Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 7, Nomor: 1, Juni 2026

PERANCANGAN SISTEM KEAMANAN LAPORAN AUDIT BERBASIS WEB MENGGUNAKAN ENKRIPSI AES DAN STEGANOGRAFI LSB

Aulia Shiddiq Asy Syifa[1], Amrullah[2]

[1] *Universitas Muhammadiyah Sumatera Utara*
Jl. Kapten Muchtar Basri No.3
[1]shddq.aulia@gmail.com, [2]amrullah@umsu.ac.id

ABSTRAK

Keamanan dokumen laporan audit merupakan aspek kritis dalam tata kelola informasi perusahaan, mengingat tingginya risiko pencurian, penyadapan, dan penyalahgunaan data pada era digital. Penelitian ini merancang dan mengimplementasikan sistem keamanan laporan audit berbasis web dengan menggabungkan algoritma kriptografi Advanced Encryption Standard 128-bit (AES-128) dan metode steganografi Least Significant Bit (LSB). Pendekatan ganda ini bertujuan tidak hanya melindungi isi dokumen melalui enkripsi, tetapi juga menyamarkan keberadaan data terenkripsi di dalam media citra digital. Sistem dirancang dengan tiga peran pengguna utama, yaitu staff yang bertugas mengunggah dan mengenkripsi laporan, auditor yang melakukan ekstraksi dan dekripsi dokumen, serta admin yang bertanggung jawab memantau seluruh aktivitas pengguna serta mengelola konfigurasi akun staff dan auditor. Pengujian sistem menunjukkan bahwa proses enkripsi dan dekripsi AES-128 berjalan efisien dengan waktu enkripsi berkisar antara 0,285 ms hingga 30,725 ms untuk ukuran file 100 KB hingga 4,68 MB. Sementara itu, metode steganografi LSB terbukti mampu menyembunyikan data terenkripsi ke dalam citra tanpa menghasilkan perubahan visual yang signifikan, sehingga keberadaan pesan tersembunyi tidak terdeteksi secara kasat mata. Hasil penelitian membuktikan bahwa kombinasi AES-128 dan LSB merupakan pendekatan yang efektif dalam meningkatkan kerahasiaan dan integritas dokumen laporan audit.

***Kata Kunci*— keamanan informasi, kriptografi, AES-128, steganografi, Least Significant Bit, laporan audit, website**

ABSTRACT

The security of audit report documents is a critical aspect of corporate information governance, given the high risks of data theft, interception, and misuse in the digital era. This study designs and implements a web-based audit report security system by combining the Advanced Encryption Standard 128-bit (AES-128) cryptographic algorithm with the Least Significant Bit (LSB) steganography method. This dual-layer approach aims not only to protect document contents through encryption, but also to conceal the existence of encrypted data within digital image media. The system is designed with three main user roles: staff responsible for uploading and encrypting reports, auditors performing document extraction and decryption, and an administrator who monitors all user activities and manages account configurations for staff and auditors. System testing demonstrates that the AES-128 encryption and decryption processes operate efficiently, with encryption times ranging from 0.285 ms to 30.725 ms for file sizes between 100 KB and 4.68 MB. Meanwhile, the LSB steganography method successfully conceals encrypted data within images without producing visually significant changes, rendering the hidden message undetectable to the naked eye. The results confirm that the combination of AES-128 and LSB constitutes an effective approach for enhancing the confidentiality and integrity of audit report documents.

***Keywords*— information security, cryptography, AES-128, steganography, Least Significant Bit, audit report, website**

Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 7, Nomor: 1, Juni 2026

I. PENDAHULUAN

Di era digital ini, komunikasi sudah dipermudah dengan adanya dokumen digital. Dokumen digital dapat memberikan informasi, baik informasi yang berbentuk tulisan, audio, maupun vidio[1]. Dengan adanya kemudahan tersebut, banyak perusahaan yang beralih menggunakan dokumen digital sebagai alat komunikasi agar lebih efisien. Meskipun dengan menggunakan dokumen digital dapat mempermudah komunikasi lebih cepat tidak menjamin kemanan dokumen tersebut aman dari serangan siber.

Keamanan data merupakan suatu upaya untuk melindungi informasi agar tidak diakses, diubah, atau digunakan oleh pihak yang tidak bertanggung jawab[2]. Informasi rahasia seperti dokumen audit perusahaan banyak dipertukarkan memalui berbagai media digital seperti email, website, dan platform daring lainnya. Namun, pertukaran digital ini menimbulkan tantangan serius terkait potensi pencurian, penyadapan, dan penyalahgunaan informasi oleh pihak-pihak yang tidak bertanggung jawab. Berdasarkan data dari Laporan Kinerja Instansi Pemerintah (LKIP) Ditreskrimsus Polda Metro Jaya, kasus pencurian terhadap data pribadi seperti file e-document pada tahun 2014 crime total sebanyak 1225 dengan crime clearance 790 sehingga memiliki presentasi 64%, di tahun 2015 sendiri crime total sebesar 1569 untuk crime clearance sebesar 851 dengan persentasi 54 % kasus, dan di tahun 2016 crime total sebesar 1207, sedang untuk crime clearance sebanyak 699 dengan persentasi 57%, dengan demikian bahwa kasus cybercrime dari data tersebut keamanan informasi menjadi sangat penting di era teknologi yang semakin meningkat[3]. Oleh karena itu, diperlukan upaya yang lebih canggih untuk melindungi data agar tetap rahasia dan hanya dapat diakses oleh orang yang berwenang[4].

Salah satu metode untuk menjaga keamanan data adalah dengan menerapkan pendekatan steganografi. Steganografi merupakan teknik penyembunyian informasi ke dalam media lain, seperti gambar digital, tanpa menarik perhatian pihak luar. Salah satu metode yang sering digunakan dalam steganografi adalah Least Significant Bit (LSB), yang menyisipkan data pada bit-bit paling rendah dari setiap piksel gambar. Teknik ini mampu menjaga tampilan visual gambar sehingga perubahan tidak mudah terdeteksi secara kasat mata. Namun, meskipun metode ini cukup aman, penggunaan metode ini tetap memiliki kelemahan karena masih rentan terhadap teknik deteksi dan analisis steganalisis[5].

