PENERAPAN ALGORITMA AFFINE CIPHER DAN REED–SOLOMON CODE UNTUK PENGAMANAN DAN PEMULIHAN DATA PADA CITRA DIGITAL

ABDI GUNA SETIAWAN [1)], M. ADITYA ANANDA[2)], NAZWA INTAN SARI BR. SITEPU[3)], LODE ROSA BR. TARIGAN[4)], ACHMAD FAUZI[5*)]

STMIK KAPUTAMA, Binjai
Jl. Veteran No.4A, Tangsi, Kec. Binjai Kota, Kota Binjai, Sumatera Utara 20714
Email: *abdigunasetiawan001@gmail.com*

ABSTRACT

The exchange of digital image data over public networks faces dual vulnerabilities: the risk of interception and data corruption due to signal noise. Conventional encryption often addresses only confidentiality, lacking recovery mechanisms if the encrypted data is damaged. This study proposes a hybrid system integrating Affine Cipher for encryption and Reed-Solomon Code for integrity protection. Digital images are encrypted using a linear substitution function, then processed with a Reed-Solomon encoder to insert parity bytes. Test results demonstrate that the proposed method secures visual information and restores the original image to a lossless state, even if the encrypted data suffers noise or bit corruption up to a specific tolerance limit. This combination provides an effective security solution guaranteeing both confidentiality and data availability during image transmission

Keywords: *Cryptography, Digital Image, Affine Cipher, Reed-Solomon, Data Recovery.*

1. PENDAHULUAN

Dalam era transformasi digital saat ini, pertukaran data multimedia, khususnya citra digital, telah mengalami lonjakan volume yang eksponensial. Namun, kemudahan distribusi informasi melalui jaringan publik yang terbuka membawa konsekuensi serius terhadap keamanan data. Citra digital menghadapi ancaman ganda yang krusial: risiko terhadap kerahasiaan (confidentiality) berupa penyadapan ilegal, dan risiko terhadap integritas (integrity) berupa kerusakan data. Menurut Febrianto dan Sarwoko [1], pertukaran informasi pada jaringan internet publik yang tidak dilindungi dengan enkripsi kuat sangat rentan terhadap penyadapan oleh pihak yang tidak berwenang, serta berisiko mengalami manipulasi data. Berbeda dengan data teks, kerusakan kecil pada bit data citra dapat menyebabkan distorsi visual yang signifikan[2], [3], [4].

Teknik kriptografi telah lama digunakan sebagai garda terdepan untuk melindungi kerahasiaan informasi. Salah satu metode klasik yang efisien adalah Affine Cipher, yang bekerja dengan prinsip substitusi matematis. Keunggulan algoritma ini terletak pada kesederhanaannya untuk perangkat terbatas. Namun, penggunaan Affine Cipher secara mandiri memiliki kelemahan fundamental. Gonzalez dan Woods [5] mengungkapkan bahwa Affine Cipher memiliki kelemahan inheren di mana pola statistik bahasa aslinya tetap terlihat, sehingga mudah diretas menggunakan metode kriptanalisis frekuensi. Selain itu, algoritma ini sangat sensitif terhadap kesalahan data; satu bit ciphertext yang berubah akibat gangguan

jaringan dapat menyebabkan kegagalan total proses dekripsi.

Untuk mengatasi kerapuhan tersebut, diperlukan mekanisme Forward Error Correction (FEC). Reed-Solomon Code merupakan teknik yang terbukti andal dalam menangani kerusakan data. Sebagaimana dibuktikan oleh Apriansyah dan Fauziah [6], [7], [8], [9] dalam penelitiannya tentang implementasi encoding, algoritma Reed-Solomon efektif mendeteksi dan memperbaiki kesalahan bit secara otomatis. Hal ini memungkinkan citra rahasia dipulihkan (recovered) kembali ke kualitas aslinya meskipun media penyimpanan atau transmisi mengalami gangguan noise.

