BAB II

TINJAUAN PUSTAKA

2.1. Landasan Teori

2.1.1 Kriptografi

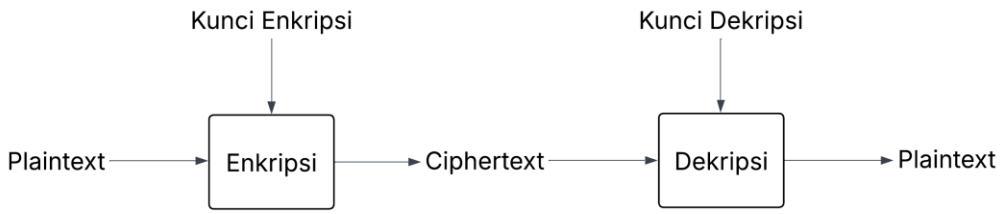
Kriptografi adalah suatu ilmu pengetahuan tentang cara mengamankan atau merahasiakan pesan dengan menggunakan sebuah teknik penyandian (Eka Putri, Kartikadewi dan Abdul Rosyid, 2021). Kriptografi sudah digunakan sejak dahulu bahkan pernah digunakan saat peperangan romawi agar informasi yang dikirim tidak diketahui oleh musuh. Menurut (Munir, 2019), kriptografi secara harfiah memiliki arti tulisan rahasia yang berasal dari Bahasa Yunani di mana "cryptos" berarti rahasia (*secret*) dan "graphein" berarti tulisan (*writing*).

Ada beberapa definisi yang sebelumnya pernah dikemukakan oleh para ahli. Hummady dan Morad mendefinisikan kriptografi sebagai proses mengubah informasi asli menjadi bentuk tak terbaca bagi pihak yang tidak berwenang (Hummady & Hussein Morad, 2022). Sedangkan menurut (Menezes et al., 1996), kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integrasi data, serta autentikasi. Kata seni yang digunakan untuk mendefinisikan kriptografi berasal dari keunikan setiap orang pada zaman dahulu untuk mengamankan atau merahasiakan pesan (Munir, 2019).

Algoritma kriptografi dibagi menjadi dua kelompok utama. Kriptografi *simetri* yaitu kriptografi yang menggunakan satu kunci yang sama untuk proses

enkripsi dan dekripsi, sedangkan kriptografi *asimetrik* menggunakan sepasang kunci, yaitu kunci publik untuk enkripsi dan kunci privat untuk dekripsi (Damrudi & Aval, 2019). AES (*Advanced Encryption Standard*) merupakan salah satu contoh algoritma simetrik yang bekerja pada blok data berukuran 128 bit dan menyediakan tingkat keamanan tinggi (Alanzy et al., 2023). Sebaliknya, RSA (Rivest–Shamir–Adleman) adalah algoritma kriptografi asimetrik yang memanfaatkan kunci publik dan privat untuk mengenkripsi dan mendekripsi pesan (Damrudi & Aval, 2019).

Kriptografi ada 2 proses yang paling penting yaitu proses enkripsi proses dekripsi. Enkripsi merupakan proses untuk mengamankan suatu informasi yang akan dikirim menjadi sebuah informasi yang tidak dapat dikenali, luaran dari proses ini adalah *ciphertext* dan kunci enkripsi. Dekripsi merupakan proses untuk mengubah informasi yang dienkripsi sebelumnya menjadi bentuk awal sebelum proses enkripsi menggunakan kunci enkripsi yang sebelumnya telah dibuat. Berikut ini merupakan alur sederhana proses kriptografi yang disajikan pada Gambar 2.1.



Gambar 2.1 Alur Sederhana Proses Kriptografi

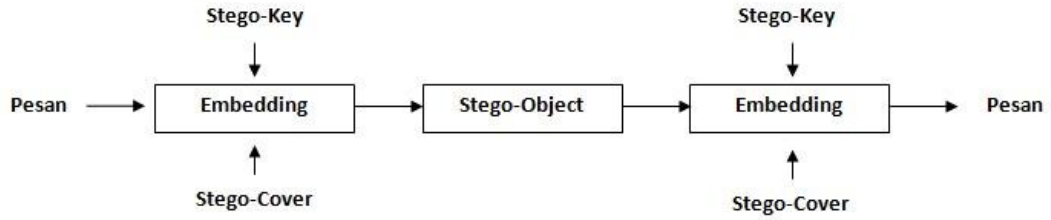
2.1.2 Steganografi

Steganografi merupakan salah satu bagian dari ilmu kriptografi. Konsep dasar di balik steganografi adalah menyembunyikan pesan rahasia dalam data yang

tampak biasa atau tidak mencurigakan (Nabila Alya, Wahidah Hamzah dan Ruriawan, 2022). Menurut (Munir, 2019) steganografi berarti tulisan tersembunyi yang berasal dari Bahasa Yunani di mana "*steganos*" yang artinya tersembunyi dan "*graphien*" yang artinya tulisan. Steganografi memiliki kelebihan di mana pesan yang dikirim tidak menarik perhatian atau kecurigaan dari pihak lain dibandingkan dengan kriptografi.