Meskipun metode LSB mampu menyembunyikan keberadaan pesan, data yang disisipkan masih berpotensi diekstraksi oleh pihak yang tidak berwenang. Oleh karena itu, diperlukan mekanisme keamanan tambahan melalui penerapan kriptografi. Kriptografi merupakan salah satu teknik keamanan yang dikembangkan untuk menjaga dan melindungi pesan rahasia sehingga terhindar dari pihak lain yang tidak berhak[6]. Proses kerja kriptografi akan menyandikan pesan atau informasi sehingga tidak dapat dimengerti oleh pihak lain. Konsep utama kriptografi melakukan enkripsi dan deskripsi. Algoritma kriptografi Advanced Encryption Standard merupakan teknik kriptografi agar data aman dan terjaga keasliannya. Blok chipertext simentrik merupakan algoritma AES yang dapat mendeskripsi (decrypt) dan mengekskripsi (encrypt) data/informasi. Kunci kriptigrafi 128, 192 dan 256 bits digunakan agar dapat melakukan enkrip dan dekrip data/informasi pada blok 128 bits. Kelebihan pada keamanan yang dimiliki AES diantaranya karakteristik algoritma dengan implementasinya dan karakteristik algoritma serta kecepatan.

Berdasarkan kelebihan yang dimiliki oleh steganografi dan kriptografi, penelitian ini mengembangkan sebuah sistem yang menggabungkan pendekatan steganografi dengan kriptografi dalam upaya meningkatkan keamanan penyembunyian informasi. Untuk meningkatkan keamanan penyembunyian data, steganografi perlu dikombinasikan dengan metode enkripsi[4]. Dalam banyak kasus kebocoran data, metode enkripsi saja tidak cukup untuk mengamankan data karena keberadaan data terenkripsi itu sendiri dapat memicu upaya dekripsi dari pihak luar.

Penelitian ini menghasilkan sebuah website yang dirancang untuk meningkatkan keamanan dokumen laporan audit dari serangan siber dengan melakukan kombinasi ganda kriptografi dan steganografi.

Dengan demikian, website ini diharapkan dapat menjaga dokumen laporan audit sehingga dapat tersampaikan kepada pihak yang dituju tanpa risiko kebocoran data yang berpotensi merugikan perusahaan.

II. METODOLOGI PENELITIAN

Cara paling mudah untuk memenuhi persyaratan format penulisan adalah dengan menggunakan dokumen ini sebagai template. Kemudian ketikkan teks anda ke dalamnya.

Objek penelitian dalam penelitian ini adalah laporan audit yang bersifat rahasia dan memiliki tingkat sensitivitas tinggi terhadap keamanan informasi. Laporan audit tersebut memuat data dan informasi penting yang hanya dapat diakses oleh pihak yang berwenang, sehingga membutuhkan mekanisme perlindungan yang memadai untuk mencegah terjadinya kebocoran, penyalahgunaan, maupun akses oleh pihak yang tidak bertanggung jawab.

Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 7, Nomor: 1, Juni 2026

Fokus objek penelitian ini terletak pada proses pengamanan laporan audit, khususnya pada tahap penyimpanan dan pengiriman laporan audit dari staff kepada auditor melalui sistem berbasis web. Oleh karena itu, penelitian ini menitikberatkan pada penerapan mekanisme keamanan data menggunakan algoritma enkripsi Advanced Encryption Standard (AES) dan metode steganografi Least Significant Bit (LSB) untuk menjaga kerahasiaan dan integritas laporan audit selama proses pengelolaan dan distribusi data.

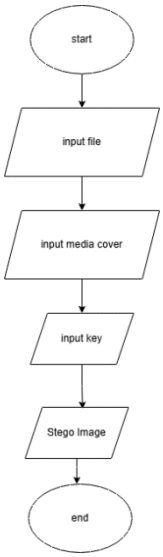
A. Objek Penelitian

Objek penelitian adalah entitas, fenomena, atau aspek tertentu yang menjadi pusat perhatian dalam kegiatan penelitian. Objek tersebut dapat mencakup perilaku, aktivitas, pandangan, kondisi, maupun proses yang diamati dan dianalisis secara sistematis guna menjawab permasalahan serta mencapai tujuan penelitian yang telah ditetapkan [7]. Objek penelitian dalam penelitian ini adalah laporan audit yang bersifat rahasia dan memiliki tingkat sensitivitas tinggi terhadap keamanan informasi. Laporan audit tersebut memuat data dan informasi penting yang hanya dapat diakses oleh pihak yang berwenang, sehingga membutuhkan mekanisme perlindungan yang memadai untuk mencegah terjadinya kebocoran, penyalahgunaan, maupun akses oleh pihak yang tidak bertanggung jawab.

Fokus objek penelitian ini terletak pada proses pengamanan laporan audit, khususnya pada tahap penyimpanan dan pengiriman laporan audit dari staff kepada auditor melalui sistem berbasis web. Oleh karena itu, penelitian ini menitikberatkan pada penerapan mekanisme keamanan data menggunakan algoritma enkripsi Advanced Encryption Standard (AES) dan metode steganografi Least Significant Bit (LSB) untuk menjaga kerahasiaan dan integritas laporan audit selama proses pengelolaan dan distribusi data.