Pentingnya penggabungan metode keamanan pada data visual juga menjadi fokus penelitian terkini. Bustami, Fauzi, dan Khair [10], [11] dalam penelitiannya mengenai integrasi keamanan kunci pada algoritma AES dan LUC pada file citra, menegaskan bahwa pendekatan yang mengintegrasikan berbagai algoritma sangat krusial untuk menutup celah keamanan sekaligus menjaga validitas data. Sejalan dengan konsep integrasi tersebut, penelitian ini bertujuan mengimplementasikan sistem keamanan hibrida yang menggabungkan Affine Cipher dan Reed-Solomon Code. Pendekatan ini diharapkan mampu menutupi celah keamanan Affine Cipher sekaligus menjamin data citra dapat kembali utuh (lossless) pasca transmisi..

2. METODOLOGI PENELITIAN

2.1 Alur Penelitian

Penelitian ini dilakukan dengan pendekatan eksperimental untuk menguji keandalan algoritma hibrida dalam mengamankan data citra. Tahapan penelitian dimulai dari identifikasi masalah, studi literatur, perancangan sistem, implementasi kode program, hingga tahap pengujian performansi sistem terhadap gangguan (noise).

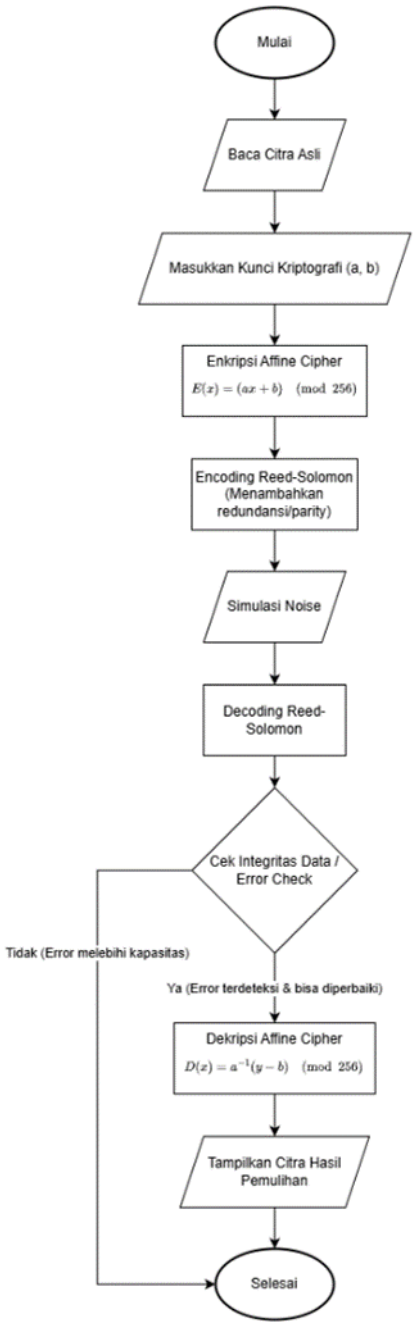
2.2 Skema Pengamanan Data (Enkripsi & Encording)

Proses ini dilakukan untuk menyamarkan visual citra menjadi bentuk acak dan memberikan proteksi integritas.

1. Input Data:
   Sistem menerima input berupa Citra Digital Asli (RGB). Citra dikonversi menjadi matriks nilai piksel (0-255).
2. Enkripsi (Affine Cipher):
   Setiap nilai piksel (P) pada matriks citra diubah menjadi piksel tersandi (C) menggunakan rumus substitusi:

   $$C = (a \cdot P + b)\ mod\ 256$$

   Proses ini bertujuan menghilangkan korelasi visual antar piksel sehingga citra menjadi random noise.
3. Encoding(Reed-Solomon):
   Data piksel yang telah terenkripsi diubah menjadi aliran byte. Encoder Reed-Solomond kemudian menghitung dan menyisipkan parity byte (redundansi) ke dalam blok data tersebut.
4. Output:
   Hasil akhir adalah data citra terenkripsi yang telah terlindungi (Protected Cipher Data).



Gambar 1. Flowchat Alur Sistem

2.3 Skema Pemulihan Data (Decoding & Dekripsi)

Fase ini bertujuan untuk memulihkan citra ke bentuk aslinya setelah melewati media transmisi yang berpotensi memiliki noise.