Steganografi dikategorikan menjadi beberapa jenis berdasarkan penggunaan kunci. Secara garis besar terdapat steganografi murni (tanpa kunci), steganografi kunci rahasia (menggunakan satu kunci bersama), dan steganografi kunci publik (menggunakan pasangan kunci publik-privat) (Damrudi & Aval, 2019). Cara kerja steganografi melibatkan proses menyisipkan pesan rahasia ke dalam media penutup seperti citra, audio, pesan dan video tanpa mengubah secara signifikan tampilan atau karakteristik media tersebut. Proses ini memanfaatkan ketidakpekaan manusia terhadap perubahan kecil dalam data media, misalnya dalam citra, pesan rahasia dapat disisipkan dengan mengubah nilai piksel yang sangat kecil atau tidak terlihat dalam citra asli. Teknik steganografi umumnya dibagi ke dalam domain spasial dan frekuensi. Dalam domain spasial, perubahan langsung dilakukan pada piksel citra, seperti metode *Least Significant Bit* (LSB) atau *Most Significant Bit* (MSB). Domain frekuensi memanfaatkan transformasi citra (misalnya DCT, DWT) untuk menyembunyikan data. Metode LSB dan MSB termasuk teknik domain spasial populer karena mudah diimplementasikan dan kapabilitasnya dalam menyembunyikan pesan tanpa perubahan visual yang

signifikan (Alanzy et al., 2023). Berikut ini merupakan alur sederhana dari cara kerja steganografi yang disajikan pada Gambar 2.2.



Gambar 2.2 Alur Sederhana Proses Steganografi

Salah satu keunggulan paling mencolok dari steganografi adalah tingkat kerahasiaan yang tinggi. Steganografi menyembunyikan pesan rahasia tersembunyi dengan cermat dalam *cover* yang bisa berbentuk citra, teks, audio, atau video, sehingga sulit dideteksi oleh indra manusia atau algoritma komputer tanpa pengetahuan yang tepat. Ini menciptakan lapisan tambahan perlindungan bagi informasi yang ingin disembunyikan, terutama dalam konteks komunikasi rahasia.

2.1.3 Algoritma AES

Algoritma *Advanced Encryption Standard* (AES) atau Algoritma Rijndael adalah salah satu algoritma kriptografi kunci simetris. Algoritma ini awalnya bernama Algoritma Rijndael yang diambil dari nama penemu dan negara asalnya yaitu Vincent **Rij**men da**n** Joan **Dae**men dari Be**l**gia (Munir, 2019). Salah satu kelebihan terbesar dari AES adalah tingkat keamanan yang tinggi yang didasarkan pada kompleksitas algoritma dan kemampuannya untuk mengenkripsi data secara signifikan selama proses enkripsi (Eka Putri, Kartikadewi dan Abdul Rosyid, 2021). Selain dari keamanannya yang sangat baik, AES juga dikenal karena efisiensinya.

Algoritma ini dirancang dengan sangat baik sehingga dapat diimplementasikan dengan mudah pada berbagai jenis perangkat keras dan perangkat lunak.

Sebagai algoritma kriptografi simetris, AES menggunakan kunci yang sama untuk enkripsi dan dekripsi data. Fleksibilitas AES terlihat dalam dukungan terhadap berbagai panjang kunci, termasuk 128-bit, 192-bit, dan 256-bit. Panjang kunci yang lebih besar umumnya dianggap lebih aman, tetapi dengan *trade-off* pada kinerja. Ini memungkinkan pengguna untuk memilih tingkat keamanan yang sesuai dengan kebutuhan mereka, yang sangat penting dalam pengamanan data.

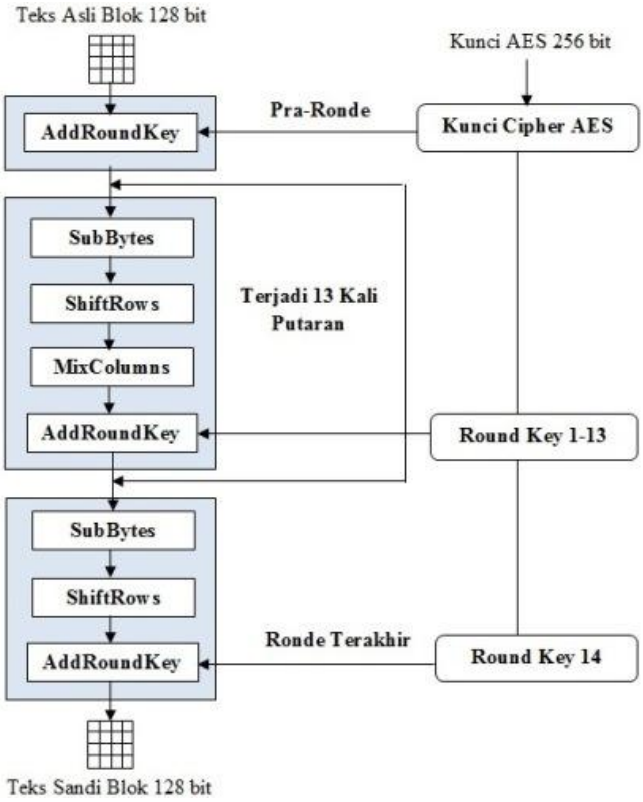
Algoritma AES unggul dalam ketahanan terhadap serangan. Algoritma ini telah dirancang dengan cermat untuk melindungi data dari serangan *Brute Force*, di mana penyerang mencoba semua kemungkinan kunci. Dengan panjang kunci 128-bit pun dibutuhkan 5,4 x 10^{18} tahun untuk mencoba keseluruhan kunci tersebut (Munir, 2019). Dari paparan di atas maka penjelasan mengenai kelebihan dan kekurangan dari Algoritma Rijndael / AES disajikan pada Tabel 2.1.