B. Flowchart Enkripsi dan Embedding File

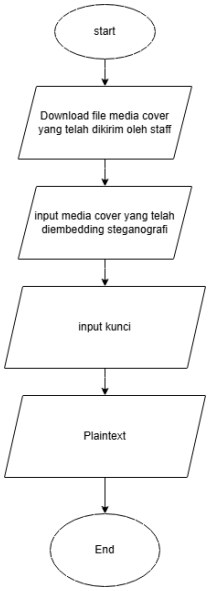
Flowchart enkripsi dan embedding file menampilkan alur proses enkripsi data yang dimulai dengan memasukkan dokumen, media cover, serta kunci. Setelah itu, akan menghasilkan keluaran berupa stego image atau gambar yang telah disisipkan oleh dokumen yang telah dienkripsi [8].



Gbr: 1 Flowchart Enkripsi dan Embedding *File*

C. Flowchart Ekstraksi dan Dekripsi File

Flowchart ektraksi dan dekripsi file menampilkan alur proses ekstraksi dari media cover yang telah disisipkan oleh dokumen yang telah dienkripsi, sehingga dapat menampilkan data asli.



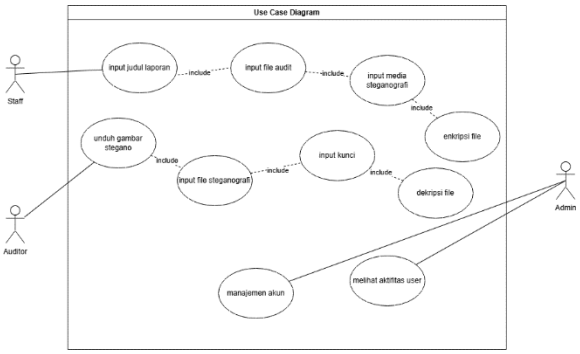
Gbr: 2 Flowchart Ekstraksi dan Dekripsi *File*

D. Use Case Diagram

Use case diagram merupakan salah satu alat pemodelan yang digunakan untuk merepresentasikan kebutuhan sistem pada tingkat konseptual. Diagram ini berperan sebagai media komunikasi yang membantu dalam memahami dan mendefinisikan kebutuhan sistem yang akan dikembangkan. Selain itu, use case diagram mendukung pendekatan pengembangan sistem

Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 7, Nomor: 1, Juni 2026

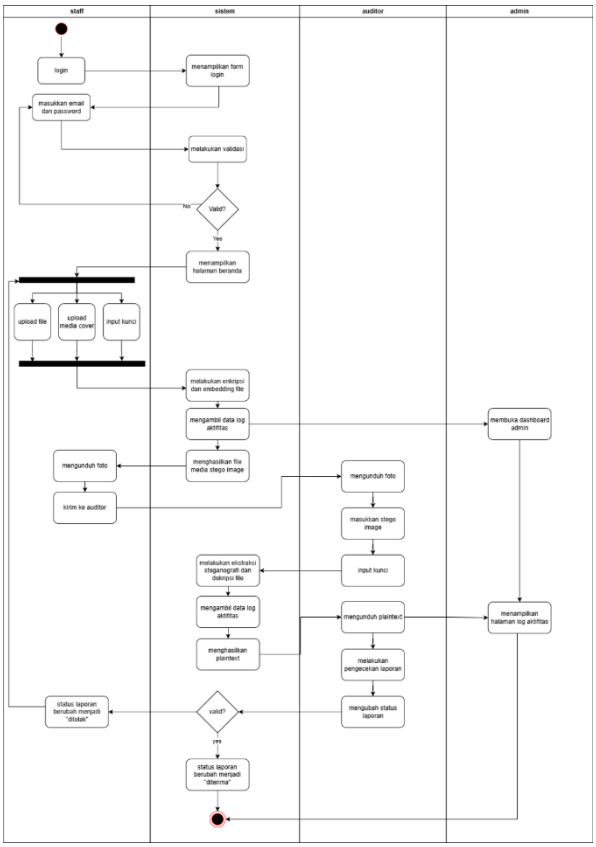
yang berorientasi pada kebutuhan dan kegunaan pengguna. Melalui diagram ini, hubungan serta interaksi antara pengguna maupun entitas eksternal lainnya dengan sistem dapat digambarkan secara jelas dan terstruktur [9]. Use Case Diagram pada penelitian menjelaskan keterlibatan setiap aktor pada sistem dalam melakukan enkripsi dan dekripsi data. Berikut use case diagram untuk sistem yang akan dirancang.



Gbr: 3 *Use Case* Diagram

E. Activity Diagram Enkripsi, Dekripsi, dan Steganografi

Activity Diagram merupakan representasi grafis yang digunakan untuk memodelkan alur aktivitas, proses, maupun mekanisme kerja dalam suatu sistem. Diagram ini berfungsi untuk menggambarkan urutan aktivitas yang dilakukan oleh sistem dalam mencapai tujuan tertentu, sekaligus menunjukkan keterkaitan antaraktivitas selama proses operasional aplikasi berlangsung. Dengan demikian, Activity Diagram dapat membantu dalam memahami logika proses bisnis serta alur kerja sistem secara lebih terstruktur dan sistematis [10]. Activity diagram pada penelitian ini menjelaskan alur aktivitas dari proses awal data asli yang kemudian dienkripsi menggunakan kriptografi dan disisipkan menggunakan steganografi hingga datanya dapat diterima oleh auditor dalam bentuk aslinya.

