Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871

Vol. 7, No. 3, June 2026, Page. 2465-2479
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484

Peningkatkan Keamanan ElGamal Menggunakan CNN dan Rolling Hash untuk Generasi Kunci dalam Enkripsi Gambar

Achmad Fauzi[1], Teuku Yuliar Arif[2], Yuwaldi Away[3], Roslidar[*4]

[1]Doctoral Program, School of Engineering Science, Universitas Syiah Kuala, Banda Aceh, Indonesia
[1]STMIK Kaputama, Jl. Veteran No. 4A–9A, Binjai, North Sumatra, Indonesia
[2,3,4]Department of Electrical and Computer Engineering, Universitas Syiah Kuala, Banda Aceh, Indonesia

Email: [4]roslidar@usk.ac.id

Received : Jan 29, 2026; Revised : Feb 5, 2026; Accepted : Feb 5, 2026; Published : Juni 15, 2026

Abstract

The large scale exchange of digital images requires security mechanisms that are robust not only at the cryptographic algorithm level but also in the key generation process, which is often the weakest component of the system. In conventional ElGamal schemes, security may degrade due to static entropy sources and predictable key patterns. This study proposes an ElGamal key generation model based on a pipeline of Convolutional Neural Networks (CNNs) and a rolling hash function, utilizing visual image content as an adaptive entropy source. The CNN extracts latent features through a fully connected layer, while the rolling hash enhances diffusion and key sensitivity to minor image variations. The model was evaluated using the CIFAR-10 dataset in PNG, WEBP, and JPG formats. Experimental results show stable key generation times ranging from 0.426 to 0.444 ms, with high entropy values between 7.98 and 7.99 bits, indicating strong randomness and resistance to prediction. Strong diffusion characteristics were also observed (PSNR 5.94 dB, SSIM −0.24, MAE 0.43). During encryption, WEBP achieved the fastest processing time (0.48 ms), followed by PNG (1.01 ms) and JPG (15.39 ms), while PNG demonstrated the highest size efficiency with a reduction of up to 70.6%. Decryption remained highly reliable, with success rates exceeding 97% across all formats. Overall, the results confirm that integrating CNNs and rolling hash significantly enhances ElGamal key generation security without compromising decryption reliability or image quality.

Keywords : *Convolutional Neural Network, Digital Image Security, ElGamal Encryption, Key Generation, Rolling Hash.*

1. PENDAHULUAN

Di era pertukaran data visual yang makin massif mulai dari dokumen identitas, rekam medis, CCTV, hingga arsip akademik citra digital sudah jadi aset sensitif**,** bukan sekadar file gambar. Masalahnya, citra punya karakter unik pada ukurannya besar, redundansinya tinggi, dan pola pikselnya sering membentuk struktur yang mudah ditebak. Ini bikin citra rentan terhadap intersepsi, manipulasi, dan serangan berbasis pola [1].

Kemudian pertukaran citra digital (dokumen identitas, rekam medis, arsip akademik, hingga bukti forensik) juga semakin intens dan menuntut mekanisme pengamanan yang bukan hanya kuat di level algoritma, tetapi juga aman pada aspek paling rentan yaitu pada pembangkitan dan manajemen kunci. Pada sistem enkripsi kunci publik seperti ElGamal, keamanan teoritis yang bertumpu pada kesulitan discrete logarithm problem dapat terdegradasi secara drastis ketika proses pembangkitan kunci bergantung pada sumber entropi yang lemah, deterministik, atau mudah direplikasi. Karena itu, peningkatan keamanan ElGamal dalam konteks enkripsi citra tidak cukup berhenti pada implementasi

Vol. 7, No. 3, June 2026, Page. 2465-2479
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484

algoritma, melainkan harus menguatkan algoritma terkhusus pada key generation yang benar-benar sulit diprediksi [2], [3].

Algoritma ElGamal dikenal kuat secara teori karena bertumpu pada kesulitan discrete logarithm problem. Namun, kekuatan kriptografi publik seperti ElGamal tetap bisa "bocor" jika kunci yang dipakai lemah, mudah ditebak, atau memiliki pola. Di sistem nyata, kelemahannya sering bukan di algoritmanya, melainkan di pipeline key generation: sumber entropi yang buruk, proses pembangkitan yang deterministik tanpa mixing yang memadai, atau kunci yang terlalu statis sehingga memperbesar risiko serangan berulang dan analisis statistic [4], [5], [6].

Namun, citra digital memiliki struktur statistik yang khas redundansi tinggi dan korelasi antar piksel yang sering kali menjadi celah bagi serangan berbasis pola. Kemudian karakteristik ini juga membuka peluang untuk representasi citra dapat diekstraksi menjadi fitur yang lebih padat dan informatif melalui Convolutional Neural Network (CNN) [7], [8], [9]. Output pada layer fully connected dapat dipandang sebagai ringkasan fitur yang sensitif terhadap konten citra dan berpotensi menjadi nilai awal pembentukan kunci. Agar nilai tidak menyisakan pola yang bisa dieksploitasi, penelitian ini mengusulkan penguatan melalui rolling hash sebagai mekanisme difusi cepat terhadap perubahan lokal fitur, sehingga perbedaan kecil pada input dapat menghasilkan perubahan signifikan pada keluaran[10].

Penelitian ini mengusulkan suatu skema keamanan dengan mempertimbangkan bahwa meskipun algoritma enkripsi ElGamal secara teoritis memiliki tingkat keamanan yang tinggi, proses pembangkitan kunci masih berpotensi menghasilkan pola yang dapat diprediksi dan rentan terhadap serangan tertentu. Untuk mengatasi permasalahan tersebut, penelitian ini memanfaatkan Convolutional Neural Network (CNN) sebagai metode ekstraksi fitur citra melalui tahapan convolutional layer, activation function (ReLU), pooling layer, dan fully connected layer. Selanjutnya, keluaran dari fully connected layer diproses menggunakan fungsi rolling hash guna meningkatkan variasi dan keacakan nilai piksel citra, sehingga proses pembangkitan kunci ElGamal menjadi lebih adaptif serta memiliki ketahanan yang lebih baik terhadap analisis pola dan serangan kriptografi.

Melalui mekanisme pengacakan pada fitur yang dihasilkan CNN, citra sumber menjadi sulit untuk ditelusuri kembali secara langsung, sementara proses pembangkitan kunci mampu menghasilkan variasi nilai piksel secara acak yang berdampak signifikan terhadap perubahan kunci. Selain itu, fungsi hash bergulir (rolling hash) digunakan untuk mengonversi keluaran fully connected layer ke dalam bentuk nilai integer yang efisien sebagai input kunci pada algoritma ElGamal. Dengan sifat sensitivitas tinggi terhadap perubahan input, perubahan kecil pada bagian tertentu citra dapat menggeser kontribusi hash secara signifikan dan menghasilkan perbedaan besar pada kunci yang dibentuk. Integrasi CNN sebagai pengekstraksi fitur dan rolling hash sebagai mekanisme difusi kunci memungkinkan pembentukan kunci ElGamal yang lebih acak, meningkatkan sensitivitas terhadap perubahan data, serta memperluas ruang kunci secara praktis dalam konteks keamanan system.