Tabel 2.1 Kelebihan dan Kelemahan Algoritma AES

Aspek	Kelebihan	Kekurangan
Kecepatan	Proses enkripsi dan dekripsi sangat cepat dan efisien, terutama untuk data yang besar.	Tidak cocok untuk perangkat dengan sumber daya terbatas karena memerlukan komputasi yang cukup tinggi.
Keamanan	AES memiliki tingkat keamanan yang sangat tinggi, bahkan dengan panjang kunci terkecil (128-bit).	Menggunakan kunci simetris, sehingga distribusi kunci harus dilakukan dengan aman.
Kesesuaian	AES mudah diimplementasikan di berbagai platform, baik	Rentan terhadap serangan *side-channel* jika implementasinya

Aspek	Kelebihan	Kekurangan
	perangkat keras maupun perangkat lunak.	tidak benar (seperti serangan *timing*).
Fleksibilitas	Mendukung tiga panjang kunci (128, 192, dan 256 bit), sehingga bisa disesuaikan dengan kebutuhan keamanan.	AES tidak menyediakan mekanisme manajemen kunci, harus ditangani secara eksternal.
Ketahanan	Sangat tahan terhadap serangan *brute force*, bahkan untuk kunci 128-bit.	Tidak memiliki resistensi bawaan terhadap serangan kuantum di masa depan (misalnya menggunakan komputer kuantum).

Cara kerja AES melibatkan serangkaian putaran, di mana setiap putaran terdiri dari empat operasi dasar: *SubBytes, ShiftRows, MixColumns, dan AddRoundKey*. Operasi *SubBytes*, setiap *byte* dalam matriks data dienkripsi digantikan oleh *byte* yang sesuai dalam tabel substitusi *S-box*, yang memberikan tingkat non-linearitas yang penting untuk keamanan AES. *ShiftRows* menggeser *byte* dalam matriks data, memberikan difusi horizontal, sementara *MixColumns* mengubah kolom-kolom dalam matriks, memberikan difusi vertikal. Setiap putaran juga melibatkan penggunaan kunci putaran yang berbeda, dan proses ini diulang sejumlah kali tergantung pada panjang kunci yang digunakan. Berikut ini merupakan diagram sederhana cara kerja algoritma AES dengan kunci 256-bit.



Gambar 2.3 Alur Enkripsi AES 256-bit

2.1.4 Algoritma RSA

RSA adalah algoritma kriptografi kunci asimetris yang ditemukan oleh **R**ivest, **S**hamir dan **A**dleman dari MIT (Munir, 2019). Kriptografi asimetris memiliki dua kunci yaitu, kunci publik yang dapat digunakan oleh siapa saja untuk mengenkripsi pesan, sementara kunci privat hanya diketahui oleh penerima yang sah untuk mendekripsi pesan (Ali Fitriani, 2020). RSA berdasarkan pada matematika teori bilangan, khususnya dalam masalah faktorisasi bilangan prima. Keamanan RSA didasarkan pada kesulitan untuk memfaktorkan produk dari dua bilangan prima yang sangat besar. Proses enkripsi RSA melibatkan pemangkasan pesan asli menjadi blok-blok yang lebih kecil, kemudian setiap blok dienkripsi menggunakan kunci publik penerima, sedangkan dekripsi dilakukan dengan

menggunakan kunci privat. Tabel 2.2 di bawah menyajikan kelebihan dan kekurangan yang dimiliki oleh algoritma RSA.