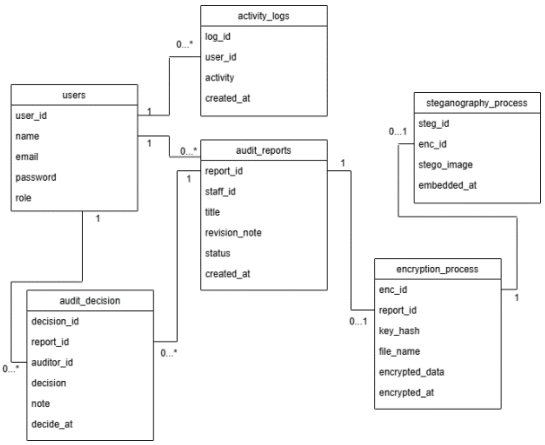


Gbr: 4 Activity Diagram Proses Enkripsi, Dekripsi, dan Steganografi

F. Class Diagram

Class Diagram merupakan salah satu diagram dalam Unified Modeling Language (UML) yang digunakan untuk memodelkan struktur statis sistem. Diagram ini menggambarkan kelas-kelas yang terdapat dalam sistem, atribut dan operasi yang dimiliki setiap kelas, serta hubungan antar kelas. Melalui Class Diagram, pengembang dapat mendefinisikan komponen-komponen sistem secara sistematis sehingga rancangan yang dihasilkan mampu mendukung kebutuhan fungsional sistem dan menjadi acuan dalam proses implementasi perangkat lunak[11]. Class diagram pada penelitian ini digunakan untuk menggambarkan semua hubungan antar kelas dalam suatu sistem. Berikut merupakan class diagram untuk sistem yang akan dirancang.

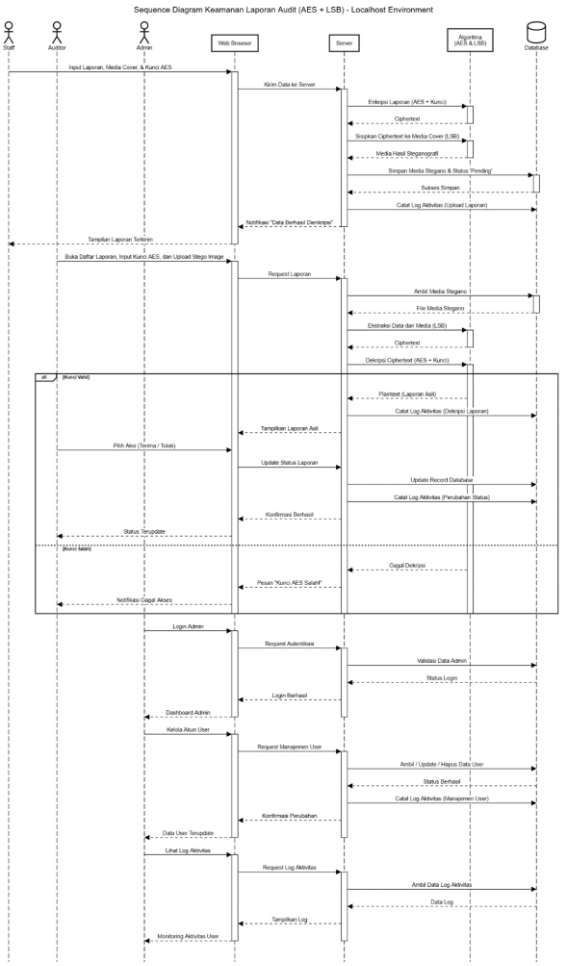
Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 7, Nomor: 1, Juni 2026



Gbr: 5 *Class Diagram*

G. Sequence Diagram

Sequence Diagram merupakan salah satu diagram dalam Unified Modeling Language (UML) yang digunakan untuk memodelkan perilaku dinamis sistem melalui representasi interaksi antarobjek secara berurutan. Diagram ini menggambarkan pertukaran pesan antarobjek berdasarkan kronologi waktu, sehingga dapat digunakan untuk memahami alur proses, mekanisme komunikasi, serta keterlibatan setiap objek dalam pelaksanaan suatu fungsi sistem [12]. Sequence diagram pada penelitian ini digunakan untuk menggambarkan alur dari interaksi antar objek secara berurutan dari sistem keamanan laporan audit yang akan dibangun. Berikut sequence diagram untuk sistem yang akan dirancang.



Gbr: 6 *Sequence Diagram*

H. Implementasi Steganografi LSB

Berbeda dengan kriptografi yang berfokus pada penyamaran isi pesan, steganografi lebih menekankan pada upaya menyembunyikan keberadaan pesan itu sendiri. Dalam lingkungan digital, teknik steganografi memanfaatkan bit-bit pada berkas media untuk menyisipkan informasi tambahan tanpa menimbulkan perubahan yang signifikan terhadap tampilan maupun kualitas media tersebut. Penyisipan informasi dalam suatu berkas dilakukan dengan memanfaatkan perubahan pada atribut-atribut tertentu, seperti format tampilan teks, jenis huruf, atau ukuran huruf, sehingga informasi tambahan dapat disimpan tanpa memengaruhi isi utama berkas secara signifikan [13].

Seiring dengan meningkatnya kebutuhan akan keamanan data, khususnya pada jaringan yang rentan terhadap penyadapan dan berbagai bentuk serangan, steganografi menjadi semakin relevan sebagai salah satu metode perlindungan informasi [14].

Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 7, Nomor: 1, Juni 2026

Meskipun demikian, penerapan steganografi masih menghadapi berbagai tantangan. Salah satu kendala utama adalah memastikan bahwa informasi yang disisipkan tidak dapat terdeteksi oleh teknik steganalisis. Steganalisis sendiri merupakan teknik untuk mendeteksi dan mengungkap keberadaan pesan tersembunyi dalam media digital [15].

Seiring dengan kemajuan teknologi, teknik steganalysis juga terus berkembang, sehingga mendorong perlunya inovasi berkelanjutan dalam pengembangan metode steganografi. Berbagai penelitian terus dilakukan untuk menghasilkan teknik steganografi yang lebih aman dan semakin sulit dideteksi, agar proses penyembunyian informasi dapat dilakukan dengan tingkat keamanan yang lebih tinggi. Selain itu, metode steganografi Least Significant Bit (LSB) yang diterapkan tanpa proses enkripsi memiliki kelemahan dari aspek keamanan, karena pesan yang disisipkan tetap tersimpan dalam bentuk plaintext. Kondisi ini memungkinkan pihak ketiga untuk mengekstraksi dan memperoleh isi pesan apabila mengetahui keberadaan data tersembunyi serta algoritma LSB yang digunakan. Dengan demikian, penggunaan steganografi LSB sebagai satu-satunya mekanisme pengamanan dinilai kurang efektif dalam menjamin kerahasiaan informasi, khususnya untuk transmisi data yang memiliki tingkat sensitivitas tinggi [16]. Dengan memanfaatkan steganografi untuk menyamarkan keberadaan data dan enkripsi untuk melindungi isi data, tingkat keamanan yang dihasilkan dapat menjadi lebih optimal dan efektif. Dalam era digital yang semakin terhubung, steganografi menawarkan solusi inovatif terhadap tantangan keamanan informasi, sehingga berperan penting dalam melindungi data sensitif dari ancaman yang terus berkembang.

