Journal of Engineering, Technology and Computing (JETCom) E-ISSN: 2828-0512
Volume 4, Nomor 3, November 2025

KEY SECURITY INTEGRATION IN THE AES ALGORITHM USING THE LUC ALGORITHM ON IMAGE FILES

[1]Harya Bustami*, [2]Achmad Fauzi, [3]Husnul Khair

[1,]Sistem Informasi , STMIK Kaputama
[2,]Teknik Informatika, STMIK Kaputama
[3,]Teknik Informatika, STMIK Kaputama
Komplek sanggar lingk IX Stabat Kab Langkat, Sumatera Utara

e-mail :[1] haryabustami95@email.com, [2] fauzyrivai88@email.com, [3] husnul.khair@email.com

Received: 2025-08-22
Revised: 2025-09-30
Accepted: 2025-10-30

Page : 18-28

Abstrak : Perkembangan teknologi informasi menuntut adanya sistem pengamanan data yang andal, khususnya pada file citra yang bersifat sensitif. Advanced Encryption Standard (AES) merupakan algoritma simetris yang cepat dan efisien, namun kelemahannya terletak pada distribusi kunci yang rawan disalahgunakan. Untuk mengatasi permasalahan tersebut, penelitian ini mengintegrasikan algoritma Lucas (LUC) sebagai pengaman kunci AES. LUC dipilih karena sifatnya sebagai algoritma asimetris yang menggunakan pasangan kunci publik dan privat, sehingga mampu melindungi kerahasiaan kunci enkripsi AES. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan file citra dengan memanfaatkan integrasi AES dan LUC menggunakan bahasa pemrograman Python serta penyimpanan kunci dalam format teks. Proses enkripsi dilakukan pada file citra berformat JPG dan PNG dengan ukuran maksimal 3 MB, sementara hasil enkripsi maupun dekripsi diuji melalui serangkaian percobaan. Hasil penelitian menunjukkan bahwa sistem berhasil mengenkripsi dan mendekripsi file citra dengan baik, serta mampu menjaga kerahasiaan kunci AES melalui pengamanan menggunakan LUC. Integrasi kedua algoritma ini terbukti meningkatkan keamanan data, sehingga dapat dijadikan rujukan dalam pengembangan sistem keamanan file digital di masa depan.

Kata kunci: AES, File Citra, Integrasi, Keamanan Kunci, LUC

Abstract : *The rapid growth of information technology requires a reliable data security system, especially for sensitive image files. The*

Journal of Engineering, Technology and Computing (JETCom) E-ISSN: 2828-0512
Volume 4, Nomor 3, November 2025

Advanced Encryption Standard (AES) is a symmetric algorithm that is fast and efficient; however, its main weakness lies in the vulnerability of key distribution. To address this issue, this research integrates the Lucas (LUC) algorithm to secure AES keys. LUC was chosen as it is an asymmetric algorithm utilizing public and private key pairs, ensuring the confidentiality of AES encryption keys. The purpose of this study is to design and implement an image file security system by integrating AES and LUC using Python programming language with key storage in text format. The encryption process was applied to JPG and PNG files with a maximum size of 3 MB, and the encrypted as well as decrypted results were tested through several experiments. The results indicate that the system successfully encrypted and decrypted image files while maintaining AES key confidentiality through LUC protection. The integration of these two algorithms enhances data security and can serve as a reference for the development of secure digital file systems in the future.

Keywords: *AES, Image File, Integration, Key Security, LUC*

DOI: https://doi.org/10.63893/jetcom.v4i3.315

1 Pendahuluan (or Introduction)

Perkembangan teknologi informasi di era digital telah mendorong transformasi besar dalam penyimpanan, pengelolaan, dan pertukaran data, termasuk file citra. File citra kini memegang peranan penting dalam berbagai aspek, baik dalam komunikasi, arsip digital, maupun sistem keamanan berbasis visual. Namun, meningkatnya penggunaan file citra juga membawa ancaman baru berupa risiko pencurian, manipulasi, dan penyalahgunaan oleh pihak yang tidak berwenang. Kondisi ini menegaskan urgensi adanya sistem keamanan yang mampu memberikan perlindungan menyeluruh, bukan hanya pada data citra itu sendiri, tetapi juga pada kunci enkripsi yang digunakan.

