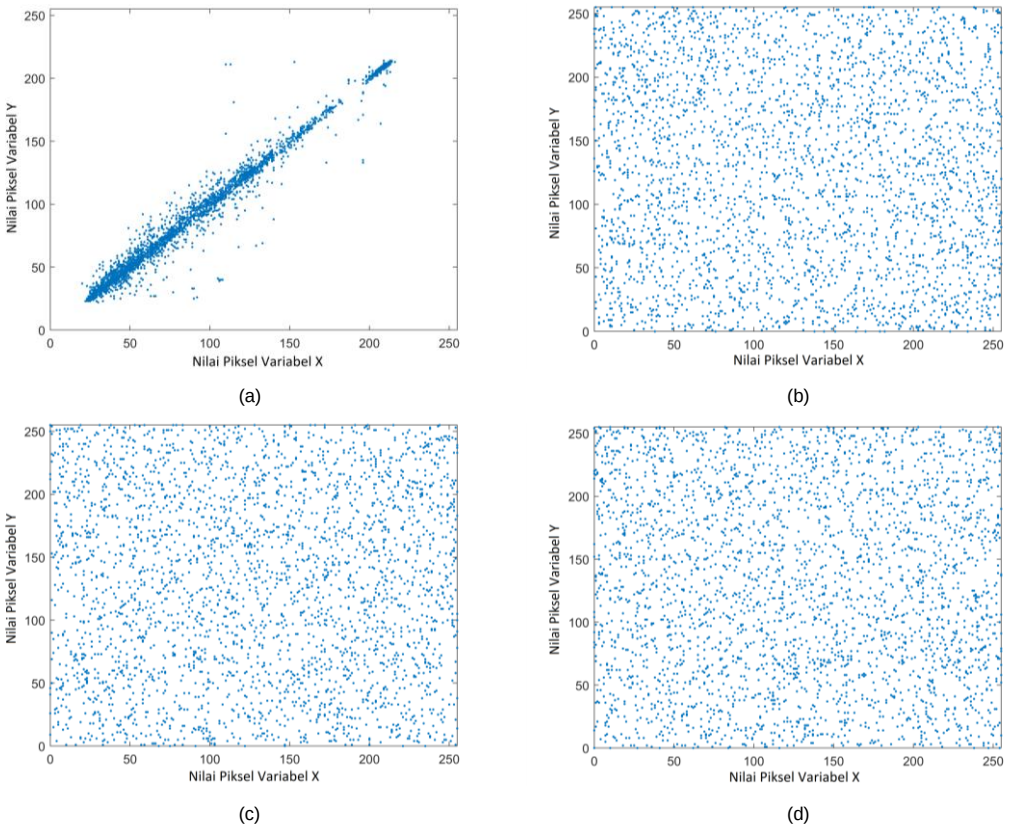
Gambar 6. Hasil pencocokan.

A. PENGENALAN WAJAH

Sistem ini menangkap citra secara *real-time* melalui masukan video *webcam* dan menyimpannya dalam basis data. Proses ini menghasilkan basis data yang berisi seratus citra dengan lima orang sebagai sampel, sehingga setiap orang memiliki sampel dengan 20 citra wajah. Pengambilan citra dilakukan secara *real-time* untuk mencocokkan data yang terdapat di dalam basis data dan wajah masukan dikonversi menjadi skala abu-abu. Gambar 5 menunjukkan sistem deteksi wajah melalui video *webcam* sebagai masukan untuk disimpan dalam basis data dan untuk pencocokan wajah. Selanjutnya, Gambar 6 menunjukkan hasil proses pencocokan antara citra yang ditangkap dengan citra basis data.