Secara umum, steganografi terbagi ke dalam dua domain utama, yaitu domain spasial dan domain transformasi. Salah satu teknik yang paling sering digunakan pada domain spasial adalah Least Significant Bit (LSB). Metode LSB dikenal sebagai teknik steganografi yang sederhana dan mudah diterapkan, yaitu dengan memodifikasi bit yang memiliki tingkat kepentingan paling rendah dalam suatu berkas. Perubahan pada bit tersebut hanya menimbulkan perbedaan yang sangat kecil, sehingga hampir tidak memengaruhi kualitas media secara visual. Penerapan teknik LSB dalam steganografi terbukti mampu menghasilkan citra stego dengan kualitas yang baik serta tetap menjaga aspek imperceptibility, yaitu ketidakmampuan manusia untuk membedakan media asli dan media yang telah disisipi pesan [17].

I. Implementasi Algoritma AES-128

Proses enkripsi pada algoritma AES diawali dengan penambahan kunci awal (initial key) ke dalam state. Selanjutnya, state tersebut diproses melalui sejumlah putaran (round) sebanyak Nr kali. Setiap putaran terdiri dari empat transformasi nonlinier yang dirancang untuk meningkatkan tingkat keamanan data. Pada putaran terakhir, salah satu transformasi linear, yaitu MixColumns, tidak lagi diterapkan sehingga menghasilkan ciphertext akhir [18]. Proses enkripsi menggunakan AES-128 dilakukan melalui sejumlah tahapan berulang yang dikenal sebagai putaran (round). Setiap putaran mencakup beberapa langkah yang bertujuan mengubah data secara bertahap menjadi bentuk yang lebih kompleks. Data asli (plaintext) terlebih dahulu dikombinasikan dengan kunci rahasia menggunakan operasi XOR. Selanjutnya, data diproses melalui beberapa putaran yang melibatkan tahapan pergeseran baris (ShiftRows), substitusi byte (SubBytes), pencampuran kolom (MixColumns), serta penambahan kunci rahasia kembali (AddRoundKey). Setiap putaran dirancang untuk meningkatkan tingkat keacakan data, sehingga informasi menjadi semakin sulit dipahami oleh pihak yang tidak berwenang. Pada putaran terakhir, beberapa tahapan tertentu tidak lagi dilakukan untuk menghasilkan data terenkripsi akhir (ciphertext). Proses dekripsi merupakan kebalikan dari enkripsi, melibatkan tahapan InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey secara berurutan.

III.HASIL DAN PEMBAHASAN

A. Perhitungan Manual Algoritma AES-128

Perhitungan manual dilakukan untuk memverifikasi kebenaran logika enkripsi yang diterapkan dalam sistem, menggunakan data sampel plaintext "AUDIT_REPORT_123" (16 byte/128 bit) dan cipher key "KUNCIRAHASIA1234" (16 byte/128 bit). Plaintext direpresentasikan dalam matriks hexadesimal 4×4, begitu pula dengan cipher key.

Proses ekspansi kunci (key expansion) menghasilkan 11 round key (176 byte) dari kunci awal 16 byte. Kunci awal dibagi menjadi empat word (W0–W3), kemudian setiap round key berikutnya diperoleh melalui fungsi g yang mencakup RotWord (rotasi byte ke kiri), SubWord (substitusi menggunakan S-Box), dan XOR dengan Rcon (Round Constant). Round key 1 yang dihasilkan adalah W4 = 69 96 56 84, W5 = 20 C4 17 CC, W6 = 61 97 4E 8D, dan W7 = 50 A5 7D B9, dengan proses yang sama dilanjutkan hingga Round Key 10.

Tahap initial round dilakukan dengan operasi XOR antara state matrix (plaintext) dengan Round Key 0 (cipher key asli), menghasilkan matriks state awal. Pada putaran pertama, tahapan SubBytes dilakukan dengan mensubstitusi setiap byte pada state matrix menggunakan tabel S-Box, di mana digit pertama byte

Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 7, Nomor: 1, Juni 2026

menjadi indeks baris dan digit kedua menjadi indeks kolom. Contoh sebagian hasil transformasi SubBytes pada putaran pertama disajikan pada Tabel 1.

TABEL I
HASILTRANSFORMASI SUB BYTES

Byte Awal (Hex)	Koordinat S-Box	Byte Akhir (Hex)
0A	Baris 0, Kolom A	67
00	Baris 0, Kolom 0	63
1D	Baris 1, Kolom D	A4
0D	Baris 0, Kolom D	D7
11	Baris 1, Kolom 1	82

Setelah SubBytes, dilakukan ShiftRows dengan menggeser baris kedua sebanyak satu posisi, baris ketiga dua posisi, dan baris keempat tiga posisi ke kiri. Tahapan MixColumns kemudian memproses setiap kolom state melalui perkalian matriks pada Galois Field GF(2^8), menghasilkan difusi maksimal pada data. Setiap putaran diakhiri dengan AddRoundKey, yaitu XOR antara state hasil MixColumns dengan round key yang bersesuaian. Pada putaran terakhir (round 10), tahapan MixColumns ditiadakan, sehingga proses langsung diakhiri dengan AddRoundKey menggunakan Round Key 10 dan menghasilkan ciphertext akhir: 40 02 4A 96 / C1 6F 51 DD / 7E 5F D1 84 / 91 EE AB D1.