Salah satu metode enkripsi yang banyak digunakan adalah Advanced Encryption Standard (AES). Algoritma ini dikenal cepat dan efisien, namun kelemahannya terletak pada pengelolaan kunci. AES memiliki tiga variasi panjang kunci yaitu 128 bit, 192 bit, dan 256 bit, yang masing-masing menentukan jumlah ronde dalam proses enkripsi dan dekripsi, yakni 10, 12, dan 14 ronde. Setiap ronde terdiri dari serangkaian transformasi utama seperti substitusi byte, pergeseran baris, transformasi kolom, dan penambahan kunci ronde. Ukuran blok data dalam AES bersifat tetap, yaitu 128 bit yang direpresentasikan dalam bentuk matriks berukuran 4×4 byte. Algoritma AES mengadopsi struktur dasar dari Rijndael cipher dan ditetapkan sebagai standar enkripsi oleh pemerintah Amerika Serikat karena menawarkan tingkat keamanan dan efisiensi tinggi. Penyesuaian panjang kunci ini turut memengaruhi kompleksitas transformasi dan ketahanan algoritma terhadap berbagai bentuk serangan kriptografi [1]. Distribusi kunci yang kurang aman dapat membuka peluang

bagi pihak tidak berwenang untuk membobol file citra, bahkan setelah dienkripsi. Hal inilah yang menimbulkan permasalahan pokok dalam penelitian ini, yaitu bagaimana merancang mekanisme yang tidak hanya mengandalkan enkripsi simetris AES, tetapi juga memperkuat keamanan kunci enkripsinya.

Sebagai solusi, penelitian ini merasionalisasikan penggunaan pendekatan kriptografi hybrid, yaitu mengintegrasikan AES dengan algoritma asimetris Lucas (LUC). Algoritma kriptografi LUC merupakan sistem kriptografi kunci publik yang diperkenalkan oleh Peter J. Smith dan Michael J.J. Lennon pada tahun 1993. Algoritma ini terdiri dari tiga tahap utama, yaitu pembangkitan kunci, proses enkripsi, dan proses dekripsi. Seluruh operasinya dilakukan dalam domain bilangan, sehingga pesan atau teks yang akan dienkripsi harus terlebih dahulu dikonversi ke dalam bentuk bilangan. Hasil enkripsi pun berupa bilangan yang menyandikan pesan asli. Selain itu, kunci dekripsi dalam algoritma LUC bergantung pada kunci enkripsi dan bilangan prima yang digunakan dalam proses pembangkit kunci. Uniknya, satu kunci enkripsi pada LUC dapat memiliki empat kemungkinan pasangan kunci dekripsi. Dengan menggabungkan keunggulan kecepatan AES dan keamanan distribusi kunci LUC, diharapkan sistem yang dirancang mampu memberikan perlindungan yang lebih komprehensif pada file citra. Kriptografi merupakan salah satu cabang ilmu dalam bidang keamanan informasi yang berperan penting dalam melindungi data melalui proses transformasi simbolik. Proses ini dilakukan dengan cara mengubah data asli atau pesan yang dapat dibaca (plaintext) menjadi bentuk tidak bermakna (ciphertext), yang kemudian hanya dapat dikembalikan ke bentuk semula oleh pihak yang memiliki otorisasi tertentu. Kriptografi berfungsi sebagai metode untuk menyamarkan informasi agar tidak dapat dipahami oleh pihak yang tidak berwenang, namun tetap dapat dikembalikan menjadi data yang utuh oleh penerima yang sah. Transformasi ini melibatkan dua proses utama, yaitu enkripsi sebagai metode pengamanan dan dekripsi sebagai sarana pemulihan data ke bentuk aslinya. Dengan demikian, kriptografi tidak hanya menjaga kerahasiaan data, tetapi juga memastikan keasliannya serta mempertahankan integritasnya [2].