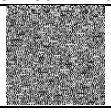
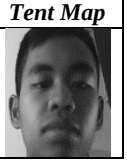
B. ENKRIPSI CITRA

Enkripsi dilakukan selama pelatihan dan sistem menyimpan citra dalam basis data. Oleh karena itu, citra yang tersimpan di dalam basis data adalah citra yang telah dienkripsi. Pada penelitian ini, proses konfusi dilakukan menggunakan ACM, sedangkan difusi menggunakan sistem *chaos* 1D. Hasil permutasi citra dikenai operasi XOR dengan *keystream* yang dihasilkan oleh salah satu sistem *chaos* 1D: *logistic map*, *Bernoulli map*, dan *tent map*. Selanjutnya, citra terenkripsi yang dihasilkan dibandingkan dengan metode pembangkitan *keystream* yang berbeda. Proses enkripsi citra untuk pengenalan wajah dilakukan pada lima orang. Sementara itu, Tabel I menunjukkan hasil enkripsi salah satu dari lima orang tersebut dengan menggunakan sistem *chaos* 1D.



Gambar 7. Grafik koefisien korelasi, (a) pada citra asli, (b) pada *logistic map*, (c) pada *Bernoulli map*, (d) pada *tent map*.

TABEL I
HASIL ENKRIPSI CITRA

Citra Asli	Citra Terenkripsi		
	Logistic Map	*Bernoulli Map*	*Tent Map*
			
	Citra Terdekripsi		
	Logistic Map	*Bernoulli Map*	*Tent Map*
			

Tabel I menunjukkan perbedaan antara hasil citra terenkripsi menggunakan ACM dan dengan *keystream* dari sistem *chaos* 1D yang berbeda. Gambar yang dihasilkan bersifat acak dan tidak beraturan, sehingga dapat mencegah serangan *brute force* pada gambar.

1) GRAFIK KOEFISIEN KORELASI

Grafik koefisien korelasi pada Gambar 7 menunjukkan bahwa ketiga skema pembangkitan *keystream* pada proses difusi menghasilkan distribusi titik-titik biru yang tersebar, tidak seperti citra asli, yang grafik koefisien korelasinya tersebar pada satu garis. Terdapat titik-titik dengan nilai piksel di sekitar garis diagonal 45°, yang mengindikasikan korelasi yang kuat di antara piksel-piksel tersebut. Sebaliknya, nilai piksel didistribusikan secara merata pada citra terenkripsi, sehingga piksel tidak berkorelasi.

Selain itu, korelasi antara dua variabel juga dapat diidentifikasi dari nilai koefisien korelasi yang dihasilkan oleh sebuah citra. Citra asli memiliki nilai koefisien korelasi yang mendekati 1, sedangkan citra terenkripsi mendekati 0. Tabel II sampai Tabel IV menunjukkan nilai koefisien korelasi yang dihasilkan oleh semua citra uji dan citra terenkripsi dengan skema *keystream* menggunakan beberapa fungsi *chaos*.