B. Perhitungan Manual Algoritma LSB

Setelah ciphertext diperoleh, tahap berikutnya adalah menyisipkan bit-bit ciphertext ke dalam bit paling tidak signifikan (LSB) dari piksel citra penampung (cover image). Ciphertext terlebih dahulu dikonversi ke dalam representasi biner, di mana setiap byte hexadesimal diterjemahkan menjadi delapan bit biner. Sebagai contoh, byte pertama ciphertext 40_{16} dikonversi menjadi 01000000_2 dan disisipkan ke dalam 8 piksel pertama citra. Proses penyisipan dilakukan dengan mengganti bit LSB setiap piksel dengan satu bit dari ciphertext sesuai persamaan I(x,y) = I(x,y) & ~1 + data[k].

Tabel 2 menunjukkan simulasi transformasi bit pada delapan piksel pertama citra saat menyisipkan byte 40_{16} (01000000_2). Perubahan nilai piksel yang terjadi hanya sebesar 0 atau −1, yang secara visual tidak dapat dibedakan dari citra aslinya.

TABEL II
TRANSFORMASI BIT PADA PIKSEEL

Piksel	Nilai (Des)	Nilai Biner	Bit Pesan	Hasil LSB	Nilai Stego	Perubahan
P1	154	10011010	0	10011010	154	0
P2	157	10011101	1	10011101	157	0
P3	155	10011011	0	10011010	154	-1
P4	158	10011110	0	10011110	158	0
P5	159	10011111	0	10011110	158	-1

C. Hasil Pengujian Enkripsi dan Dekripsi

Pengujian enkripsi dan dekripsi dilakukan untuk mengukur waktu yang dibutuhkan algoritma AES-128 dalam memproses file dengan ukuran yang bervariasi. Pengujian dilakukan terhadap lima sampel file dengan ukuran mulai dari 100 KB hingga 4,68 MB. Hasil pengujian disajikan pada Tabel 3.

TABEL III
PENGUJIAN WAKTU ENKRIPSI DAN DEKRIPSI

No	Ukuran File	Waktu Enkripsi	Waktu Dekripsi
1	100 KB	0,285 ms	0,132 ms
2	128 KB	0,270 ms	0,301 ms
3	412 KB	2,199 ms	0,548 ms
4	1,73 MB	3,954 ms	10,587 ms
5	4,68 MB	30,725 ms	14,658 ms

Berdasarkan Tabel 3, waktu enkripsi dan dekripsi meningkat seiring dengan bertambahnya ukuran file yang diproses. Untuk file berukuran kecil (100 KB), proses enkripsi hanya memerlukan 0,285 ms, sedangkan untuk file terbesar (4,68 MB) memerlukan 30,725 ms. Meskipun terdapat peningkatan waktu proses yang proporsional terhadap ukuran file, seluruh nilai tersebut masih berada dalam rentang yang sangat cepat dan dapat diterima untuk kebutuhan pengamanan dokumen laporan audit secara praktis. Hal ini konsisten dengan keunggulan algoritma AES-128 yang dikenal memiliki kecepatan enkripsi tinggi sekaligus tingkat keamanan yang kuat [19].

Pengujian fungsional juga dilakukan untuk memverifikasi keberhasilan proses dekripsi. Hasil pengujian menunjukkan bahwa seluruh file yang dienkripsi dapat didekripsi kembali menjadi dokumen asli tanpa kehilangan data, membuktikan bahwa implementasi AES-128 pada sistem berjalan dengan benar dan konsisten.

Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 7, Nomor: 1, Juni 2026

D. Hasil Pengujian Steganografi

Pengujian steganografi dilakukan untuk mengevaluasi kemampuan metode LSB dalam menyembunyikan dokumen laporan audit yang telah dienkripsi ke dalam citra digital tanpa menurunkan kualitas visual secara signifikan. Pengujian menggunakan citra berformat PNG sebagai cover image dengan proses embedding dilakukan pada setiap kanal warna citra. Tabel 4 menyajikan perbandingan ukuran dan resolusi citra sebelum dan sesudah proses penyisipan.

TABEL IV
PERBANDINGAN UKURAN DAN RESOLUSI STEGANOGRAFI

No	Ukuran Sebelum Disisipkan	Ukuran Setelah Disisipkan	Resolusi
1	1,00 MB	751 KB	775 x 607
2	1,49 MB	1,45 MB	1024 x 1536
3	55,9 KB	78,3 KB	500 x 500
4	829 KB	745 KB	1280 x 720
5	55,9 KB	65,6 KB	500 x 500

Berdasarkan Tabel IV, proses steganografi menggunakan metode LSB tidak menyebabkan perubahan ukuran file yang signifikan. Pada beberapa sampel, ukuran stego image tercatat lebih kecil dibandingkan citra asli. Kondisi ini bukan disebabkan oleh proses penyisipan data menggunakan LSB, melainkan oleh mekanisme penyimpanan citra pada sistem. Dalam implementasi yang digunakan, citra hasil steganografi disimpan dalam format PNG sehingga pada beberapa kasus terjadi perubahan format dari citra asli (misalnya JPEG) ke PNG. Perbedaan algoritma kompresi dan pengelolaan metadata pada kedua format tersebut dapat menyebabkan ukuran file hasil menjadi lebih kecil maupun lebih besar dibandingkan file asli.

Selain itu, dimensi (resolusi) citra tetap sama antara sebelum dan sesudah proses embedding, yang menunjukkan bahwa metode LSB tidak mengubah struktur dasar citra. Hasil pengamatan visual juga menunjukkan tidak terdapat perbedaan yang dapat dideteksi oleh mata manusia antara citra asli dan stego image. Hal ini menunjukkan bahwa karakteristik imperceptibility dari metode LSB tetap terjaga, sehingga keberadaan data rahasia yang disisipkan tidak mudah dikenali secara visual.