Tujuan utama penelitian ini adalah untuk merancang sistem enkripsi file citra dengan mengintegrasikan algoritma AES dan algoritma LUC, lalu untuk menerapkan dan mengimplementasikan algoritma AES dalam proses enkripsi file citra, serta algoritma LUC dalam proses pengamanan kunci AES. Penelitian ini memiliki signifikansi yaitu menjadi referensi dalam membangun sistem keamanan file citra dengan memanfaatkan kombinasi algoritma AES dan LUC, menambah literatur dan pengetahuan mengenai integrasi algoritma kriptografi simetris dan asimetris dalam pengamanan file citra, memberikan pemahaman bahwa keamanan data, khususnya file citra, dapat ditingkatkan melalui pengamanan terhadap kunci enkripsinya. Kriptografi simetris merupakan metode enkripsi yang menggunakan satu kunci yang sama dalam proses enkripsi dan dekripsi. Artinya, baik pengirim maupun penerima pesan harus memiliki dan menjaga kerahasiaan kunci yang sama agar informasi dapat diubah dan dibaca kembali ke bentuk semula. Metode ini dinilai efisien dari sisi kecepatan dan cocok untuk pengamanan data berukuran besar, seperti file citra digital atau data transaksi. Namun, kriptografi simetris memiliki kelemahan mendasar dalam hal distribusi kunci. Apabila kunci jatuh ke tangan yang tidak berwenang, maka kerahasiaan seluruh sistem bisa terganggu. Kriptografi simetris menggunakan kunci yang identik untuk kedua proses, sehingga dibutuhkan pengelolaan kunci yang sangat ketat [3]. Kriptografi asimetris adalah metode penyandian data yang menggunakan dua kunci berbeda, yaitu kunci publik dan kunci privat. Kunci publik digunakan untuk mengenkripsi data, sedangkan kunci privat digunakan untuk mendekripsinya. Kedua kunci tersebut saling berkaitan secara matematis namun tidak identik. Metode ini memungkinkan komunikasi yang aman tanpa harus berbagi kunci secara langsung. Kriptografi asimetris efektif

digunakan dalam sistem terbuka yang melibatkan banyak pihak. Keamanan data lebih terjamin karena hanya pihak dengan kunci privat yang dapat mengakses isi pesan. Teknologi ini juga mendukung implementasi autentikasi digital dan integritas data [4].

Selain itu, penelitian ini menegaskan bahwa keamanan data tidak hanya ditentukan oleh algoritma enkripsi yang digunakan, tetapi juga oleh strategi perlindungan kunci enkripsi. Dengan mengintegrasikan AES dan LUC, penelitian ini menawarkan pendekatan baru yang lebih komprehensif dibanding penelitian terdahulu yang sebagian besar hanya berfokus pada data teks.

2 Tinjauan Literatur (or Literature Review)

Penelitian yang relevan dilakukan oleh [5], dengan judul "Performance Analysis The Combination Of Advanced Encryption Standard Cryptography Algorithms With Luc For Text Security" yang menganalisis kombinasi algoritma kriptografi simetris AES dengan algoritma asimetris LUC dalam skema hybrid untuk pengamanan data teks. Dalam penelitian tersebut, algoritma AES digunakan untuk proses enkripsi dan dekripsi pesan, sementara algoritma LUC dimanfaatkan untuk mengenkripsi kunci eksternal AES. Hasil penelitian menunjukkan bahwa kombinasi keduanya dapat meningkatkan tingkat keamanan data, meskipun dari sisi waktu komputasi mengalami peningkatan yang cukup signifikan akibat kompleksitas pemrosesan kunci LUC. Selain itu, simulasi terhadap serangan brute force membuktikan bahwa peningkatan nilai kunci publik pada LUC turut memperpanjang waktu untuk menebak kunci, sehingga secara tidak langsung menambah lapisan keamanan pada sistem hybrid yang dibangun.

Penelitian oleh [6] dengan judul "Pengamanan Data Teks Menggunakan Metode Digital Signature Algorithm (DSA) Dan Advanced Encryption Standard (AES)" juga menunjukkan penerapan kriptografi hybrid dengan menggabungkan algoritma asimetris Digital Signature Algorithm (DSA) dan AES. DSA digunakan untuk memastikan keaslian data, sementara AES bertugas dalam proses enkripsi dan dekripsi. Penelitian ini menekankan bahwa data teks yang telah dienkripsi dapat dikembalikan ke bentuk semula tanpa kehilangan informasi, menunjukkan bahwa kombinasi kriptografi asimetris dan simetris dapat berfungsi secara optimal dari sisi fungsionalitas. Meskipun objek yang digunakan berupa teks, pendekatan metode hybrid ini memberikan dukungan konseptual terhadap penelitian yang menggabungkan LUC dan AES dalam konteks file citra.