TABEL II
KOEFISIEN KORELASI MENGGUNAKAN *LOGISTIC MAP KEYSTREAM*

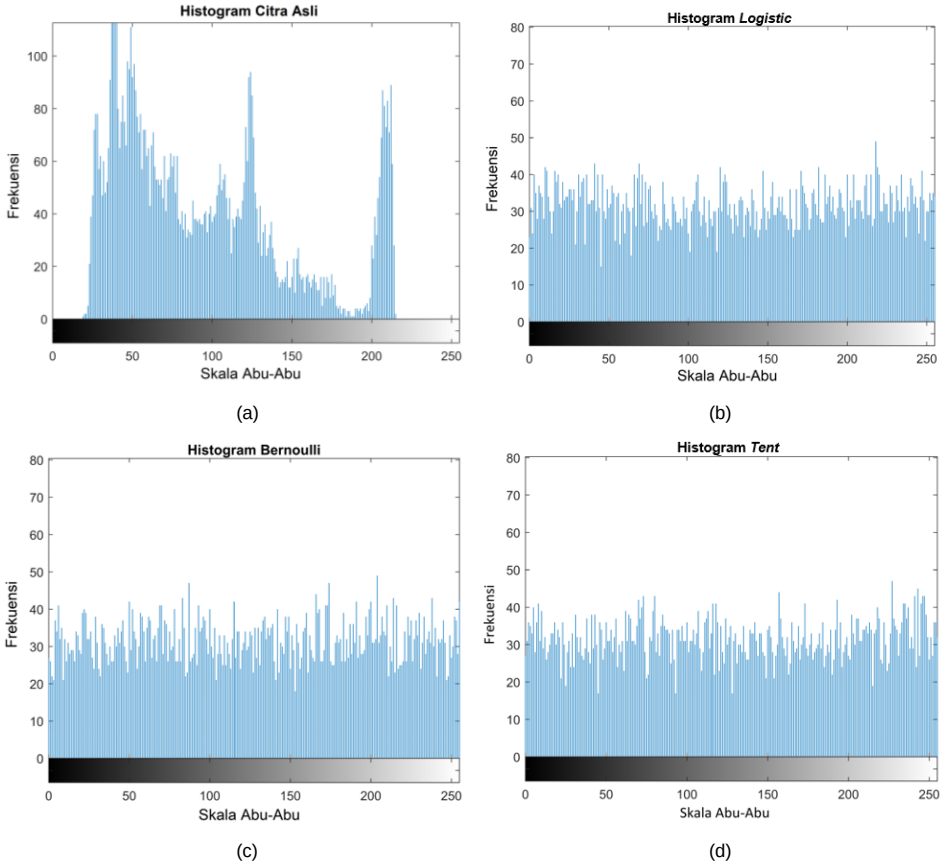
Citra	Diagonal		Horizontal		Vertikal	
	P(x)	*C(x)*	*P(x)*	*C(x)*	*P(x)*	*C(x)*
I	0,9507	-0,0029	0,9199	-0,0027	0,9869	0,0117
II	0,9399	0,0052	0,9322	0,0122	0,9836	0,0122
III	0,8469	0,0132	0,8700	-0,0096	0,9287	0,0085
IV	0,9234	0,0086	0,9332	-0,0020	0,9739	-0,0096
V	0,9548	-0,0068	0,9463	0,0034	0,9863	0,0150

TABEL III
KOEFISIEN KORELASI MENGGUNAKAN *BERNOULLI MAP KEYSTREAM*

Citra	Diagonal		Horizontal		Vertikal	
	P(x)	*C(x)*	*P(x)*	*C(x)*	*P(x)*	*C(x)*
I	0,9507	0,0067	0,9199	-0,3807	0,9869	-0,0090
II	0,9399	0,0047	0,9322	-0,7326	0,9836	-0,0059
III	0,8469	-0,0425	0,8700	-0,5813	0,9287	0,0289
IV	0,9234	0,0111	0,9332	-0,4356	0,9739	-0,0123
V	0,9548	-4,3672	0,9463	-0,4815	0,9863	-0,0060

TABEL IV
KOEFISIEN KORELASI MENGGUNAKAN *TENT MAP KEYSTREAM*

Citra	Diagonal		Horizontal		Vertikal	
	P(x)	*C(x)*	*P(x)*	*C(x)*	*P(x)*	*C(x)*
I	0,9507	0,0022	0,9199	-0,0024	0,9869	0,0137
II	0,9399	0,0102	0,9322	0,0278	0,9836	-0,0092
III	0,8469	-0,0118	0,8700	0,0017	0,9287	-0,0017
IV	0,9234	0,0131	0,9332	0,0104	0,9739	-0,0156
V	0,9548	0,0057	0,9463	0,0137	0,9863	0,0245



Gambar 8. Histogram, (a) pada citra asli, (b) pada *logistic map*, (c) pada *Bernoulli map*, (d) pada *tent map*.