Tabel 2.2 Kelebihan dan Kelemahan Algoritma RSA

Aspek	Kelebihan	Kelemahan
Keamanan	Menggunakan kunci asimetris (kunci publik dan privat) sehingga lebih aman dibandingkan algoritma simetris.	Keamanan RSA bergantung pada ukuran kunci yang besar, sehingga membutuhkan sumber daya komputasi tinggi.
Manajemen Kunci	Lebih mudah dalam manajemen kunci karena kunci publik dapat dibagikan secara terbuka tanpa mengurangi keamanan.	Proses pembuatan kunci lebih lambat dibandingkan algoritma simetris seperti AES.
Keandalan	RSA tahan terhadap serangan *brute force* karena pemfaktoran bilangan prima yang besar sangat sulit dilakukan.	Rentan terhadap serangan faktorisasi jika ukuran kunci yang digunakan terlalu kecil (misalnya di bawah 1024-bit).
Fleksibilitas	RSA dapat digunakan untuk enkripsi kunci simetris, tanda tangan digital, dan autentikasi data.	Tidak efisien untuk enkripsi data dalam jumlah besar karena proses enkripsinya lebih lambat dibandingkan AES.
Penggunaan	Umum digunakan dalam banyak aplikasi keamanan seperti SSL/TLS, VPN, dan tanda tangan digital.	Memerlukan panjang kunci yang besar untuk menjaga keamanan, yang meningkatkan kebutuhan penyimpanan kunci dan waktu pemrosesan.

2.1.5 Most Significant Bit & Least Significant Bit

Most Significant Bit (MSB) dan *Least Significant Bit* (LSB) merupakan salah satu teknik steganografi yang digunakan untuk menyembunyikan pesan

rahasia dalam media digital (Lutfi et al., 2018). Penyisipan menggunakan metode MSB dan LSB biasanya informasi disisipkan ke dalam nilai piksel *cover image*. Nilai piksel *cover image* berbeda tergantung dari jenis citra yang digunakan, untuk citra *grayscale* nilai nya adalah 1 *byte* (8 *bit*) dengan rentang nilai 0-255 yang direpresentasikan menggunakan bilangan biner dan citra RGB yaitu 3 *byte* dimana tiap *byte* merepresentasikan salah satu warna pada *color space* tersebut (Merah, Hijau, Biru) (Munir, 2019).

Most Significant Bit (MSB) melakukan penyisipan bit pesan terhadap bit yang paling signifikan, misalkan pada bit **0**1010100 (angka yang bergaris bawah merupakan bit yang signifikan) berubah menjadi **1**1010100 setelah dilakukan *embedding*, hasil citra *stego* akan terlihat berubah signifikan karena rentang nilai nya berubah sekitar 128 pada piksel yang dilakukan *embedding*. Berbeda dengan MSB, *Least Significant Bit* (LSB) melakukan penyisipan bit pesan terhadap bit yang kurang signifikan, misalkan pada bit 0101010**0** (angka yang bergaris bawah merupakan bit yang kurang signifikan) berubah menjadi 0101010**1** setelah dilakukan *embedding*, hasil citra *stego* akan terlihat sama secara kasat mata karena rentang nilai nya hanya bertambah 1 terhadap piksel yang dilakukan *embedding*. Perbandingan lebih lengkap antara MSB dan LSB dapat dilihat pada Tabel 2.3.

Tabel 2.3 Perbandingan antara MSB dan LSB

Aspek	**MSB (*Most Significant Bit*)**	**LSB (*Least Significant Bit*)**
Definisi	Bit paling signifikan dalam sebuah byte yang membawa nilai terbesar (biasanya bit pertama dari kiri)	Bit paling tidak signifikan dalam sebuah byte yang membawa nilai terkecil (biasanya bit terakhir dari kanan)

Aspek	MSB (*Most Significant Bit*)	LSB (*Least Significant Bit*)
Posisi Bit	Bit pertama (bit ke-7 dalam byte 8-bit)	Bit terakhir (bit ke-0 dalam byte 8-bit)
Penggunaan dalam Steganografi	Jarang digunakan karena perubahan MSB terlihat jelas dan mengubah nilai keseluruhan secara signifikan	Sangat umum digunakan dalam steganografi karena perubahan LSB tidak mudah terlihat dan tidak memengaruhi kualitas media secara signifikan
Pengaruh terhadap Kualitas Media	Perubahan di MSB akan menghasilkan perbedaan visual atau auditori yang besar dalam citra atau suara	Perubahan di LSB menghasilkan sedikit perubahan, biasanya tidak dapat dilihat atau didengar oleh manusia
Keamanan Penyisipan Data	Tidak aman untuk menyisipkan data karena perubahan bit ini mudah terdeteksi	Lebih aman untuk penyisipan data karena perubahan sulit dideteksi tanpa analisis mendalam
Kapasitas Penyisipan	Kapasitas lebih rendah karena tidak semua bit MSB dapat digunakan tanpa mengubah media secara drastis	Kapasitas lebih tinggi karena bisa menyisipkan bit dalam LSB dari setiap byte tanpa mengurangi kualitas media
Deteksi oleh Steganalisis	Mudah dideteksi karena perubahan MSB memengaruhi nilai byte secara signifikan	Sulit dideteksi karena perubahan LSB hanya memengaruhi nilai byte secara minimal
Efek terhadap Nilai Byte Asli	Mengubah MSB dapat mengubah nilai byte secara drastis, sehingga mengganggu struktur data asli	Mengubah LSB hanya mengubah nilai byte secara kecil (biasanya hanya 1), sehingga data asli tetap hampir tidak berubah
Efisiensi	Kurang efisien untuk menyembunyikan data karena memengaruhi kualitas secara besar	Sangat efisien untuk steganografi karena dapat menyembunyikan data tanpa terlihat secara visual atau auditori