Kombinasi keduanya membentuk skema hibrida CNN untuk ekstraksi fitur, rolling hash untuk pengacakan terstruktur, lalu diintegrasikan menjadi key generation bagi ElGamal [11], [12], [13], [14].

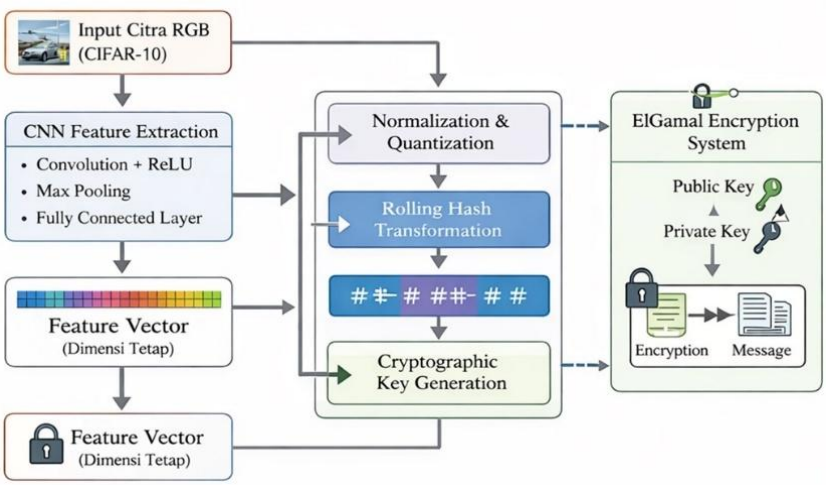
2. METODOLOGI PENELITIAN

Pada skema ElGamal konvensional dapat dilihat pada skema distribusi kunci publik yang dihasilkan dari proses CNN yaitu dari Output Fully Connected, kemudian melalui tahapan fully connected selanjutnya dilakukan melalui kanal distribusi public key, tetapi proses pembangkitan kunci terhubung dengan karakteristik citra atau fitur CNN, yang telah dijelaskan pada gambar 1.

Gambar 1. Menjelaskan CNN mengekstraksi fitur citra, di mana lapisan fully connected berperan menggabungkan seluruh fitur lokal menjadi feature vector berdimensi tetap sebagai representasi global citra. Feature vector ini kemudian dinormalisasi dan ditransformasikan menggunakan rolling hash untuk menghasilkan nilai hash yang sensitif terhadap perubahan fitur. Nilai hash tersebut digunakan sebagai

Vol. 7, No. 3, June 2026, Page. 2465-2479
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484

dasar pembangkitan kunci pada algoritma ElGamal, sehingga kunci kriptografi yang dihasilkan bergantung langsung pada karakteristik citra CIFAR-10 [15].



Gambar 1. Diagram Alir Sistem Pembangkitan Kunci Kriptografi Berbasis Ekstraksi Fitur CNN Dan Transformasi Rolling Hash Untuk Skema Enkripsi Elgamal

2.1. Dataset dan Bahan Penelitan

Pada penelitian ini dilakukan pengujian dengan perangkat komputasi dan perangkat lunak yang sudah disesuaikan, sehingga proses deep learning (CNN) dan komputasi kriptografi (ElGamal) cenderung berjalan lebih stabil, dan integrasi alur kerja dari input citra, ekstraksi fitur, Pembangkit kunci dan proses enkripsi serta proses dekripsi, berikut spesifikasi alat dan bahan penelitian dapat di lihat pada tabel 1.

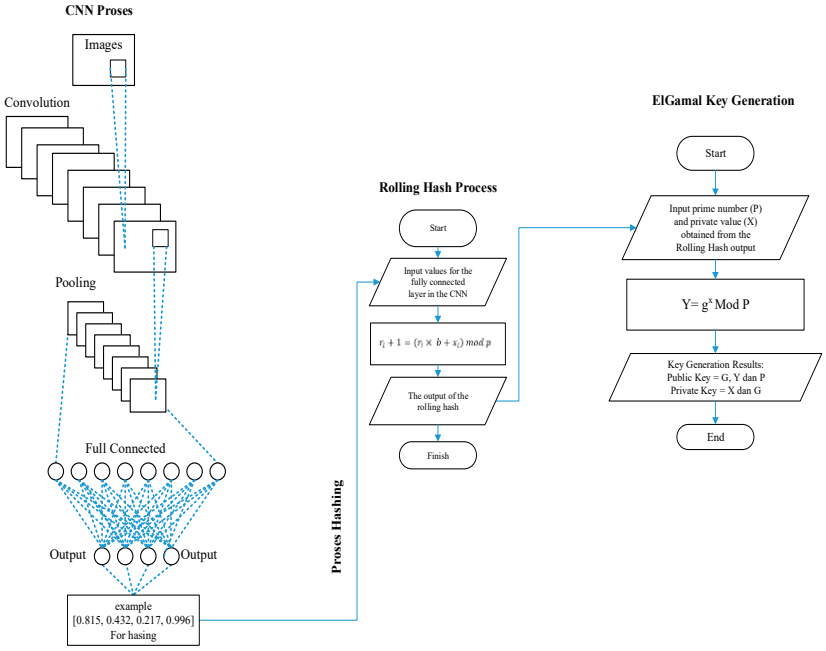
Tabel 1. Alat dan Bahan Penelitian

No	Alat/Bahan	Spesifikasi/Keterangan	Spesifikasi/Keterangan
1	Laptop	Core i7, RAM 16GB, GPU RTX 3060	Memungkinkan proses deep learning dan kriptografi berjalan secara efisien dan stabil tanpa bottleneck komputasi.
2	GUI Python	Versi 3.11	Digunakan sebagai antarmuka sistem untuk mengintegrasikan seluruh modul penelitian
3	PyTorch	Deep Learning Framework	PyTorch dipilih karena mendukung komputasi berbasis GPU, fleksibel dalam pengembangan arsitektur jaringan.
4	Dataset CIFAR-10	Dataset citra untuk eksperimen	Menggunakan jumlah dataset sebanyak 10.000 ribu, dataset dipilih karena memiliki variasi visual yang cukup kompleks untuk menguji ketahanan sistem pembangkitan kunci berbasis citra terhadap perubahan pola spasial.

2.2. Arsitektur Sistem yang Diusulkan (Pipeline)

Desain ini menerapakan proses pembangkit kunci yang didapatkan dari CNN hasil dari fully connected layer, kemudian dilakukan proses rolling hash hasil yang selanjutnya digunakan untuk membentuk pembangkit kunci secara acak pada proses enkripsi citra dengan ElGamal, dapat dilihat pada gambar 2.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 7, No. 3, June 2026, Page. 2465-2479
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484



Gambar 2. Desain *Key Generation System*

Pada gambar 2. Citra lebih dulu diproses dengan menggunakan CNN untuk mengambil fitur (output fully connected), kemudian fitur tersebut dilakukan konversi dengan *rolling hash* menjadi nilai yang stabil dan ringkas, dan angka ini dipakai sebagai Pembangkit kunci untuk membentuk parameter ElGamal (p, q dan x), kemudian sistem menghitung $y = g^x \ mod \ p$ membentuk public key, dan proses enkripsi ElGamal tetap berjalan seperti biasa menghasilkan cipher image (c1, c2).