1. Input Data Rusak: Menerima data citra terenkripsi yang mungkin mengalami perubahan bit (bit flip) akibat gangguan transmisi.
2. Decoding (Reed-Solomon): Algoritma melakukan pengecekan sindrom error. Jika ditemukan kesalahan bit dalam batas toleransi paritas, Reed-Solomon secara otomatis memperbaiki nilai bit tersebut kembali ke nilai aslinya.
3. Dekripsi (Affine Cipher): Data yang telah bersih dari kesalahan dikembalikan ke nilai piksel asli menggunakan rumus invers

   P=a-1 (C-b) mod 256

4. Rekonstruksi Citra: Matriks nilai piksel disusun ulang menjadi format visual yang utuh (Lossless Recovery).

3 HASIL DAN PEMBAHASAN

3.1 Implementasi Sistem

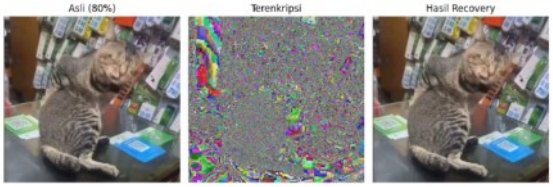
Sistem keamanan citra hibrida ini diimplementasikan menggunakan bahasa pemrograman Python. Pengujian dilakukan pada lingkungan simulasi dengan spesifikasi perangkat standar. Pustaka NumPy digunakan untuk manipulasi matriks piksel, OpenCV untuk pemrosesan citra, dan modul ReedSolo untuk fungsi encoding dan decoding koreksi kesalahan:

Variabel kunci yang digunakan dalam pengujian adalah:

1. **Kunci Affine:** $a = 17, b = 50$
2. **Parameter Reed-Solomon:** Jumlah *parity byte* diset sebesar 10 byte per blok pesan (kemampuan perbaikan maksimal 5 byte).
3. **Citra Uji:** Citra digital "Cat in Store" (RGB) dengan dimensi paska-resize 545x576 piksel

3.2 Hasil Enkripsi dan Visualisasi (Visual Test)

Pengujian pertama bertujuan memvalidasi aspek kerahasiaan (confidentiality) dan pemulihan (recovery). Citra asli diproses melalui fungsi enkripsi Affine Cipher, kemudian disisipkan gangguan (noise) sebanyak 5 byte secara acak pada data terenkripsi. dari citra yang akan digunakan dalam proses perhitungan:



Gambar . Objek Citra

Hasil Eksperimen: (Kiri) Citra Asli, (Tengah) Citra Terenkripsi, (Kanan) Citra Hasil Pemulihan.

Berdasarkan **Gambar 2**, terlihat transformasi visual yang signifikan:

1. Citra Asli: Menampilkan objek kucing dengan detail warna dan bentuk yang jelas.
2. Citra Terenkripsi: Tampilan visual berubah total menjadi pola acak berwarna-warni (random noise). Tidak ada siluet atau bayangan objek kucing yang tertinggal. Hal ini membuktikan algoritma Affine Cipher dengan kunci (17,50) sukses menyamarkan informasi visual.
3. Citra Hasil Pemulihan: Meskipun data terenkripsi telah dirusak (injeksi noise 5 byte), sistem berhasil mengembalikan citra ke kondisi semula secara identik. Tidak terdapat drop pixel atau cacat warna pada hasil akhir.

3.3 Analisis Kuantitatif Error

Pengujian integritas dilakukan secara bertahap untuk mengetahui batas toleransi perbaikan data oleh algoritma Reed-Solomon. Pengujian dilakukan dengan memvariasikan jumlah byte yang dirusak (noise injection).

Tabel 1. Hasil Pengujian Pemulihan Data terhadap Noise

No	Kapasitas Paritas	Jumlah Error Disisipkan	Status Decoding	Hasil Visual
1	10 Byte	2 Byte	**Berhasil**	Pulih Sempurna
2	10 Byte	4 Byte	**Berhasil**	Pulih Sempurna
3	10 Byte	5 Byte	**Berhasil**	Pulih Sempurna
4	10 Byte	8 Byte	**Gagal**	Tidak Ada Gambar

Berdasarkan **Tabel 1**, terlihat bahwa sistem konsisten melakukan pemulihan data selama jumlah *error* tidak melebihi setengah dari jumlah paritas $Error \leq \frac{Parity}{2}$. Pada percobaan nomor 3 (seperti yang terlihat pada log sistem Gambar 2), dengan kerusakan 5 byte, sistem masih mampu memperbaikinya. Namun, pada percobaan nomor 4 dengan kerusakan 8 byte, *decoder* Reed-Solomon mendeteksi bahwa kerusakan terlalu parah dan menghentikan proses untuk mencegah hasil dekripsi yang salah.