Merujuk dari hasil perbandingan di atas, maka algoritma yang paling cocok digunakan untuk menyembunyikan pesan adalah metode *Least Significant Bit*

(LSB). Alasan pemilihan ini didasarkan pada perubahan yang tidak signifikan terhadap nilai pixel yang disisipkan, setelah dilakukan proses *embedding* citra *stego* terlihat mirip secara kasat mata dibandingkan dengan metode *Most Significant Bit* (MSB).

2.1.6 Base64

Base64 adalah skema pengkodean *binary-to-text* yang mengubah data biner menjadi format teks (menggunakan alfabet [A–Z, a–z, 0–9, +, /] plus padding) sehingga data menjadi lebih mudah ditangani dan ditransfer. Encoding Base64 sering digunakan untuk memastikan data tetap utuh saat dikirim melalui saluran teks (misalnya pada HTTP atau email) dan memudahkan sisipan data biner ke dalam objek lain (Pepić et al., 2024). Base64 bukanlah algoritma enkripsi kriptografi tapi hanya mengonversi format data. Oleh karena itu keamanan sistem tetap bergantung pada algoritma kriptografi lain yang digunakan bersamanya. Sebagai contoh, beberapa metode pertama melakukan enkripsi data (misalnya dengan AES atau RC4) kemudian hasilnya di *encode* dalam Base64 untuk transmisi yang aman

2.1.7 StegExpose

StegExpose merupakan alat steganalisis yang dirancang khusus untuk mendeteksi keberadaan pesan tersembunyi dalam citra digital, khususnya yang menggunakan metode LSB (*Least Significant Bit*). Alat ini dikembangkan dengan pendekatan praktis, memungkinkan analisis massal terhadap file citra lossless seperti BMP dan PNG secara otomatis tanpa supervisi manusia. Keunggulan utama

dari StegExpose adalah kemampuannya dalam menggabungkan beberapa metode deteksi (seperti RS analysis, Sample Pair, Chi-Square, dan Primary Sets) menggunakan teknik *detector fusion* untuk meningkatkan akurasi deteksi, baik melalui *standard fusion* maupun *fast fusion* (Boehm, 2014) .

Standard fusion menggunakan rata-rata aritmatika dari hasil semua detektor dan terbukti memiliki akurasi tertinggi berdasarkan nilai AUC (Area Under Curve), mengungguli detektor individual seperti RS analysis. Sementara itu, *fast fusion* dirancang untuk efisiensi waktu dengan tetap mempertahankan akurasi yang mendekati *standard fusion*. Strategi ini sangat berguna dalam skenario forensik nyata, di mana file bersih jauh lebih banyak daripada file yang mengandung pesan tersembunyi. Oleh karena itu, StegExpose tidak hanya relevan secara akademik, tetapi juga bermanfaat dalam praktik analisis forensik digital secara besar-besaran

Dalam implementasinya, StegExpose dikembangkan menggunakan Java dan tersedia secara *open source*. Program ini menghasilkan dua jenis laporan: *standard report* untuk output sederhana di konsol dan *full report* dalam format CSV yang mencakup data detail dari setiap detektor. Selain itu, pengguna dapat mengatur parameter seperti mode deteksi (*standard* atau *fast*) serta ambang batas (*threshold*) untuk menyesuaikan kebutuhan analisis antara akurasi dan kecepatan

2.1.8 PSNR & MSE

Dalam evaluasi kualitas citra hasil steganografi, dua metrik utama yang sering digunakan adalah *Mean Squared Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR). MSE merupakan rata-rata kuadrat selisih nilai piksel antara citra asli

dan citra stego. PSNR adalah ukuran logaritmik dari rasio nilai puncak (maksimum) piksel terhadap kesalahan (MSE). PSNR yang lebih tinggi (dan MSE lebih rendah) menandakan citra stego sangat mirip dengan citra asli (perbedaan visual minimal). Sebagai pedoman umum, Nilai PSNR di rentang 30-40 dB menunjukkan kualitas citra yang dapat diterima sedangkan nilai PSNR lebih dari 40 dB menunjukkan kualitas stego yang sangat baik dengan perbedaan yang nyaris tak terlihat (Adeshina et al., 2025).

Dalam konteks steganografi, MSE dan PSNR berperan penting untuk menilai *imperceptibility* (tingkat ketidakterbedaan). MSE menghitung degradasi rata-rata, sedangkan PSNR menguantifikasi tingkat distorsi relatif. Misalnya, (Naz & Zade, 2022) melaporkan nilai PSNR 71 dB untuk citra stego berukuran 512 x 512 dan 37 dB untuk citra berukuran 256 x 256 setelah dilakukan proses steganografi, kedua nilai tersebut masuk ke dalam kategori nilai PSNR yang baik.