Penelitian oleh [7] berjudul "Pengamanan Data dengan Kriptografi Hibrida Algoritma Hill Cipher dan Algoritma LUC serta Steganografi Chaotic LSB" menggabungkan Hill Cipher dan LUC dalam skema hybrid untuk mengenkripsi data, kemudian menyembunyikannya menggunakan metode steganografi. Dalam penelitian ini, algoritma LUC digunakan untuk mengenkripsi kunci dari Hill Cipher, menunjukkan bahwa LUC dapat diterapkan dalam sistem kriptografi hybrid untuk meningkatkan keamanan kunci dan kerahasiaan data.

Penelitian oleh [8] menegaskan bahwa tingkat keamanan pada algoritma kunci simetris sangat bergantung pada kerahasiaan dan pengelolaan kunci yang digunakan dalam sistem.

Dari kajian literatur tersebut, terlihat bahwa sebagian besar penelitian masih berfokus pada penerapan hybrid cryptosystem pada data teks, sedangkan penelitian terkait integrasi LUC dengan AES pada file citra masih sangat terbatas. Padahal, file citra memiliki karakteristik yang berbeda dengan teks, baik dari sisi ukuran data, struktur file, maupun tingkat kerentanannya terhadap serangan. Kekosongan inilah yang menjadi celah penelitian yang perlu diisi.

Oleh karena itu, penelitian ini secara khusus difokuskan pada integrasi algoritma AES dan LUC untuk pengamanan file citra. AES digunakan untuk enkripsi konten citra karena efisiensi dan

kecepatannya, sementara LUC digunakan untuk mengamankan kunci AES agar tidak mudah diakses pihak tidak berwenang. Dengan demikian, penelitian ini tidak hanya melanjutkan tren integrasi kriptografi hybrid, tetapi juga menawarkan kontribusi baru dengan memperluas penerapannya pada file citra digital yang selama ini belum banyak dieksplorasi.

3 Metode Penelitian (or Research Method)

Penelitian ini menggunakan pendekatan eksperimen dengan tujuan merancang dan mengimplementasikan sistem keamanan file citra berbasis integrasi algoritma Advanced Encryption Standard (AES) dan Lucas (LUC). Data yang digunakan berupa file citra berformat PNG dan JPG dengan ukuran maksimal 3 MB. Format Portable Network Graphics (PNG) dikenal sebagai jenis format gambar yang menggunakan kompresi lossless, sehingga tidak mengurangi kualitas gambar meskipun ukuran filenya kecil. Format ini umumnya dipilih untuk penyimpanan gambar berbasis garis, teks, dan ikon karena mampu mempertahankan kejelasan visual tanpa membebani ruang penyimpanan secara signifikan [9]. Pemilihan format ini didasarkan pada karakteristiknya yang umum digunakan dalam pertukaran data digital dan memiliki struktur yang memengaruhi proses enkripsi.

Alat utama yang digunakan dalam penelitian ini adalah perangkat komputer dengan spesifikasi standar untuk pemrograman dan pengolahan citra, serta bahasa pemrograman Python sebagai media implementasi algoritma. Python merupakan bahasa pemrograman berbasis objek yang bersifat interpretatif dan interaktif, serta memiliki struktur data tingkat tinggi yang memungkinkan pengembangan program secara efisien dan mudah dipahami [10]. Beberapa perangkat lunak pendukung seperti Binary Viewer juga digunakan untuk membantu proses konversi file citra ke dalam representasi heksadesimal sebelum dilakukan enkripsi.

Rancangan kegiatan penelitian meliputi beberapa tahap, yaitu: studi literatur untuk memahami konsep dasar kriptografi simetris dan asimetris serta penelitian terdahulu yang relevan, analisis kebutuhan sistem dan batasan penelitian, perancangan sistem dengan pembuatan flowchart, diagram alur, dan desain antarmuka, implementasi algoritma AES untuk enkripsi file citra serta algoritma LUC untuk pengamanan kunci, pengujian sistem untuk memastikan keberhasilan enkripsi dan dekripsi, serta evaluasi hasil guna menilai keandalan sistem yang dibangun.