Temuan ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa metode steganografi LSB mampu menghasilkan citra stego dengan kualitas visual yang baik tanpa menimbulkan perubahan yang signifikan pada tampilan citra. Selain itu, penggunaan format PNG sebagai media keluaran memberikan keuntungan karena menggunakan kompresi *lossless*, sehingga nilai piksel yang telah dimodifikasi untuk proses penyisipan data tetap terjaga dan dapat diekstraksi kembali dengan baik [20]. Kombinasi algoritma AES-128 dan steganografi LSB pada penelitian ini memberikan mekanisme keamanan berlapis, di mana AES-128 melindungi kerahasiaan isi dokumen melalui proses enkripsi, sedangkan LSB menyamarkan keberadaan data tersebut di dalam citra digital. Dengan demikian, keamanan penyimpanan dan transmisi laporan audit dapat ditingkatkan secara lebih efektif.

KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem keamanan laporan audit berbasis web dengan menggabungkan algoritma kriptografi AES-128 dan steganografi LSB. Sistem memiliki tiga peran pengguna, yaitu staff untuk mengunggah dan mengenkripsi laporan, auditor untuk melakukan ekstraksi dan dekripsi dokumen, serta admin untuk memantau aktivitas dan mengelola akun. Pembagian peran tersebut memastikan akses informasi sensitif hanya dilakukan oleh pihak yang berwenang.

Hasil pengujian menunjukkan bahwa AES-128 mampu mengenkripsi dan mendekripsi dokumen secara efisien dengan waktu proses antara 0,285 ms hingga 30,725 ms pada ukuran file 100 KB sampai 4,68 MB tanpa kehilangan data. Metode LSB juga berhasil menyembunyikan ciphertext ke dalam citra digital tanpa perubahan visual yang terlihat dan tanpa mengubah dimensi citra. Kombinasi kedua metode menghasilkan keamanan berlapis melalui perlindungan isi dokumen dan penyamaran keberadaan data rahasia.

Secara keseluruhan, sistem telah memenuhi tujuan penelitian dalam meningkatkan kerahasiaan dan integritas laporan audit dari ancaman kebocoran data. Pengembangan selanjutnya dapat dilakukan dengan menambahkan pengujian terhadap serangan steganalisis, mekanisme tanda tangan digital, serta dukungan lebih banyak format file untuk memperluas penggunaan sistem.

PENUTUP

Berdasarkan hasil perancangan dan implementasi sistem keamanan laporan audit berbasis web menggunakan metode enkripsi AES dan steganografi LSB, dapat disimpulkan bahwa sistem yang dikembangkan mampu meningkatkan keamanan data laporan audit dari ancaman akses tidak sah. Metode AES digunakan untuk mengenkripsi isi laporan sehingga data tidak dapat dibaca tanpa kunci yang sesuai, sedangkan metode Least Significant Bit (LSB) digunakan untuk menyembunyikan data terenkripsi ke

dalam media gambar sehingga keberadaan data menjadi lebih sulit diketahui.

Penerapan kombinasi kedua metode tersebut memberikan lapisan keamanan ganda, yaitu keamanan melalui proses enkripsi dan keamanan melalui penyembunyian data. Sistem berbasis web yang dirancang juga memudahkan pengguna dalam melakukan proses unggah, enkripsi, penyisipan, ekstraksi, dan dekripsi laporan audit secara lebih praktis dan efisien.

Hasil pengujian menunjukkan bahwa sistem dapat menjalankan fungsi utama dengan baik, mulai dari proses enkripsi AES, penyisipan data menggunakan steganografi LSB, hingga proses ekstraksi dan dekripsi kembali data laporan audit tanpa mengalami perubahan isi data. Dengan demikian, sistem yang dirancang dapat menjadi solusi untuk menjaga kerahasiaan dan keamanan laporan audit digital.

UCAPAN TERIMA KASIH

Penulis mengucapkan puji dan syukur kepada Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga jurnal yang berjudul "Perancangan Sistem Keamanan Laporan Audit Berbasis Web Menggunakan Enkripsi AES dan Steganografi LSB" dapat diselesaikan dengan baik.

Penulis juga menyampaikan terima kasih kepada semua pihak yang telah memberikan dukungan, bantuan, serta motivasi selama proses penyusunan jurnal ini, baik secara langsung maupun tidak langsung.

Terima kasih disampaikan kepada Risanuri Hidayat yang telah meluangkan waktu untuk membuat template ini.

REFERENSI

[1] Y. J. El Anwar, R. Habibi, and N. Riza, "PENERAPAN METODE KRIPTOGRAFI AES UNTUK MENGAMANKAN FILE DOKUMEN," *Jurnal Tekno Insentif*, vol. 16, no. 2, pp. 92–104, Dec. 2022, doi: 10.36787/jti.v16i2.852.

[2] M. Habib Maulana, M. Tahir, N. Farrohah, F. Maulana, and R. Rurye Aprilianyani, "Jurnal Restikom : Riset Teknik Informatika dan Komputer PERANCANGAN SISTEM KEAMANAN FILE MENGGUNAKAN HYBRID ENCRYPTION UNTUK PERLINDUNGAN DATA," vol. 7, no. 1, pp. 87–96, 2025, [Online]. Available: https://restikom.nusaputra.ac.id

[3] Imron Mohammad and Pratama Aditya, "InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan," vol. 6, 2022, doi: 10.30743/infotekjar.v6i2.4346.