2.1.9 Entropi

Entropi informasi merupakan ukuran ketidakpastian atau derajat keacakan dalam sekumpulan data. Secara teori informasi, entropi Shannon mendefinisikan tingkat *surprise* (informasi tak terduga) dalam kejadian acak. Dalam konteks kriptografi, entropi sering digunakan untuk mengukur kekuatan kunci kriptografi. Kunci dengan entropi tinggi (mendekati distribusi seragam) sulit diprediksi atau diterka oleh penyerang. Sebagai contoh, (Zolfaghari et al., 2022) menekankan bahwa entropi kunci telah menjadi ukuran keamanan kriptografi selama puluhan

tahun. Dengan kata lain, semakin tinggi entropi kunci, semakin kuat sistem kriptografi tersebut.

Dalam domain steganografi, entropi digunakan untuk menganalisis seberapa banyak proses penyisipan data mengubah konten citra. Menurut sistem penilaian statistik, citra dengan entropi tinggi memiliki distribusi pixel acak tinggi. Penurunan entropi setelah *embedding* dapat mengindikasikan pola tersembunyi atau kerusakan pada tekstur alami citra. (Rahman et al., 2025) juga mencatat bahwa *information entropy* biasanya dipakai untuk mengevaluasi keamanan metode steganografi, karena metode steganografi yang aman umumnya mempertahankan keacakan citra tinggi. Dengan demikian, entropi tinggi setelah steganografi menunjukkan *embedding* yang minimal mengganggu pola acak citra, sedangkan penurunan entropi mengindikasikan pola baru yang bisa mempermudah deteksi.

2.1.10 Algoritma Hash SHA-256

SHA-256 adalah salah satu fungsi hash kriptografi dalam keluarga SHA-2 (Standar NIST), yang menghasilkan nilai hash sepanjang 256 bit untuk setiap pesan masukan apa pun (Franck et al., 2024). Secara umum, fungsi hash kriptografi dirancang satu-arah mudah dihitung tetapi sulit dibalik. SHA-256 dipatenkan oleh NIST pada tahun 2002 dan hingga sekarang masih banyak dipakai dalam sistem keamanan modern. SHA-256 memenuhi persyaratan keamanan penting: tahan tabrakan (*collision-resistant*), tahan *preimage*, dan tahan *second-preimage* (Łeska & Furtak, 2025). Artinya, sulit untuk menemukan dua pesan berbeda yang menghasilkan hash sama, atau untuk menemukan pesan asli hanya dari hash nya.

SHA-256 banyak digunakan untuk menjaga integritas data dan pada tanda tangan digital. Dalam skema tanda tangan RSA atau ECDSA, misalnya, pesan pertama-tama di-hash dengan SHA-256, lalu hash tersebut yang ditandatangani secara kriptografis. Penggunaan SHA-256 memastikan bahwa setiap perubahan data apa pun mengubah hash, sehingga merusak validitas tanda tangan. Selain itu, SHA-256 digunakan luas di berbagai aplikasi keamanan: pengesahan perangkat lunak (*software signing*), protokol TLS untuk enkripsi saluran komunikasi, pembuatan sidik jari (*fingerprint*) data, hingga *blockchain* seperti Bitcoin yang memanfaatkan SHA-256 sebagai bagian dari *proof-of-work* (Vaughn & Borowczak, 2024). Karena kekuatan kriptografisnya, NIST bahkan menganjurkan penggunaan minimal SHA-256 (atau SHA-3) untuk aplikasi apa pun yang memerlukan interoperabilitas keamanan tinggi. Dengan sifat tersebut, SHA-256 memperkuat sistem keamanan modern: menghasilkan *digest* unik untuk setiap data (menjaga keutuhan/integritas), serta menyediakan basis untuk autentikasi dan tanda tangan digital yang sulit dibajak

2.2. Penelitian Terkait dan Kebaruan Penelitian

2.2.1 Penelitian Terkait (*State Of The Art*)

Tabel 2.4 *State Of The Art* Penelitian

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
1	Enhanced Security: Implementation of Hybrid Image Steganography Technique using Low-Contrast LSB and AES-CBC Cryptography	(Jacinto et al., 2022)	AES-CBC & LSB	Penelitian ini menggabungkan AES-CBC dengan LSB pada area citra berkontras rendah. Keunggulan penelitian ini terletak pada pemanfaatan area yang sulit terdeteksi oleh mata manusia maupun analisis statistik, sehingga memperkuat penyembunyian pesan. Namun, kelemahannya adalah penggunaan AES-CBC yang tidak mendukung autentikasi data, membuat sistem masih rentan terhadap manipulasi. Berbeda dengan pendekatan AES-GCM, metode ini tidak memberikan jaminan integritas data.
2.	Analisa Keamanan Data Teks Dengan Menerapkan Kriptografi RSA dan Steganografi LSB	(Ali Fitriani, 2020)	RSA & LSB	Penelitian ini menggunakan kombinasi RSA dan LSB. Metode ini kuat dalam hal penyebaran kunci karena RSA bersifat asimetris. Namun, RSA murni tanpa kriptografi simetris tidak efisien untuk data besar dan tidak memberikan perlindungan terhadap integritas. Pendekatan hibrida yang menggabungkan RSA untuk pengelolaan kunci dan AES-GCM untuk