Berikut mekanisme arsitektur penelitian yang di usulkan:

1. Menakisme CNN

Citra RGB terlebih dahulu diproses oleh CNN. Lapisan convolution dan pooling mengekstraksi pola visual penting, kemudian lapisan fully connected menggabungkan seluruh fitur menjadi feature vector berdimensi tetap. Feature vector ini merepresentasikan karakteristik global citra dan menjadi data masukan untuk proses hashing.

Pada skema kerja arsitektur CNN seperti pada gambar, fitur citra biasanya diekstraksi secara manual atau menggunakan metode sederhana berbasis statistic tekstur, sehingga representasi citra kurang kaya, kurang robust terhadap perubahan pencahayaan/posisi, dan sering gagal menangkap pola spasial yang kompleks, dapat dilihat pada gambar skema kerja CNN [11], [16], [17], [18].

2. Mekanisme Rolling Hash

Nilai dari feature vector hasil fully connected diproses secara berurutan menggunakan fungsi rolling hash. Setiap elemen fitur dimasukkan ke rumus rolling hash sehingga menghasilkan nilai hash akhir. Mekanisme ini memastikan bahwa perubahan kecil pada fitur CNN akan menghasilkan perubahan signifikan pada nilai hash.

3. Mekanisme Pembangkit Kunci ElGamal

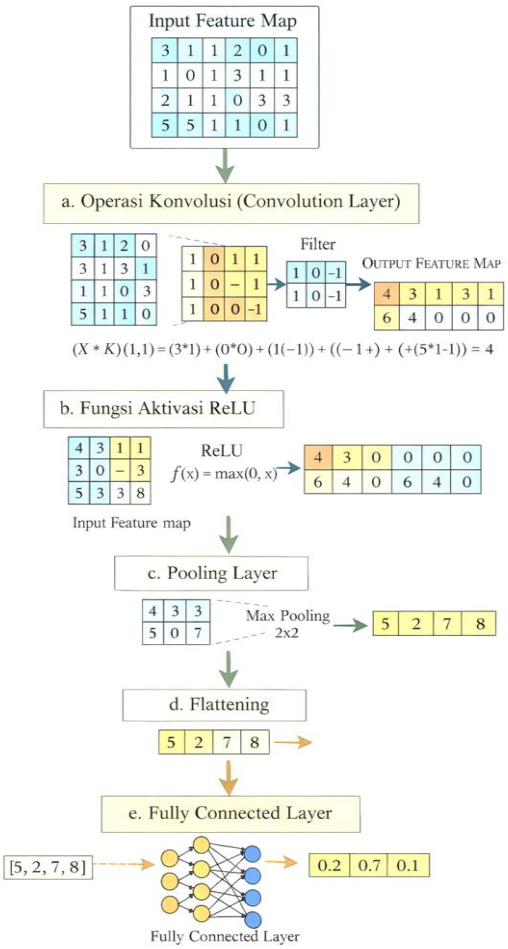
Nilai hash yang dihasilkan digunakan sebagai dasar pembangkitan kunci ElGamal. Dari nilai tersebut ditentukan private key (x), kemudian public key (Y) dihitung menggunakan persamaan ElGamal. Dengan demikian, pasangan kunci yang dihasilkan bergantung langsung pada fitur citra

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 7, No. 3, June 2026, Page. 2465-2479
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484

2.3. Skema CNN Sebagai Ekstraksi Fitur

Pada CNN mempunyai fungsi sebagai arsitektur pemrosesan citra dan klasifikasi. CNN terdiri dari dua tahap utama: ekstraksi fitur (*feature extraction*) dan klasifikasi (*classification*) [19], [20].

Diagram CNN terdiri dari beberapa jenis layer sebagai esktraksi fitur dapat dilihat pada gambar 3.



Gambar 3. Diagram Kerja CNN

Gambar 3. Menunjukan alur kerja CNN dalam mengekstraksi fitur citra, proses dimulai dari konvolusi untuk menghasilkan peta fitur, dilanjutkan dengan aktivasi ReLU untuk menghilangkan nilai negative, kemudian dilakukan max pooling untuk mereduksi ukuran data, kemudian hasilnya diubah menjadi vektor melalui flattening dan diproses pada fully connected layer untuk menghasilkan keluaran akhir [21], [22].

Proses Operasi konvolusi adalah inti dari CNN, dimana dimulai input citra I dan filter K, maka output pada posisi (i,j) dihitung dengan:

$$O(i,j) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \mathrm{I}(i+m, j+n).K\,(m,n) \quad (1)$$

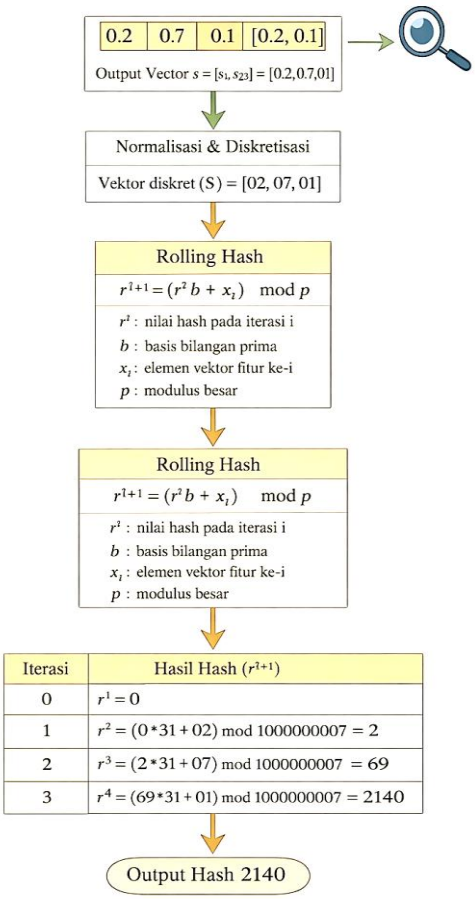
Keterangan:

- I (¡ , j) : nilai piksel input
- $K\,(m,n)$: nilai kernel/filter
- $O(i,j)$: nilai output setelah konvolusi

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 7, No. 3, June 2026, Page. 2465-2479
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484

2.4. Rolling Hash untuk Difusi Fitur

Rolling hash adalah teknik fungsi hash yang memungkinkan nilai hash suatu jendela (substring) diperbarui dalam waktu O(1) ketika jendela digeser satu karakter, sehingga sangat efisien untuk pemrosesan aliran data Panjang, sebagai proses tahapan rolling hash dapat dilihat pada gambar 4.