Ruang lingkup penelitian dibatasi pada proses enkripsi file citra menggunakan algoritma AES-128 dan pengamanan kunci enkripsi AES menggunakan algoritma LUC. Fokus penelitian tidak mencakup pengujian autentikasi pengguna maupun efisiensi waktu komputasi, melainkan diarahkan pada keberhasilan sistem dalam menjaga kerahasiaan file citra serta keamanan kunci enkripsi. Objek penelitian berupa data citra digital yang diproses melalui mekanisme hybrid cryptosystem.

Teknik pengumpulan data dilakukan melalui eksperimen langsung pada file citra yang dienkripsi menggunakan sistem yang dirancang. Hasil enkripsi dan dekripsi dibandingkan untuk menguji keakuratan proses. Selain itu, dilakukan analisis terhadap ciphertext yang dihasilkan guna memastikan bahwa file citra tidak dapat dikenali tanpa kunci dekripsi yang sesuai.

Teknik analisis yang digunakan adalah analisis deskriptif dengan membandingkan hasil proses enkripsi dan dekripsi secara fungsional. Analisis dilakukan untuk memastikan bahwa integrasi algoritma AES–LUC dapat menjaga kerahasiaan data citra sekaligus meningkatkan keamanan distribusi kunci. Hasil pengujian kemudian dievaluasi secara kualitatif untuk menilai sejauh mana sistem yang dibangun mampu menjawab permasalahan keamanan file citra digital.

Journal of Engineering, Technology and Computing (JETCom) E-ISSN: 2828-0512
Volume 4, Nomor 3, November 2025

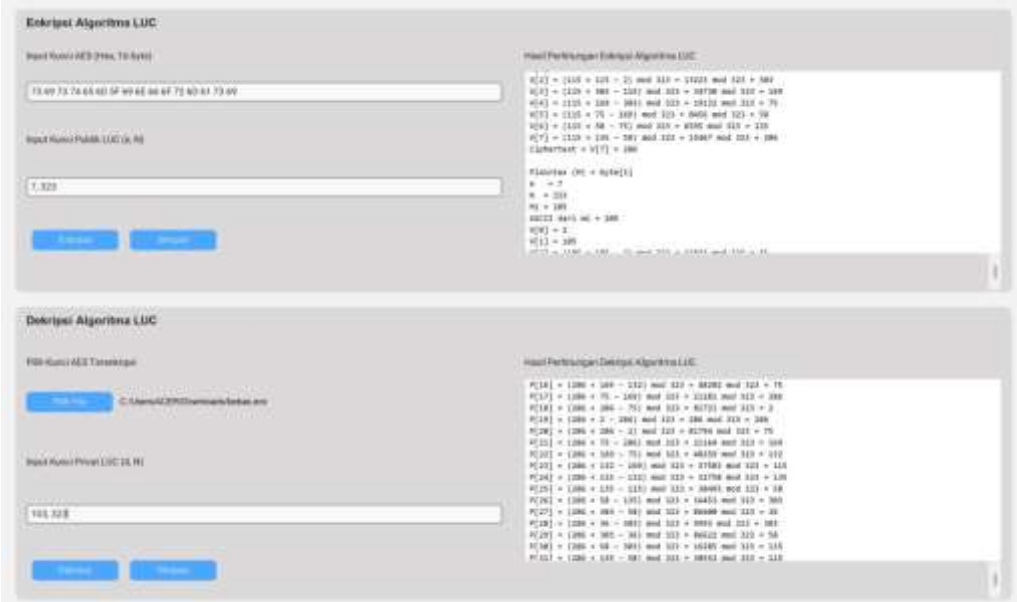
4 Hasil dan Pembahasan (or Results and Analysis)

Berikut ini merupakan tahapan implementasi program yang dilakukan secara menyeluruh, dimulai dari proses awal hingga tahap akhir untuk memastikan bahwa sistem berjalan dengan baik sesuai dengan rancangan. Uji coba ini meliputi tiga tahapan utama, yaitu pengujian proses integrasi AES LUC , pengujian proses enkripsi, dan pengujian proses dekripsi.