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
				enkripsi data dapat memberikan efisiensi dan keamanan yang lebih baik.
3	Good Performance Images Encryption Using Selective Bit T-Des On Inverted Lsb Steganography	(Sari et al., 2019)	T-DES & 4-LSB	Penelitian ini mengusulkan T-DES dengan LSB terbalik. Penelitian ini unggul dari segi efisiensi waktu dan menghasilkan citra stego berkualitas tinggi (PSNR > 50 dB). Sayangnya, T-DES memiliki kelemahan dalam keamanan kriptografi modern dan tidak menyertakan pengelolaan kunci yang kuat. Alternatif algoritma seperti AES-GCM dapat memberikan keamanan yang lebih modern dan tangguh.
4	Implementasi Kriptografi Algoritma RC4 Dan 3DES Dan Steganografi Dengan Algoritma EOF Untuk Keamanan Data Berbasis Desktop Pada SMK AS-SU'UDIYYAH	(Basim & Painem, 2020)	RC4 (*Ron's Code 4*), 3DES (*Triple Data Encryption Standard*), dan Steganografi EOF (*End Of File*)	Penelitian ini mengombinasikan RC4, 3DES, dan steganografi EOF. Kelebihannya adalah fleksibilitas implementasi dalam desktop. Namun RC4 telah lama dianggap usang karena kelemahan keamanannya, dan steganografi EOF lebih mudah dideteksi dibanding LSB. Pemilihan algoritma dan teknik steganografi yang lebih mutakhir dapat meningkatkan ketahanan sistem terhadap deteksi dan serangan.

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
5	Aplikasi Steganografi Pengamanan Data Nasabah di Standard Chartered Bank Menggunakan Metode Least Significant Bit dan RC4	(Syahril & Jaya, 2019)	RC4 & LSB	Penelitian ini menggunakan LSB dan RC4 untuk data nasabah. Metode ini berhasil melindungi data, tetapi RC4 memiliki banyak celah keamanan yang telah diekspos dalam berbagai studi. Penggunaan algoritma modern seperti AES-GCM memberikan penguatan keamanan terhadap berbagai jenis serangan kriptografis.
6	Implementasi Steganografi LSB dengan Enkripsi Vigenere Cipher pada Citra	(Laila & Sindar RMS, 2018)	Vignere Chiper & LSB	Penelitian ini mengombinasikan Vigenere Cipher dan LSB. Pendekatan ini sederhana dan cukup aman untuk kebutuhan dasar, namun algoritma kriptografi klasik seperti Vigenere rentan terhadap analisis frekuensi. Algoritma kriptografi modern lebih direkomendasikan untuk menjawab kebutuhan keamanan masa kini.
7	Steganografi LSB Dengan Modifikasi Kriptografi: Caesar, Vigenere, Hill Cipher Dan Playfair Pada Image	(Claudy Frobenius & Hidayat S H S, 2020)	Caesar, Vigenere, Hill, Playfair & LSB	Penelitian ini menggabungkan beberapa kriptografi klasik dengan LSB berbasis mobile. Kelebihannya terletak pada keragaman teknik kriptografi, namun kompleksitas tidak menjamin keamanan tinggi, terutama karena semua algoritma yang digunakan bersifat klasik dan rentan. Pendekatan berbasis algoritma modern menawarkan tingkat perlindungan yang lebih optimal.

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
8	Implementasi Kriptografi *Secret Sharing Scheme* dan Steganografi Audio Least Significant Bit (LSB*)*	(Firjan Humaira et al., 2023)	*Secret Sharing Scheme* & LSB	Peneltian ini menggunakan skema secret sharing dan LSB pada audio. Teknik ini unggul dalam perlindungan berbasis distribusi, namun implementasi terbatas pada media audio dan belum mencakup proteksi data dalam konteks integritas pesan. Kombinasi teknik kriptografi dan steganografi pada media citra dengan enkripsi autentikasi dapat memberikan cakupan yang lebih luas.
9	Implementasi Algoritma OTP Dan Steganografi EOF Dalam Penyisipan Pesan Teks Pada Citra	(Arief, Simanjuntak dan Prahmana, 2022)	OTP & EOF	Penelitian ini menggabungkan OTP dan steganografi EOF. OTP memberikan keamanan kuat secara teori, namun sulit dalam praktik karena keharusan distribusi kunci yang panjang dan acak. RSA dapat menjadi solusi untuk manajemen kunci yang lebih praktis dan aman.
10	Implementasi Penyisipan Pesan Teks Terenkripsi Menggunakan Kriptografi ElGamal pada Citra Digital Menggunakan Steganogarafi LSB	(Saragih et al., 2023)	El Gamal & LSB	Penelitian ini menerapkan ElGamal dan LSB, yang efektif dalam mengamankan pesan, namun ElGamal tidak secepat AES dan tidak menyediakan autentikasi. Alternatif seperti AES-GCM memberikan keunggulan dari segi efisiensi dan integritas data.