Gambar 4. Tahapan rolling hash

Gambar 4. Menjelaskan tahapan rolling hash dari hasil fully connected yang selanjutnya di hashingkan kedalam nilai integer.

Proses Inisialisasi dimulai dari $r_0 = 0$, lalu untuk setiap karakter lakukan pembaruan berikut:

$$r\hat{}\{i+1\} = (r_i * b + x_i) \, mod \, p \qquad (2)$$

imana:

r_i : nilai hash sementara

x_i : elemen input

p : modulus (biasanya bilangan prima)

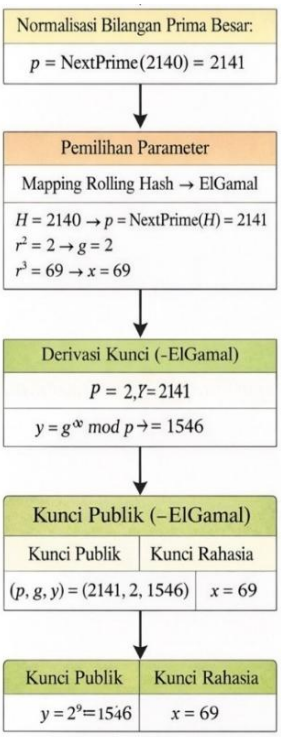
b : basis (base) yaitu faktor pengali yang menentukan "posisi bobot" setiap digit/elemen input.

2.5 Algoritma ElGamal

ElGamal adalah algoritma kriptografi asimetris berbasis pada kesulitan logaritma diskret. ElGamal menyediakan keamanan melalui dua bagian *cipher image* (C1) dan (C2), dan digunakan secara luas dalam skema keamanan berbasis citra. Meskipun memiliki efisiensi rendah dalam ukuran data besar seperti citra, integrasi dengan sistem chaos atau kurva eliptik dapat mengatasi kekurangannya [23], [24], [25].

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 7, No. 3, June 2026, Page. 2465-2479
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484

Algoritma ElGamal adalah skema kriptografi asimetris yang didasarkan pada kesulitan masalah logaritma diskret dalam grup bilangan prima. Proses enkripsi dimulai dengan memilih bilangan prima besar {p}, elemen dasar {g}, dan kunci privat {x}[26], [25], [27].



Gambar 5. Tahapan Pembangkit Kunci Algoritma Elgamal

Algoritma ElGamal memiliki keunggulan utama dari sisi keamanan karena didasarkan pada permasalahan logaritma diskrit pada bilangan prima besar, yang hingga saat ini masih sulit dipecahkan secara komputasional [28].

Proses enkripsi dan dekripsi memanfaatkan operasi eksponensial modular dengan bilangan besar sehingga meningkatkan ketahanan terhadap serangan kriptanalisis. Namun, karakteristik tersebut menyebabkan cipher image yang dihasilkan terdiri dari dua komponen, sehingga ukurannya menjadi dua kali lebih besar dibandingkan citra awal.

Berikut merupakan kreteria pembangkit kunci pada algoritma Elgamal:

1. P: Bilangan prima (tidak rahasia)
2. G: Bilangan acak (tidak rahasia)
3. X: Bilangan acak (rahasia)
4. Y: Kunci public (tidak rahasia)
5. K: Kunci bebas (tidak rahasia)

Kunci publik terdiri dari (p,g,y) dengan Persamaan:

$$y = g\text{^}x \ mod \ p \quad (3)$$

Untuk mengenkripsi pesan m, pengirim memilih bilangan acak k dengan persamaan:

$$c1 = g^k mod \ p \quad (4)$$

$$c2 = m \cdot y\text{^}k \ mod \ p \quad (5)$$

Vol. 7, No. 3, June 2026, Page. 2465-2479
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484

Kemudian ciphertext yang dikirim adalah pasangan $(c1, c2)$. Penerima, dengan kunci privat x, dapat mendekripsi pesan dengan menghitung menggunakan Persamaan:

$$m = bi \cdot ai^{p-1-x} \; mod \; p \qquad (6)$$

Keamanan algoritma ini bergantung pada kesulitan menghitung logaritma diskret, yang membuatnya tahan terhadap serangan *brute-force*.

3. HASIL

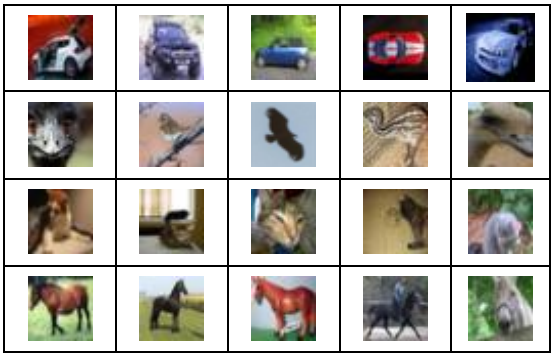
Pengujian penelitian ini membahas hasil pengujian terhadap sistem yang diusulkan berdasarkan skenario dan data uji yang telah ditentukan. Hasil pengujian digunakan untuk mengevaluasi kinerja, keakuratan, dan tingkat keamanan metode yang diterapkan secara objektif dan terukur

3.1 Hasil Pengujian Data

Sampel pengujian data digunakan sebagai representasi data uji dalam proses evaluasi sistem. Data ini mencakup seluruh komponen yang terlibat dalam proses pengamanan, mulai dari pembangkitan kunci hingga proses enkripsi dan dekripsi, sehingga hasil pengujian dapat menggambarkan performa sistem secara menyeluruh

3.1.1 Data Pembangkit Kunci

Data pembangkit kunci yang digunakan adalah citra CIFAR-10 untuk menghasilkan kunci kriptografi yang berperan sebagai elemen utama dalam proses enkripsi dan dekripsi. Pengujian pada tahap ini bertujuan memastikan kunci yang dihasilkan memenuhi kebutuhan keamanan system, berikut data citra CIFAR-10 sebagai pengujian pembangkit kunci, dengan berbagai warna pixel dan dengan nilai pixel yang berbeda-beda. Dibawah ini merupakan data citra cifar-10 yang digunakan untuk proses pembangkit kunci dari CNN dilihat pada gambar 5.