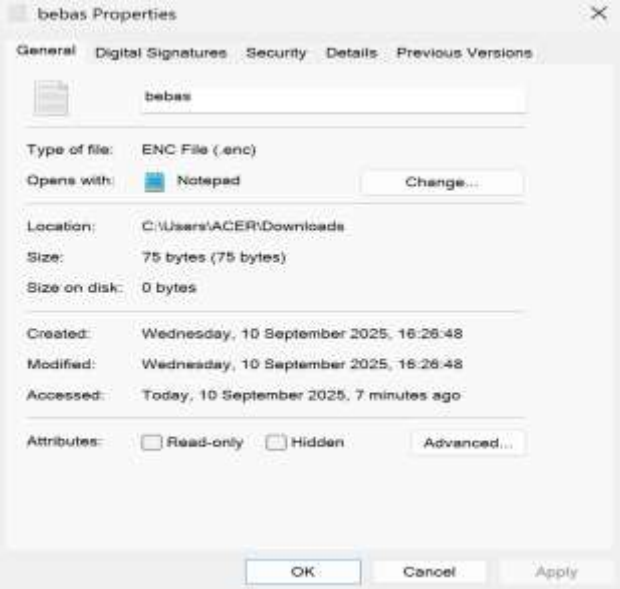
4.1 Proses Integrasi AES LUC

Pengguna terlebih dulu memasukkan string 16 karakter sebagai kunci AES; sistem memvalidasi panjang sesuai standar AES-128 dan menampilkan peringatan jika tidak tepat. Setelah valid, kunci otomatis dikonversi ke heksadesimal dan seluruh hasil ekspansi kunci (key schedule) untuk setiap ronde AES ditampilkan agar proses internal dapat dipantau. Berikutnya, pengguna mengisikan bilangan prima p dan q untuk pembangkitan kunci LUC; sistem menghitung N, φ(N), lalu membentuk pasangan kunci publik dan privat LUC. Kunci AES kemudian dienkripsi dengan LUC sehingga menghasilkan cipherkey dalam bilangan desimal, dan semua keluaran ditayangkan pada area teks. Berdasarkan uji coba, seluruh tahapan— validasi kunci AES, visualisasi key schedule, pembangkitan kunci LUC, serta enkripsi kunci AES—berjalan lancar, sehingga mekanisme pengamanan kunci AES melalui LUC dinyatakan berfungsi dengan baik.

Journal of Engineering, Technology and Computing (JETCom) E-ISSN: 2828-0512
Volume 4, Nomor 3, November 2025



Gambar IV.1 Form Integrasi AES LUC



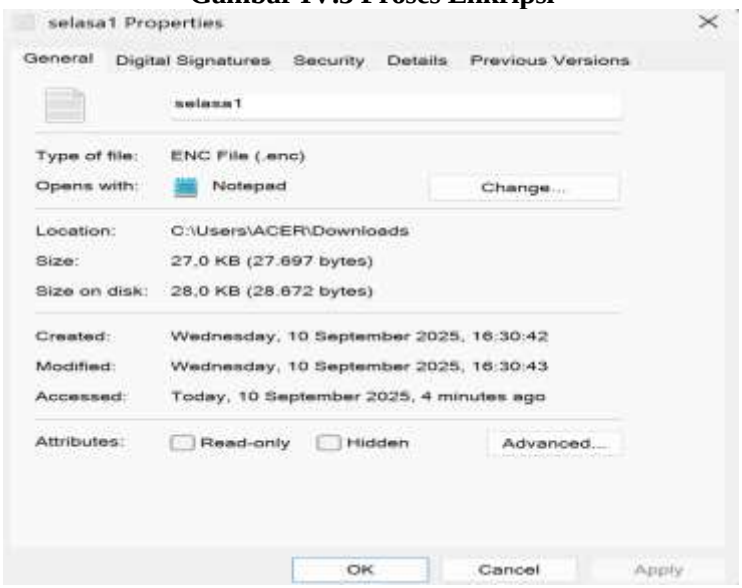
Gambar IV.2 Hasil Integrasi Kunci AES LUC