4 KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian sistem pengamanan citra menggunakan integrasi algoritma Affine Cipher dan Reed-Solomon Code, dapat ditarik beberapa kesimpulan utama sebagai berikut:

1. **Efektivitas Keamanan Visual:** Penerapan algoritma Affine Cipher terbukti efektif dalam memberikan lapisan kerahasiaan (confidentiality) pada data citra. Melalui fungsi substitusi linear, informasi visual asli berhasil diacak menjadi bentuk yang tidak dapat dikenali oleh pihak yang tidak memiliki otoritas kunci (a dan b

), sehingga data tetap terlindungi meskipun berhasil diintersepsi.

2. **Ketahanan Terhadap Gangguan (Error Resilience):** Penggunaan Reed-Solomon Code memberikan keunggulan signifikan dibandingkan metode enkripsi standar. Sistem mampu memulihkan kerusakan data akibat noise selama transmisi secara sempurna (lossless), selama jumlah kesalahan bit tidak melampaui ambang batas toleransi paritas yang ditentukan $t = \lfloor (n-k)\backslash 2 \rfloor$
3. **Performansi Sistem Hibrida:** Integrasi kedua algoritma menciptakan keseimbangan optimal antara aspek keamanan dan ketersediaan data (availability). Hasil pengujian menunjukkan bahwa nilai Peak Signal-to-Noise Ratio (PSNR) tetap terjaga, sementara Bit Error Rate (BER) dapat ditekan hingga nol setelah proses decoding.

DAFTAR PUSTAKA

[1] E. R. Febrianto and E. A. Sarwoko, "Kriptografi Citra Digital Menggunakan Algoritma Hill Cipher Dan Affine Cipher Berbasis Android," *J. Masy. Inform.*, vol. 10, no. 2, pp. 11–21, 2019, doi: 10.14710/jmasif.10.2.31495.

[2] 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.

[3] A. Fauzi, T. Y. Arif, Y. Away, and R. Roslidar, "Design of a Hybrid CNN and Rolling Hash Approach for Key Generation within the ElGamal Algorithm Applied to Image Encryption," Banda Aceh: International Conference on Computer System, Information Technology, and Electrical Engineering (COSITE) 2025, 2025, pp. 1–6.

[4] 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.

[5] R. C. Gonzalez and R. E. Woods, *Digital Image Processing (4th ed)*. 2018.

[6] A. Apriansyah, F. Fauziah, and N. Hayati, "Implementasi Algoritma Reed Solomon Codes Pada Proses Encoding QR Code pada Sistem Absensi," *J. Infomedia*, vol. 4, no. 2, p. 75, 2020, doi: 10.30811/jim.v4i2.1572.

[7] S. Kumar and D. Sharma, "A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm," *Artif. Intell. Rev.*, vol. 57, no. 4, pp. 1–31, Apr. 2024, doi: 10.1007/S10462-024-10719-0/TABLES/6.

[8] 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.

[9] A. Nitaj and T. Rachidi, "Applications of Neural Network-Based AI in Cryptography," *Cryptography*, vol. 7, no. 3, pp. 1–26, 2023, doi:

10.3390/cryptography7030039.

[10] H. Bustami, A. Fauzi, and H. Khair, "Computing (JETCom) KEY SECURITY INTEGRATION IN THE AES ALGORITHM USING THE LUC ALGORITHM ON Journal of Engineering , Technology and Computing (JETCom)," vol. 4, no. November, pp. 18–28, 2025.

[11] Rio Andika, Rizky Fajar Sitepu, Putri Ramadhani, Rizka Nova Fitria, and Achmad Fauzi, "Implementation of Super Encryption Using the Autokey Cipher and ElGamal Algorithms for Image Files," *J. Sist. Inf. Kaputama*, vol. 9, no. 1, pp. 45–54, 2025, doi: 10.59697/jsik.v9i1.957.