TABEL V
NILAI ENTROPI

Citra	Citra Asli	*Logistic Map*	*Bernoulli Map*	*Tent Map*
I	7,2132	7,9778	7,9764	7,9793
II	5,8787	7,9789	7,9726	7,9795
III	6,6086	7,9731	7,9771	7,9782
IV	7,1905	7,9783	7,9782	7,9763
V	6,9445	7,9758	7,9774	7,9777

2) ANALISIS ENTROPI

Selain koefisien korelasi, nilai entropi informasi dapat mengukur keacakan suatu citra. Nilai entropi maksimum yang dapat dihasilkan oleh citra skala abu-abu adalah 8. Apabila nilai entropi yang dihasilkan mendekati 8, tingkat keacakan piksel citra tersebut tinggi.

Tabel V menunjukkan bahwa ketiga skema yang diusulkan memiliki kekuatan enkripsi yang baik. Entropi merupakan salah satu parameter pengujian hasil enkripsi algoritma kriptografi. Analisis entropi menentukan kekuatan kriptosistem atau keacakan hasil eksekusi program algoritma kriptografi. Entropi yang ideal terjadi ketika nilainya mendekati 8, sedangkan untuk citra yang kurang teracak dengan baik, nilai entropinya jauh dari 8. Teks maupun citra terenkripsi dengan nilai entropi yang baik tidak dapat diprediksi.

Pada penelitian ini, uji entropi dilakukan pada citra asli dan citra terenkripsi. Dapat dilihat pada Tabel V bahwa citra terenkripsi memiliki nilai yang mendekati 8, sedangkan citra asli memiliki nilai entropi yang jauh dari 8. *Keystream* yang dihasilkan oleh *logistic map* menjadi skema enkripsi dengan nilai rata-rata entropi sebesar 7,97678. Nilai entropi rata-rata untuk *keystream* yang dihasilkan oleh *tent map* adalah 7,9782 dan yang dihasilkan oleh *Bernoulli map* adalah 7,97634.

3) ANALISIS HISTOGRAM

Analisis histogram digunakan untuk menemukan informasi tentang distribusi nilai piksel dari citra asli dan citra terenkripsi. Enkripsi yang sangat baik dan kuat akan menghasilkan histogram dengan distribusi nilai piksel yang lebih acak atau merata dalam ruang nilai piksel. Histogram dari citra terenkripsi dan citra asli akan berbeda untuk mencegah serangan statistik pada algoritma.

Gambar 8 menunjukkan bahwa histogram yang dihasilkan oleh citra asli tidak merata dan terdapat banyak penumpukan pada nilai tertentu. Histogram dari citra terenkripsi dengan proses difusi menggunakan *keystream* dari ketiga jenis sistem *chaos* 1D yang diusulkan memiliki distribusi garis yang merata, yang mengindikasikan bahwa skema enkripsi yang diimplementasikan memiliki keamanan yang cukup baik dalam melindungi citra asli.

4) NPCR DAN UACI

NPCR dan UACI adalah dua parameter standar yang digunakan untuk memeriksa efek perubahan piksel tunggal pada seluruh citra. NPCR berfokus pada jumlah absolut piksel yang berubah nilainya dalam serangan diferensial, sedangkan UACI berfokus pada perbedaan rata-rata antara dua citra yang dibandingkan. Secara umum, persamaan berikut ini digunakan untuk menghitung nilai NPCR.

$$\text{NPCR}\,(L_1, L_2) = \frac{\sum_{m,n} D(m,n)}{W \; x \; H} \; \text{x}\; 100\% \qquad (9)$$

dengan W dan H adalah lebar dan tinggi citra yang dienkripsi, L_1 dan L_2, sedangkan $D_{(m,n)}$ mewakili nilai korespondensi piksel antara L_1 dan L_2. NPCR menghitung jumlah piksel yang berubah nilainya di antara dua citra yang dienkripsi. Sebagai perbandingan, UACI mengukur perbedaan rata-rata dalam nilai