Gambar 5. Citra CIFAR-10 Sebagai Pembangkit Kunci

3.1.2 Data Citra (Target Keamanan)

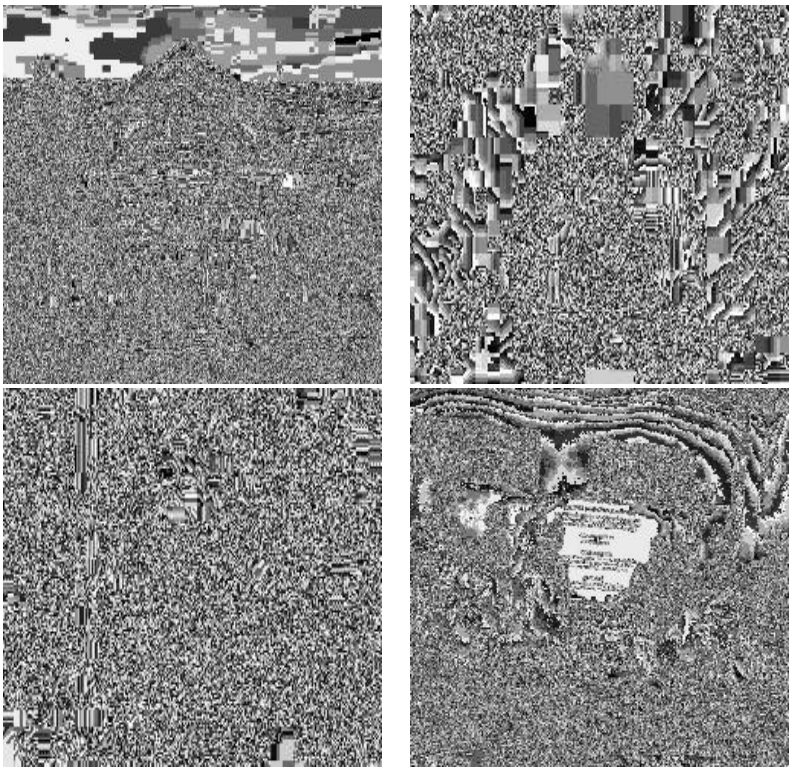
Data citra berfungsi sebagai objek yang diamankan dalam pengujian. Citra ini digunakan untuk mengevaluasi efektivitas metode pengamanan terhadap data visual digital. Berikut citra awal sebagai target dalam proses pengamanan dapat dilihat pada gambar 6.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 7, No. 3, June 2026, Page. 2465-2479
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484

Gambar 6. Data Citra Target

3.1.3 Data Enkripsi

Data enkripsi merupakan hasil transformasi citra asli ke bentuk data yang tidak dapat dikenali. Tahap ini digunakan untuk menilai kemampuan algoritma dalam menyamarkan informasi, data cipher image citra yang sudah di enkripsi dan diamankan dapat dilihat pada gambar 7.



Gambar 7. Data Citra Rahasia

3.1.4 Data Dekripsi

Data dekripsi adalah hasil pemulihan data terenkripsi menjadi citra asli. Pengujian dilakukan untuk memastikan akurasi dan keandalan sistem dalam mengembalikan data tanpa kehilangan informasi. Data dekripsi citra yang sudah kembali keawal dapat dilihat pada gambar 8.

Gambar 8. Data Citra Awal

Jurnal Teknik Informatika (JUTIF) Vol. 7, No. 3, June 2026, Page. 2465-2479
P-ISSN: 2723-3863 https://jutif.if.unsoed.ac.id
E-ISSN: 2723-3871 DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484

3.2 Pengujian Keamanan Citra Berdasarkan Kinerja Waktu

Hasil Pengujian disediakan untuk memastikan bahwa proses enkripsi dan dekripsi yang diimplementasikan pada aplikasi berjalan benar, konsisten, dan terukur**.** Melalui proses pengujian, pengguna dapat melihat hasil proses pembangkit kunci, proses enkripsi dan proses dekripsi berdasarkan serangkaian uji coba pada beberapa citra dengan variasi ukuran dan karakteristik piksel. Hasil pengujian tidak hanya digunakan untuk menunjukkan bahwa cipher image berbeda dari citra asli, tetapi juga untuk membuktikan bahwa citra hasil dekripsi dapat kembali mendekati citra awal dengan tingkat kesalahan yang minimal, hasil pengujian pembangkit kunci dapat di lihat pada tabel 1.

Tabel 1. Pengujian Pembangkit Kunci

No	Tipe Gambar	Data Latih	Data Uji	Epoch	Durasi Proses (ms)	PNSR (dB)	SSIM	MAE	Status Pembangkit Kunci
1	CIFAR-10	10000	5000	10	0.430	5.938832	-0.24197269	0.43089618	Berhasil
2	CIFAR-10	10000	5000	20	0.444	5.938832	-0.24197269	0.43089618	Berhasil
3	CIFAR-10	10000	5000	30	0.426	5.938832	-0.24197269	0.43089618	Berhasil

Tabel 1. Menjelaskan hasil pengujian pembangkit kunci menggunakan dataset CIFAR-10 dengan variasi parameter pelatihan (jumlah epoch). Parameter yang diuji mencakup jumlah data latih dan uji, epoch, serta kecepatan rata-rata pembangkitan kunci, disertai metrik kualitas (PSNR, SSIM, MAE) untuk menggambarkan stabilitas output terhadap perubahan konfigurasi pengujian.

Setelah proses pengujian pembangkit kunci pada citra selesai, selanjutnya dilakukan proses pengujian entropi untuk mendapatkan pembangkit kunci pada citra, dapat dilihat pada tabel 2.

Tabel 2. Pengujian Entropi Pembangkit Kunci

No	Tipe Gambar	Data Latih	Panjang Kunci	Entropy	Status
1	CIFAR-10	10000	128 bit	7.95	Berhasil
2	CIFAR-10	10000	128 bit	7.96	Berhasil
3	CIFAR-10	10000	128 bit	7.94	Berhasil

Setelah proses pengujian entropi pembangkit kunci pada citra selesai, selanjutnya dilakukan pengujian enkripsi pada citra, hasil pengujian dapat dilihat pada tabel 3.

Tabel 3. Data Pengujian Proses Enkripsi

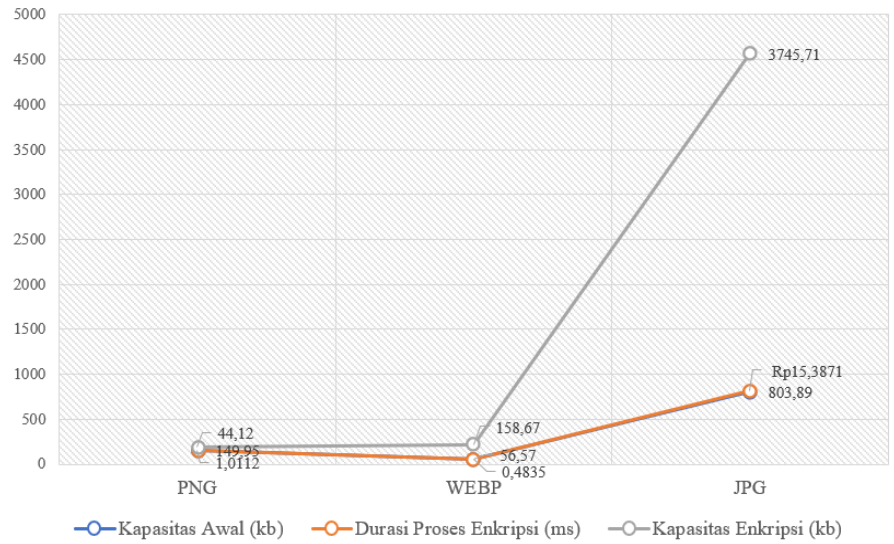
No	Tipe Gambar	Kapasitas awal (kb)	Durasi Proses (ms)	Kapasitas Enkripsi (kb)	Status Enkripsi
1	.PNG	149.95	1.0112	44.12	Berhasil
2	.WEBP	56.57	0.4835	158.67	Berhasil
3	.JPG	803.89	15.3871	3745.71	Berhasil