4.2 Proses Enkripsi

Setelah integrasi AES–LUC tervalidasi, dilakukan pengujian enkripsi file citra. Pada form enkripsi, pengguna memilih berkas PNG/JPG serta cipherkey AES hasil enkripsi LUC (format .enc). Saat tombol Enkripsi dijalankan, sistem memetakan data citra ke blok heksadesimal berukuran 16 byte dan memprosesnya menggunakan algoritma AES. Hasil enkripsi berupa ciphertext ditampilkan pada area teks, dan berkas terenkripsi dapat disimpan untuk pengujian lanjutan. Uji coba

menunjukkan berkas citra hasil enkripsi tidak dapat dibuka maupun dikenali secara visual, sehingga konten asli sepenuhnya tersamarkan. Temuan ini menegaskan bahwa AES efektif mengamankan data citra, dan keamanan diperkuat karena kuncinya terlebih dahulu diamankan oleh algoritma LUC.

Gambar IV.3 Proses Enkripsi



Gambar IV.4 Hasil Enkripsi

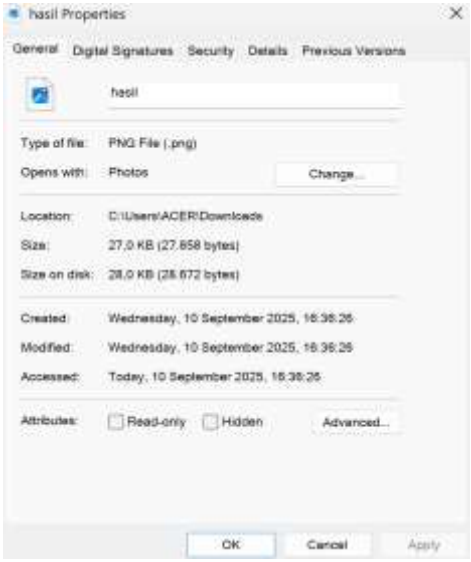
4.3 Proses Dekripsi

Tahap terakhir menguji dekripsi untuk memastikan citra terenkripsi kembali utuh. Pada form dekripsi, pengguna memilih berkas citra terenkripsi dan memasukkan cipherkey AES hasil dekripsi

Journal of Engineering, Technology and Computing (JETCom) E-ISSN: 2828-0512
Volume 4, Nomor 3, November 2025

LUC, lalu menekan Dekripsi. Sistem menampilkan proses perhitungan dan merekonstruksi ciphertext menjadi citra asli tanpa kehilangan data atau perubahan struktur—file dapat dibuka dan tampil dengan kualitas identik sebelum enkripsi. Hasil ini menegaskan AES menjaga integritas data, sementara integrasi dengan LUC memastikan hanya pemilik kunci privat yang valid yang dapat melakukan dekripsi.

Gambar IV.5 Proses Dekripsi



Gambar IV.6 Hasil Dekripsi

Hasil penelitian ini menunjukkan bahwa integrasi AES–LUC dapat meningkatkan keamanan data citra. AES terbukti efektif dalam mengubah citra menjadi bentuk yang tidak dikenali, sedangkan LUC berfungsi optimal dalam melindungi distribusi kunci. Hal ini sejalan dengan penelitian [5] yang menunjukkan keunggulan kombinasi AES dan LUC pada data teks, serta mendukung temuan [7] terkait efektivitas LUC dalam mengamankan kunci simetris.

Namun, penelitian ini menawarkan keunikan dibanding penelitian terdahulu, yaitu penerapannya pada file citra dengan ukuran besar (hingga 3 MB), bukan sekadar data teks. Selain itu, penelitian ini berhasil menunjukkan bahwa integrasi AES–LUC dapat menjaga kualitas file citra tanpa kehilangan data, yang belum banyak ditunjukkan pada penelitian sebelumnya.

Kelebihan penelitian yaitu menyajikan bukti empiris bahwa integrasi AES–LUC dapat diterapkan pada file citra, bukan hanya data teks. Hasil enkripsi citra tidak dapat dikenali secara visual, sementara hasil dekripsi mengembalikan file ke bentuk asli dengan kualitas 100%. Sistem yang dirancang mampu menjaga keamanan kunci AES melalui perlindungan LUC, yang jarang diteliti dalam konteks citra digital.