TABEL VI
NILAI NPCR DAN UACI

Citra	NPCR			UACI		
	Logistic Map	*Bernoulli Map*	*Tent Map*	*Logistic Map*	*Bernoulli Map*	*Tent Map*
I	99,5556%	99,5679%	99,6173%	31,6531%	31,1214%	31,4001%
II	99,5556%	99,6420%	99,5185%	36,4674%	36,4076%	36,8611%
III	99,5802%	99,5556%	99,6543%	30,5049%	30,5465%	30,2400%
IV	99,6420%	99,7037%	99,6173%	32,3277%	32,6082%	33,0326%
V	99,6420%	99,7901%	99,5802%	31,2585%	30,9979%	30,9502%
Rata-rata	99,5951%	99,6519%	99,5975%	32,4423%	32,3363%	32,4968%

piksel antara dua citra, atau lebih tepatnya adalah intensitasnya. Persamaan untuk mendapatkan nilai UACI dapat didefinisikan sebagai berikut.

$$\text{UACI} = (L_1, L_2) = \frac{1}{W\,x\,H}\left[\sum_{\text{m,n}} \frac{L_1(\text{m,n}) - L_2(\text{m,n})}{255}\right] \times 100\%. \quad (10)$$

Nilai NPCR yang tinggi mengindikasikan bahwa algoritma enkripsi menyebabkan banyak perubahan pada piksel citra, sedangkan UACI yang tinggi berarti intensitas citra yang dienkripsi dengan citra asli.

Tabel VI menunjukkan bahwa nilai NPCR dari lima sampel citra yang dienkripsi dengan tiga skema enkripsi yang diusulkan mendekati 100%, yang mengindikasikan bahwa terdapat perubahan yang signifikan pada piksel citra asli dengan citra terenkripsi. Sementara itu, nilai UACI sekitar 30% berarti terjadi perubahan intensitas antara citra asli dengan citra terenkripsi.

V. KESIMPULAN

Penelitian ini menunjukkan bahwa penggunaan algoritma enkripsi pada citra dengan menggunakan *keystream* dari sistem *chaotic* 1D (*logistic* dan yang lainnya) pada sistem pengenalan wajah telah meningkatkan keamanan dan privasi data citra. Koefisien korelasi titik-titik yang terdistribusi secara merata pada semua jenis sistem *chaos* 1D menunjukkan keefektifan dalam meminimalkan ketergantungan antarpiksel pada citra. Hal ini menunjukkan bahwa semua jenis sistem *chaos* 1D menghasilkan *keystream* dengan tingkat keacakan yang relatif tinggi dengan histogram yang terdistribusi merata. Berdasarkan analisis entropi, *tent map* menjadi *keystream* untuk proses difusi dengan nilai entropi tertinggi, yaitu 7,9782. Analisis NPCR dari *keystream* ketiga dari sistem *chaos* 1D mendekati 100%, yang mengindikasikan adanya perubahan yang signifikan antara citra asli dan citra terenkripsi.

Selain itu, nilai UACI sekitar 30% menunjukkan perubahan intensitas antara citra asli dan citra terenkripsi. Kedua metrik ini mengonfirmasi bahwa algoritma enkripsi berhasil mencapai tingkat perubahan yang signifikan pada citra yang dienkripsi, yang merupakan karakteristik penting dari algoritma enkripsi yang baik. Dengan demikian, algoritma sebagai pembangkit *keystream* yang paling kuat adalah *tent map*. Secara keseluruhan, penelitian ini menemukan bahwa penggunaan sistem *chaos* 1D dalam algoritma enkripsi citra sistem pengenalan wajah dapat menghasilkan citra terenkripsi yang kompleks secara visual, tetapi tetap mempertahankan kemampuan pengenalan wajah dan dapat meningkatkan keamanan data.

KONFLIK KEPENTINGAN

Penulis menyatakan bahwa tidak terdapat konflik kepentingan.