Tabel 2. Tabel ini menunjukkan hasil pengujian menunjukkan bahwa format WEBP memiliki waktu enkripsi tercepat (0.4835 ms), namun ukuran hasil enkripsi meningkat signifikan, sedangkan PNG menunjukkan waktu enkripsi relatif cepat (1.0112 ms) dengan ukuran hasil enkripsi yang justru

Vol. 7, No. 3, June 2026, Page. 2465-2479
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484

menurun, mengindikasikan adanya efek kompresi. Sebaliknya, JPG memiliki waktu enkripsi paling lambat (15.3871 ms) dengan peningkatan ukuran keluaran yang sangat besar, sehingga menghasilkan beban komputasi dan kebutuhan kapasitas tertinggi, khususnya pada citra berukuran besar, meskipun seluruh format menunjukkan status enkripsi yang berhasil.

Dibawah ini merupakan hasil enkripsi yang menjelaskan dalam bentuk grafik data pengujian pada proses enkripsi citra, dapat dilihat pada gambar 9.



Gambar 9. Grafik Data Pengujian Proses Enkripsi

Gambar 8. Menjelaskan data pengujian enkripsi membandingkan tiga format citra, yaitu PNG, WEBP, dan JPG, berdasarkan ukuran awal, waktu enkripsi, dan ukuran hasil enkripsi. Hasil menunjukkan bahwa WEBP memiliki waktu enkripsi tercepat (0.4835 ms) namun ukuran hasil enkripsi meningkat, PNG membutuhkan waktu sedikit lebih lama (1.0112 ms) dengan ukuran hasil enkripsi yang menurun, sedangkan JPG memiliki ukuran awal terbesar, waktu enkripsi paling lama (15.3871 ms), dan peningkatan ukuran hasil enkripsi yang sangat signifikan. Seluruh proses enkripsi pada penelitian ini berhasil, dan pengujian dilanjutkan dengan proses pengembalian cipher image, hasil pengujian dapat dilihat pada tabel 3.

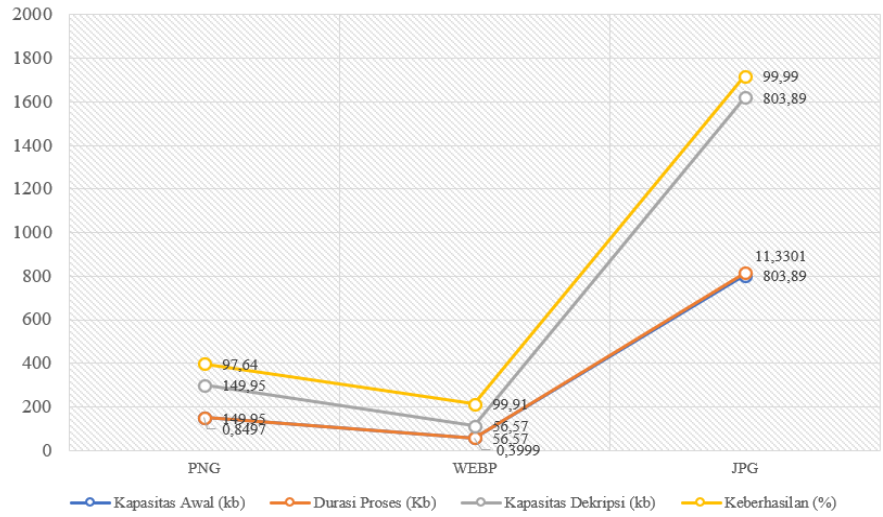
Tabel 3. Data Pengujian Proses Dekripsi

No	Tipe Gambar	Kapasitas awal (Kb)	Durasi Proses (ms)	Kapasitas Dekripsi (kb)	Tingkat Keberhasilan keamanan proses dekripsi	Status Dekripsi
1	.PNG	149.95	0.8497	149.95	97.64%	Berhasil
2	.WEBP	56.57	0.3999	56.57	99.91%	Berhasil
3	.JPG	803.89	11.3301	803.89	99.99%	Berhasil

Tabel 3. Menjelaskan bahwa hasil pengujian dekripsi menunjukkan bahwa format WEBP memiliki durasi dekripsi tercepat (0.3999 ms) dengan ukuran hasil yang identik dengan citra awal serta tingkat keberhasilan 99.91%, PNG memerlukan waktu dekripsi 0.8497 ms dengan tingkat keberhasilan 97.64%, sedangkan JPG memiliki durasi dekripsi paling lama (11.3301 ms) namun menunjukkan tingkat keberhasilan tertinggi sebesar 99.99%. Seluruh format citra berhasil didekripsi dengan ukuran keluaran yang sama dengan citra asli.

Dibawah ini merupakan hasil dekripsi yang menjelaskan dalam bentuk grafik data pengujian pada proses enkripsi citra, dapat dilihat pada gambar 10.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 7, No. 3, June 2026, Page. 2465-2479
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484



Gambar 10. Grafik Data Pengujian Proses Dekripsi

Gambar 9. Menjelaskan Data Pengujian Proses Dekripsi diatas menampilkan perbandingan tiga format citra (PNG, WEBP, JPG) berdasarkan kapasitas awal (KB), durasi dekripsi (ms), kapasitas hasil dekripsi (KB), dan tingkat keberhasilan (%). Pada penelitian ini kapasitas dekripsi pada semua format sama dengan kapasitas awal, yang menunjukkan data berhasil dikembalikan ke ukuran semula setelah didekripsi. Dari sisi waktu, WEBP menjadi yang tercepat (0.3999 ms), diikuti PNG (0.8497 ms), sedangkan JPG paling lama (11.3301 ms) karena ukuran datanya paling besar (803.89 KB), sementara mempunyai tingkat keberhasilan dekripsi juga tinggi pada semua format, yaitu 97.64% (PNG), 99.91% (WEBP), dan 99.99% (JPG).

4. PEMBAHASAN

Pada penelitian ini yaitu menginterpretasikan hasil-hasil yang ditemukan pada saat proses pengujian, menghubungkannya dengan tujuan penelitian, serta membandingkannya dengan literatur yang digunakan untuk penelitian.

4.1 Interpretasi kinerja tinggi dan efisiensi

Kinerja sistem menunjukkan bahwa format dengan ukuran data lebih kecil cenderung diproses lebih cepat, sedangkan data yang lebih besar membutuhkan waktu lebih lama. Pada enkripsi citra .WEBP menjadi yang tercepat (0.4835 ms), disusul PNG (1.0112 ms), sementara JPG paling lambat (15.3871 ms). Dari sisi efisiensi ukuran hasil enkripsi, PNG paling efisien karena ukuran turun dari 149.95 KB menjadi 44.12 KB, sedangkan WEBP mengalami overhead dari 56.57 KB menjadi 158.67 KB, dan JPG meningkat sangat besar dari 803.89 KB menjadi 3.745.71 KB. Dari ringkasan diatas kinerja tinggi tidak hanya dilihat dari waktu proses, tetapi juga dari kemampuan menekan overhead ukuran hasil enkripsi.