5 Kesimpulan (or Conclusion)

Sistem integrasi keamanan file citra berbasis algoritma AES-128 dan LUC berhasil dirancang serta diimplementasikan sesuai dengan tujuan penelitian. Algoritma AES digunakan untuk melakukan enkripsi terhadap isi file citra sehingga menghasilkan ciphertext yang tidak dapat dikenali secara visual, sedangkan algoritma LUC berfungsi untuk mengamankan kunci AES dengan menghasilkan cipherkey yang tidak dapat dibaca secara langsung, sehingga distribusi kunci menjadi lebih terjamin. Proses dekripsi yang dilakukan mampu mengembalikan file citra ke bentuk semula dengan struktur byte yang identik dengan file asli, sehingga membuktikan efektivitas sistem yang dibangun. Proses penerapan dan implementasi sistem dilakukan menggunakan bahasa pemrograman Python. Sistem dilengkapi dengan form dekstop, form integrasi AES–LUC, form enkripsi, dan form dekripsi yang saling terhubung secara fungsional. Melalui fitur-fitur tersebut, pengguna dapat melakukan pembangkitan kunci AES, pembangkitan kunci LUC, enkripsi dan dekripsi kunci AES, serta enkripsi dan dekripsi file citra secara terpadu. Hasil pengujian menunjukkan bahwa sistem berjalan sesuai dengan rancangan serta mampu berfungsi dengan baik sesuai harapan dan kebutuhan penelitian.

Referensi (Reference)

[1] S. R. Siburian, R. Alek, S. Sinaga, and F. Yudistira, “KRIPTOSISTEM HYBRID MENGGUNAKAN KOMBINASI AES DAN RSA UNTUK ENKRIPSI TEKS PESAN.” [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

[2] N. Oper, S. Balafif, and F. Al-KhaliqZ, “MODIFIKASI ALGORITMA KRIPTOGRAFI CAESAR CIPHER MENJADI ALGORITMA KRIPTOGRAFI ASIMETRIS DENGAN METODE AGILE,” 2022.

[3] T. H. Saputro, N. Hidayati, and E. I. H. Ujianto, “JIP (Jurnal Informatika Polinema) SURVEI TENTANG ALGORITMA KRIPTOGRAFI ASIMETRIS”.

[4] D. Alfatah, “Penggunaan Kriptografi Asimetris Dalam Pengamanan Komunikasi IOT,” 2024.

[5] W. Ady Putra, S. Suyanto, and M. Zarlis, “Performance Analysis Of The Combination Of Advanced Encryption Standard Cryptography Algorithms With Luc For Text Security,” *SinkrOn*, vol. 8, no. 2, pp. 890–897, Apr. 2023, doi: 10.33395/sinkron.v8i2.12202.

[6] M. R. Alfani, M. Furqan, and Y. R. Nasution, “PENGAMANAN DATA TEKS MENGGUNAKAN METODE DIGITAL SIGNATURE ALGORITHM (DSA) DAN ADVANCED ENCRYPTION STANDARD (AES),” 2024. [Online]. Available: http://jurnal.goretanpena.com/index.php/JSSR

[7] N. Permata Dewi, D. J. M. Sembiring, R. BR. Ginting, and M. BR. Ginting, “Pengamanan Data dengan Kriptografi Hibrida Algoritma Hill Cipher dan Algoritma Luc Serta Steganografi

Chaotic Lsb," *Jurnal Syntax Admiration*, vol. 3, no. 2, pp. 341–361, Feb. 2022, doi: 10.46799/jsa.v3i2.389.

[8] M. Firman Aditya, W. Arfanda, and V. Ndika purnama, "STUDI ALGORITMA KRIPTOGRAFI KUNCI SIMETRIS PADA KEAMANAN DATA DENGAN METODE KOMPARASI." [Online]. Available: https://journal.iteba.ac.id/index.php/jurnalsiteba/index

[9] Y. S. Yudanto and I. M. Suartana, "Analisis Kekuatan Enkripsi Data Pada Citra Digital Menggunakan Metode Rubiks Cube," *Journal of Informatics and Computer Science*, vol. 03, 2022.

[10] A. Triono, A. Setia Budi, and R. Abdillah, "IMPLEMENTASI PERETASAN SANDI VIGENERE CHIPHER MENGGUNAKAN BAHASA PEMROGRAMAN PYTHON," 2023.