KONTRIBUSI PENULIS

Konseptualisasi, Magfirawaty; metodologi, Magfirawaty; perangkat lunak, Ariska Allamanda dan Malika Ayunasari; validasi, Muhamad Nadhif Zulfikar; analisis formal, Malika Ayunasari; investigasi, Ariska Allamanda; sumber daya, Muhamad Nadhif Zulfikar; kurasi data, Malika Ayunasari; penulisan, Ariska Allamanda dan Malika Ayunasari; pengawasan, Magfirawaty; perolehan dana, Magfirawaty.

REFERENSI

[1] Q. Xiao, "Technology review - Biometrics-technology, application, challenge, and computational intelligence solutions," *IEEE Comput. Intell. Mag.*, vol. 2, no. 2, hal. 5–10, Mei 2007, doi: 10.1109/MCI.2007.353415.

[2] M.S. Obaidat, I. Traore, dan I. Woungang, *Biometric-Based Physical and Cybersecurity Systems.* Cham, Swiss: Springer, 2018.

[3] F. Gong, Y.M. Zhang, dan X.Z. Jiang, "Application research of face recognition algorithm based on MATLAB," *J. Phys., Conf. Ser.*, vol. 2290, hal. 1–6, Jun. 2022, doi: 10.1088/1742-6596/2290/1/012102.

[4] L.A. Ibrahim, Nasser, dan M. Ali, "Face recognition based on statistical texture features," *Embedded Selforganising Syst.*, vol. 7, no. 1, hal. 10–15, Feb. 2020, doi: 10.14464/ess.v7i1.471.

[5] U. Jain, K. Choudhary, S. Gupta, dan M.J.P. Privadarsini, "Analysis of face detection and recognition algorithms using Viola Jones algorithm with PCA and LDA," *2018. 2nd Int. Conf. Trends Electron. Informat. (ICOEI)*, 2018, hal. 945–950, doi: 10.1109/ICOEI.2018.8553811.

[6] L. Liying dan H. Yue, "Study on access control system based on face recognition," *2008 Int. Conf. Comput. Sci. Softw. Eng.*, 2008, hal. 876–878, doi: 10.1109/CSSE.2008.451.

[7] R. Boda dan M.J.P. Priyadarsini, "Face detection and tracking using KLT and Viola Jones," *ARPN J. Eng. Appl. Sci.*, vol. 11, no. 23, hal. 13472–13476, Des. 2016.

[8] E. Abusham, B. Ibrahim, K. Zia, dan M. Rehman, "Facial image encryption for secure face recognition system," *Electron.*, vol. 12, no. 3, hal. 1–26, Feb. 2023, doi: 10.3390/electronics12030774.

[9] M. Magfirawaty dkk., "Principal component analysis and data encryption model for face recognition system," *2022 2nd Int. Conf. Electron. Electr. Eng. Intell. Syst. (ICE3IS)*, 2022, hal. 381–386, doi: 10.1109/ICE3IS56585.2022.10010080.

[10] K. Padmavathi dan K. Thangadurai, "Implementation of RGB and grayscale images in plant leaves disease detection - Comparative study," *Indian J. Sci. Technol.*, vol. 9, no. 6, hal. 1–6, Feb. 2016, doi: 10.17485/ijst/2016/v9i6/77739.

[11] M. Gao dan T.-F. Lu, "Image processing and analysis for autonomous grapevine pruning," *2006 Int. Conf. Mechatronics Autom.*, 2006, hal. 922–927, doi: 10.1109/ICMA.2006.257748.

[12] V. Goel, S. Singhal, T. Jain, dan S. Kole, "Specific color detection in images using RGB modelling in MATLAB," *Int. J. Comput. Appl.*, vol. 161, no. 8, hal. 38–42, Mar. 2017, doi: 10.5120/ijca2017913254.

[13] P.S. Sneha, S. Sankar, dan A.S. Kumar, "A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 3, hal. 1289–1308, Mar. 2020, doi: 10.1007/s12652-019-01385-0.