4.2 Peningkatan keamanan

Indikator keamanan terlihat dari keberhasilan pemulihan data pada tahap dekripsi, karena seluruh format menunjukkan ukuran hasil dekripsi kembali sama dengan ukuran awal dan berstatus Berhasil. Tingkat keberhasilan dekripsi juga tinggi, yaitu 97.64% (PNG), 99.91% (WEBP), dan 99.99% (JPG). Pada penelitian ini mengindikasikan proses enkripsi mampu menjaga kerahasiaan data, sementara dekripsi mampu mengembalikan data secara konsisten dan akurat, sehingga sistem memiliki reliabilitas keamanan yang baik pada berbagai format citra.

4.3 Analisis dan Diskusi Kinerja Keamanan Sistem

Pada penelitian ini menunjukan bahwa Metode pembangkitan kunci dan enkripsi citra yang diusulkan terbukti memiliki kinerja yang baik dari sisi efisiensi waktu, akurasi dekripsi, entropi, dan keamanan sistem. Pengujian menunjukkan proses enkripsi dan dekripsi berjalan efisien, citra hasil dekripsi dapat dipulihkan mendekati citra asli dengan kesalahan rendah, serta kunci yang dihasilkan memiliki tingkat keacakan tinggi dan stabil. Dibandingkan dengan metode berbasis pseudo-random number generator (PRNG), pendekatan berbasis CNN menghasilkan kunci yang lebih kompleks dan sulit diprediksi melalui pemanfaatan fitur non-linear citra. Oleh karena itu, metode ini berpotensi diterapkan pada sistem keamanan citra digital dengan kebutuhan perlindungan tinggi, meskipun memerlukan sumber daya komputasi yang lebih besar.

5. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa model pembangkitan kunci berbasis Convolutional Neural Network (CNN) yang dikombinasikan dengan iterasi rolling hash berhasil diterapkan secara efektif pada algoritma ElGamal, adapun kesimpulan penelitian ini dapat dirangkum sebagai berikut:

1. Integrasi CNN dan rolling hash efektif memperkuat pembangkitan kunci ElGamal dengan menghasilkan kunci berentropi tinggi, sensitif terhadap karakteristik visual citra, dan sulit diprediksi, sehingga relevan untuk pengamanan citra sensitif seperti citra medis, biometrik, dan sistem identitas digital.
2. Sistem enkripsi dan ekripsi menunjukkan reliabilitas tinggi, ditandai dengan tingkat keberhasilan dekripsi di atas 97% dan kemampuan memulihkan citra secara identik, yang menegaskan bahwa peningkatan keamanan tidak mengorbankan akurasi dan integritas data pada aplikasi dunia nyata.
3. Kinerja sistem dipengaruhi oleh format citra, di mana WEBP unggul dalam kecepatan, PNG lebih efisien dari sisi ukuran, dan JPG aman namun kurang optimal untuk citra besar. Oleh karena itu, pemilihan format citra menjadi faktor penting dalam implementasi sistem keamanan citra berbasis ElGamal.

6. SARAN

Berdasarkan hasil penelitian dan keterbatasan yang masih terdapat dalam sistem yang diusulkan, beberapa saran untuk pengembangan penelitian selanjutnya adalah sebagai berikut:

1. Pengujian pada dunia nyata perlu diperluas pada citra sensitif (medis, biometrik, identitas digital, dan forensik) untuk mengevaluasi keandalan sistem dalam menjaga keamanan dan integritas data.
2. Dataset yang lebih besar dan beragam diperlukan untuk menilai skalabilitas sistem serta memastikan pembangkitan kunci berbasis CNN dan rolling hash tetap memiliki entropi dan keacakan yang tinggi
3. Pengembangan arsitektur CNN yang lebih efisien direkomendasikan guna meningkatkan kualitas ekstraksi fitur, keamanan kunci, dan efisiensi komputasi pada berbagai platform.

KONFILK KEPENTINGAN

Kami seluruh penulis menyatakan bahwa tidak ada konflik kepentingan dalam melakukan penelitian maupun pada objek penelitian ini

UCAPAN TERIMAKASIH

Kami ucapkan terimakasih kepada teman-teman yang mendukung pada penelitian ini, terutama saya ucapkan kepada bapak/ibu promotor dan co-promotor saya yang selalu membimbing dan pengarahkan dalam penulisan penelitian ini.

Vol. 7, No. 3, June 2026, Page. 2465-2479
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484

DAFTAR PUSTAKA

[1] C. Wu, Y. Ding, A. Yan, T. C. Poon, and P. W. M. Tsang, "Asymmetric Optical Scanning Holography Encryption with Elgamal Algorithm," *Photonics*, vol. 11, no. 9, 2024, doi: 10.3390/photonics11090878.

[2] E. A. Adeniyi, P. B. Falola, M. S. Maashi, M. Aljebreen, and S. Bharany, "Secure Sensitive Data Sharing Using RSA and ElGamal Cryptographic Algorithms with Hash Functions," *Inf.*, vol. 13, no. 10, pp. 1–14, 2022, doi: 10.3390/info13100442.

[3] Maxrizal and S. Irawadi, "Nonsingular matrix as private key on ElGamal cryptosystem," *J. Phys. Conf. Ser.*, vol. 1821, no. 1, 2021, doi: 10.1088/1742-6596/1821.

[4] C. Annamalai, C. Vijayakumaran, V. Ponnusamy, and H. Kim, "Optimal ElGamal Encryption with Hybrid Deep-Learning-Based Classification on Secure Internet of Things Environment," *Sensors*, vol. 23, no. 12, pp. 1–15, 2023, doi: 10.3390/s23125596.

[5] M. Kumar, A. S. Chivukula, and G. Barua, "Deep learning-based encryption scheme for medical images using DCGAN and virtual planet domain," *Sci. Reports 2025 151*, vol. 15, no. 1, pp. 1–42, Jan. 2025, doi: 10.1038/s41598-024-84186-6.

[6] M. Al Kahfi, M. Auva, D. P. Putra, C. D. P. B. Ginting, and A. Fauzi, "Super Text Data Encryption: Combination of Affine Cipher, Elgamal, and RSA Algorithms for Optimal Protection," *J. Sist. Inf. Kaputama*, vol. 9, no. 1, pp. 20–34, Jan. 2025, doi: 10.59697/JSIK.V9I1.949.

[7] F. Fahry, T. C. Miswaty, and H. Harun, "Analyzing Marketplace Reviews Using Word2Vec, CNN, and Deep K-Means with Sociolinguistic Approaches," *J. Tek. Inform.*, vol. 6, no. 6, pp. 5489–5502, Dec. 2025, doi: 10.52436/1.JUTIF.2025.6.6.5340.