[4] F. C. Maria Baria Set, C. N. Maria Bana, M. Angliadi Anunut, D. Da Costa, and Y. Niis, "Penerapan Steganografi LSB dan Enkripsi AES untuk Keamanan Data Rahasia pada Gambar Digital," *Blantika: Multidisciplinary Jornal*, vol. 3, p. 2025, 2025, [Online]. Available: https://blantika.publikasiku.id/

[5] A. Kautsar and M. Ikhsan, "Sistemasi: Jurnal Sistem Informasi Implementasi Algoritma Advanced Encryption Standard (AES) dan Teknik Steganografi Bit Plane Complexity Segmentation (BPCS) dalam Eskalasi Keamanan File Teks Implementation of the Advanced Encryption Standard (AES) Algorithm and Bit Plane Complexity Segmentation (BPCS) Steganography Technique for Enhancing Text File Security," 2025. [Online]. Available: http://sistemasi.ftik.unisi.ac.id

[6] E. Nirmala, J. Surya, K. No, and T. Selatan, "Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android," 2020, [Online]. Available: http://openjournal.unpam.ac.id/index.php/informatika36

[7] P. G. Subhaktiyasa, "Menentukan Populasi dan Sampel: Pendekatan Metodologi Penelitian Kuantitatif dan Kualitatif," *Jurnal Ilmiah Profesi Pendidikan*, vol. 9, no. 4, pp. 2721–2731, Nov. 2024, doi: 10.29303/jipp.v9i4.2657.

[8] Siska Narulita, Ahmad Nugroho, and M. Zakki Abdillah, "Diagram Unified Modelling Language (UML) untuk Perancangan Sistem Informasi Manajemen Penelitian dan Pengabdian Masyarakat (SIMLITABMAS)," *Bridge : Jurnal publikasi Sistem Informasi dan Telekomunikasi*, vol. 2, no. 3, pp. 244–256, Aug. 2024, doi: 10.62951/bridge.v2i3.174.

[9] Annisa Tri Hidayati, Aditya Eka Widyantoro, and Hertas Jelang Ramadhani, "Perancangan Sistem Informasi Wirausaha Mahasiswa (Siwirma) Berbasis Web dengan Unified Modelling Languange (UML)," *Jurnal Penelitian Rumpun Ilmu Teknik*, vol. 2, no. 4, pp. 86–107, Nov. 2023, doi: 10.55606/juprit.v2i4.2906.

[10] K. Hafidz, M. D. Irawan, and H. D. Nawar, "Sistem Penginputan Data Bahan Pokok pada Pasar Tradisional Sumatera Utara Berbasis Website di Disperindag Sumut," *sudo Jurnal Teknik Informatika*, vol. 1, no. 3, pp. 98–107, Jul. 2022, doi: 10.56211/sudo.v1i3.27.

[11] Aldi Ramadani, "Sistem Informasi Cuti Kepegawaian pada Rumah Sakit Umum Daerah Kabupaten Batu Bara," *Modem : Jurnal Informatika dan Sains Teknologi.*, vol. 3, no. 1, pp. 67–75, Jan. 2025, doi: 10.62951/modem.v3i1.350.

[12] A. Wisandra, P. Saffanah Azzahra, A. Rumah Sakit STIKes Dharma Landbouw Padang, and R. Medis dan Informasi Kesehatan STIKes Dharma Landbouw Padang, "PERANCANGAN SISTEM INFORMASI PENDAFTARAN ONLINE PASIEN RAWAT JALAN PADA PUSKESMAS MENGGUNAKAN METODE PROTOTYPE REGISTRATION INFORMATION SYSTEM DESIGN ONLINE OUTPATIENT AT PUSKESMAS USING PROTOTYPE METHOD," 2023.

[13] M. Na and im Al Jum, "Jurnal Informatika dan Rekayasa Perangkat Lunak Implementasi Steganografi Metode Least Significant Bit (LSB) untuk Menyembunyikan File Pesan dalam Gambar," pp. 102–108, 2024.

[14] M. Rizky Anggara Yunan Putra, B. Putra Aryatama, N. Christiano David, G. Pamungkas, and I. Ady Saputro, "IMPLEMENTASI STEGANOGRAFI UNTUK KEAMANAN JARINGAN TEKNIK TERSEMBUNYI DALAM KOMUNIKASI DATA," 2025. [Online]. Available: https://journal.hasbaedukasi.co.id/index.php/jurmie

[15] S. Puspita Ali and W. Noviani Purwanti, "PENGEMBANGAN APLIKASI WEB STEGANOGRAFI UNTUK KEAMANAN DATA: IMPLEMENTASI DAN ANALISIS KEAMANAN," *Prosiding Seminar Nasional Sains dan Teknologi Seri IV Fakultas Sains dan Teknologi*, vol. 2, no. 2, 2025.

[16] I. Firmansyah, B. Winata, D. Azkia, and R. Ula, "Rancang Bangun Aplikasi Steganografi Berbasis Web Menggunakan Metode Least Significant Bit (LSB) Dan XOR Untuk Enkripsi File Berbasis Citra," 2026.

[17] A. R. Mido, E. Iman, and H. Ujianto, "ANALISIS PENGARUH CITRA TERHADAP KOMBINASI KRIPTOGRAFI RSA DAN STEGANOGRAFI LSB," vol. 9, no. 2, pp. 279–286, 2022, doi: 10.25126/jtiik.202294852.

[18] Zulfiqar Tamin and B. Hendrik, "Penerapan Algoritme Advanced Encryption Standard (AES-128) untuk Mengamankan File Rekam Medis Pasien," *Jurnal KomtekInfo*, pp. 22–30, Mar. 2025, doi: 10.35134/komtekinfo.v12i1.592.

[19] A. P. Indraka and M. A. Romli, "Keamanan Arsip Kelurahan Bumijo Menggunakan Metode Advanced Encryption Standard (AES 128) Berbasis Web," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 5, no. 1, pp. 232–241, Dec. 2024, doi: 10.57152/malcom.v5i1.1728.

[20] L. A. Fitriyani and F. Fachri, "Penerapan Teknik Steganografi dalam Gambar pada Aplikasi Telegram Menggunakan Metode Least Significant Bit (LSB)," *Jurnal Teknologi Informasi dan Multimedia*, vol. 8, no. 2, pp. 357–368, May 2026, doi: 10.35746/jtim.v8i2.1021.