[14] R. Munir, "Algoritma enkripsi citra digital berbasis chaos dengan penggabungan teknik permutasi dan teknik substitusi menggunakan Arnold cat map dan logistic map," *J. Nas. Pendidik. Tek. Inform., JANAPATI*, vol. 1, no. 3, hal. 166–181, Des. 2012, doi: 10.23887/janapati.v1i3.9814.

[15] W. Zhang, Z. Zhu, dan H. Yu, "A symmetric image encryption algorithm based on a coupled logistic-Bernoulli map and cellular automata diffusion strategy," *Entropy*, vol. 21, no. 5, hal. 1–23, Mei 2019, doi: 10.3390/e21050504.

[16] J. Khan dkk., "SMSH: Secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption," *IEEE Access*, vol. 8, hal. 15747–15767, Jan. 2020, doi: 10.1109/ACCESS.2020.2966656.

[17] D. Elmaci dan N.B. Catak, "An efficient image encryption algorithm for the period of Arnold's cat map," *Int. J. Intell. Syst. Appl. Eng.*, vol. 6, no. 1, hal. 80–84, Jan.-Mar. 2018, doi: 10.18201/ijisae.2018637935.

[18] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," *Optics Commun.*, vol. 284, no. 22, hal. 5290–5298, Okt. 2011, doi: 10.1016/j.optcom.2011.07.070.

[19] A.P. Kari, A.H. Navin, A.M. Bidgoli, dan M. Mirnia, "A new image encryption scheme based on hybrid chaotic maps," *Multimedia Tools Appl.*, vol. 80, no. 2, hal. 2753–2772, Jan. 2021, doi: 10.1007/s11042-020-09648-1.

[20] Y. Niu dan X. Zhang, "A novel plaintext-related image encryption scheme based on chaotic system and pixel permutation," *IEEE Access*, vol. 8, hal. 22082–22093, Jan. 2020, doi: 10.1109/ACCESS.2020.2970103.

[21] C. Irawan dan E.H. Rachmawanto, "Implementasi kriptografi dengan menggunakan algoritma Arnold's cat map dan Henon map," *J. Masy. Inform.*, vol. 13, no. 1, hal. 15–32, Mei 2022, doi: 10.14710/jmasif.13.1.43312.

[22] P. Sankhe, S. Pimple, S. Singh, dan A. Lahane, "An image cryptography using Henon map and Arnold cat map," *Int. Res. J. Eng. Technol.*, vol. 5, no. 4, hal. 1900–1904, Apr. 2018.

[23] M. Tang, G. Zeng, Y. Yang, dan J. Chen, "A hyperchaotic image encryption scheme based on the triple dislocation of the Liu and Lorenz system," *Optik*, vol. 261, hal. 1–22, Jul. 2022, doi: 10.1016/j.ijleo.2022.169133.

[24] S. Kanwal dkk., "An effective color image encryption based on Henon map, tent chaotic map, and orthogonal matrices," *Sensors*, vol. 22, no. 12, hal. 1–17, Jun. 2022, doi: 10.3390/s22124359.

[25] W. Alexan dkk., "Color image encryption through chaos and KAA map," *IEEE Access*, vol. 11, hal. 11541–11554, Feb. 2023, doi: 10.1109/ACCESS.2023.3242311.

[26] P. Viola dan M. Jones, "Rapid object detection using a boosted cascade of simple features," *Proc. 2001 IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR 2001)*, 2001, hal. I-511–I-518, doi: 10.1109/CVPR.2001.990517.

[27] N.H. Barnouti, M.H.N. Al-Mayyahi, dan S.S.M. Al-Dabbagh, "Real-time face tracking and recognition system using Kanade-Lucas-Tomasi and two-dimensional principal component analysis," *2018 Int. Conf. Adv. Sci. Eng. (ICOASE)*, 2018, hal. 24–29, 2018, doi: 10.1109/ICOASE.2018.8548818.