[8] M. J. Mubarok, R. F. Haya, E. Fitria, and B. S. Budi, "Detection of Endangered Indonesian Species Across Multiple Taxonomic Classes Using Faster R-CNN," *J. Tek. Inform.*, vol. 6, no. 6, pp. 5435–5449, Dec. 2025, doi: 10.52436/1.JUTIF.2025.6.6.4793.

[9] I. B. K. Widiartha, A. Y. Husodo, T. T. T. Thuy, and S. I. Murpratiwi, "Incremental CNN-k-NN Hybrid Facial Recognition for Helmeted Facial Recognition in IoT-Enabled Smart Parking: A Case Study at Universitas Mataram," *J. Tek. Inform.*, vol. 6, no. 6, pp. 5539–5552, Dec. 2025, doi: 10.52436/1.JUTIF.2025.6.6.5447.

[10] N. G. Rezk, S. Alshathri, A. Sayed, E. E. D. Hemdan, and H. El-Behery, "Secure Hybrid Deep Learning for MRI-Based Brain Tumor Detection in Smart Medical IoT Systems," *Diagnostics*, vol. 15, no. 5, p. 639, Mar. 2025, doi: 10.3390.

[11] A. Fauzi, S. Ramadani, H. Khair, and A. M. H. Pardede, "Integration Of Data Filtering With Hybrid RSA Deep Learning Algorithm For Iot Data Security And Classification.," *J. Theor. Appl. Inf. Technol.*, vol. 103, no. 22, 2025.

[12] T. Gizachew Yirga, H. Gizachew Yirga, and E. G. Addisu, "Cryptographic key generation using deep learning with biometric face and finger vein data," *Front. Artif. Intell.*, vol. 8, p. 1545946, Apr. 2025, doi: 10.3389/FRAI.2025.1545946.

[13] A. N. A. Saputra, R. E. Saputro, and D. I. S. Saputra, "Labeling Optimization and Hybrid CNN Model in Sentiment Analysis of Movie Reviews with Slang Handling," *J. Tek. Inform.*, vol. 6, no. 6, pp. 5333–5348, Dec. 2025, doi: 10.52436/1.JUTIF.2025.6.6.4465.

[14] Y. E. Karabacak, "Deep learning-based CNC milling tool wear stage estimation with multi-signal analysis," *Eksploat. i Niezawodn.*, vol. 25, no. 3, pp. 0–2, 2023, doi: 10.17531/ein/168082.

[15] C. Jiang and G. Goldsztein, "Convolutional Neural Network Approach to Classifying the CIFAR-10 Dataset," *J. Student Res.*, vol. 12, no. 2, pp. 1–7, May 2023, doi: 10.47611/jsrhs.v12i2.4388.

[16] N. Widaad and D. Anggraini, "Sentiment Analysis Of ChatGPT APP User Reviews Using SVM

Vol. 7, No. 3, June 2026, Page. 2465-2479
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.4484

And CNN Methods," *J. Tek. Inform.*, vol. 5, no. 6, pp. 1687–1700, Dec. 2024, doi: 10.52436/1.JUTIF.2024.5.6.4010.

[17] A. M. Huda, G. F. Shidik, and V. Praskatama, "Comparative Analysis Of LSTM, BILSTM, GRU, CNN, And RNN For Depression Detection In Social Media," *J. Tek. Inform.*, vol. 5, no. 6, pp. 1723–1735, Dec. 2024, doi: 10.52436/1.JUTIF.2024.5.6.4060.

[18] S. Y. Riska and A. Noercholis, "Performance Comparison Of Faster R-Convolutional Neural Network (CNN) And Efficientnet For Train Detection Under Diverse Lighting And Image Quality Conditions," *J. Tek. Inform.*, vol. 5, no. 6, pp. 1811–1821, Dec. 2024, doi: 10.52436/1.JUTIF.2024.5.6.3438.

[19] H. Fransiska and A. Azhari STMIK Kalirejo, "Application of Transformer-Based Deep Learning for Early Detection of Cyberattacks on IoT-Based Critical Infrastructure," *RIGGS J. Artif. Intell. Digit. Bus.*, vol. 4, no. 2, pp. 3818–3825, Jun. 2025, doi: DOI:10.31004/riggs.v4i2.1118.

[20] C.-Y. Chang, C.-F. Yang, C.-C. Chang, P.-T. Wu, and Y.-M. Ooi, "Evaluation of Impact of Convolutional Neural Network-Based Feature Extractors on Deep Reinforcement Learning for Autonomous Driving," *Eng. Proc. 2025, Vol. 120, Page 27*, vol. 120, no. 1, p. 27, Feb. 2026, doi: 10.3390/engproc2025120027.

[21] Y. Wang, T. Lan, Q. Ye, D. Sheng, Z. Bao, and R. Song, "Series Arc Fault Detection Method Based on TDDA-CNN Prototype Learning Model," *Electron. 2026, Vol. 15, Page 681*, vol. 15, no. 3, p. 681, Feb. 2026, doi: 10.3390/electronics15030681.

[22] O. ' Shaughnessy, E. Tabane, E. Mnkandla, and Z. Wang, "Ensemble Deep Learning Models for Multi-Class DNA Sequence Classification: A Comparative Study of CNN, BiLSTM, and GRU Architectures," *Appl. Sci. 2026, Vol. 16, Page 1545*, vol. 16, no. 3, p. 1545, Feb. 2026, doi: 10.3390/app16031545.

[23] M. Alawida, "A novel chaos-based permutation for image encryption," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 6, Jun. 2023, doi: 10.1016/j.jksuci.2023.101595.

[24] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019, doi: 10.1109/ACCESS.2019.2906052.

[25] Y. Qin and B. Zhang, "Privacy-Preserving Biometrics Image Encryption and Digital Signature Technique Using Arnold and ElGamal," *Appl. Sci. 2023, Vol. 13, Page 8117*, vol. 13, no. 14, p. 8117, Jul. 2023, doi: 10.3390/APP13148117.

[26] B. Harjito, T. Setyawati, and A. Wijayanto, "Comparative Analysis between Elgamal and NTRU Algorithms and their implementation of Digital Signature for Electronic Certificate," *Int. J. Electr. Comput. Eng. Syst.*, vol. 13, no. 9, pp. 729–739, 2022, doi: doi.org/10.32985/ijeces1391.

[27] D. R. and I. P. S. M. A. Budiman, "A tutorial on using ElGamal cryptosystem and RC4-P1 cipher in a hybrid scheme A tutorial on using ElGamal cryptosystem and RC4-P1 cipher in a hybrid scheme," 2023, doi: 10.1088/1742-6596/2421/1/012033.

[28] R. Imanda *et al.*, "Development Of Hybrid Encryption Method Using Affine Cipher, Vigenere Cipher, And Elgamal Algorithm To Secure Text Messages In Data Communication System," *J. Artif. Intell. Eng. Appl.*, vol. 2, no. 2, pp. 30–40, Feb. 2023, doi: 10.59934/JAIEA.V2I2.154.