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
11	Implementasi Steganografi LSB dengan Enkripsi Base64 Pada Citra dengan Ruang Warna CMYK	(Al Isfahani & Nugraha, 2020)	Base64 & LSB	Penelitian ini menggunakan Base64 dan LSB pada gambar CMYK. Kelebihan metode ini adalah format data lebih mudah dikendalikan. Namun Base64 bukan algoritma kriptografi dan hasil ekstraksi mudah dikonversi kembali ke bentuk asli. Penggunaan enkripsi yang sebenarnya akan memberikan perlindungan yang lebih baik terhadap kerahasiaan data.
12	Teknik Algoritma ElGamal Dan Steganografi *First Of File* (FOF) Untuk Penyisipan Pesan Dalam Citra	(Hidayat et al., 2022)	ElGamal & FOF	Penelitian ini menggabungkan ElGamal dan steganografi FOF. Metode ini cukup kuat namun lebih lambat dan FOF kurang efektif dibanding LSB dalam menyembunyikan data tanpa terlihat. Teknik LSB dengan algoritma enkripsi efisien lebih disarankan dalam konteks performa dan penyembunyian.
13	Implementasi Algoritma Caesar Cipher Dan Steganografi *Least Significant Bit* Untuk File Dokumen	(Yusup et al., 2020)	Caesar Cipher & LSB	Penelitian ini menggunakan Caesar Cipher dan LSB untuk dokumen. Pendekatan ini sangat terbatas karena hanya mampu mengenkripsi huruf A–Z dan mudah dipecahkan. Penggunaan algoritma kriptografi modern dengan cakupan karakter lebih luas dan tingkat keamanan lebih tinggi sangat dibutuhkan.

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
14	Pengamanan Teks Terenkripsi Dengan Algoritma RC4+ Dan Steganografi DCS Pada Citra Digital	(Lase, 2021)	RC4+ & DCS	Penelitian ini memadukan RC4+ dan DCS. Meski DCS efektif dalam menyamarkan keberadaan teks, RC4+ tetap tidak cukup kuat secara kriptografi modern. Kombinasi algoritma yang lebih kuat dan tahan terhadap serangan kontemporer dapat meningkatkan keamanan sistem.
15	Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Kombinasi Multi Bit LSB Dengan Hill Cipher	(Hamrul et al., 2022)	Hill Cipher & LSB	Penelitian ini menggunakan Hill Cipher dan multi-bit LSB. Teknik ini meningkatkan kapasitas penyisipan namun PSNR menurun seiring banyaknya data. Hill Cipher juga memiliki kelemahan terhadap serangan matriks. Pendekatan yang seimbang antara kapasitas, keamanan, dan kualitas citra sangat penting.
16	A Secure Image Steganography using LSB and Double XOR Operations	(Ahmed & Ahmed, 2020)	Double XOR & LSB	Penelitian ini menggunakan Double XOR dan LSB. Metode ini sederhana dan memberikan hasil yang dapat diterima, tetapi keamanan XOR sangat terbatas dan dapat ditebak. Algoritma yang lebih kompleks dan tahan terhadap serangan modern dapat memberikan perlindungan lebih baik.

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
17	Secure Mobile Computing Authentication Utilizing Hash, Cryptography and Steganography Combination	(Alotaibi et al., 2019)	Hash, AES, LSB	Penelitian ini menggabungkan Hash, AES, dan LSB untuk autentikasi mobile. Penelitian ini mendekati pendekatan hibrida modern, namun tidak menjelaskan bagaimana distribusi kunci dilakukan. Penambahan RSA atau skema asimetris lain dapat melengkapi kekurangan tersebut.
18	Hide Image And Text Using LSB, DWT And RSA Based On Image Steganography	(Bhargava & Mukhija, 2019)	LSB, DWT, RSA	Penelitian ini menggunakan LSB, DWT, dan RSA. Teknik ini kuat dari sisi embedding karena memanfaatkan DWT, namun belum menyediakan autentikasi data. Enkripsi yang mendukung autentikasi seperti AES-GCM dapat memperkuat aspek integritas pesan.
19	Image Steganography Using LSB and Hybrid Encryption Algorithms	(Alanzy et al., 2023)	AES, Blowfish, LSB	Penelitian ini menggunakan AES, Blowfish, dan LSB. Metode ini sangat kuat karena hybrid encryption dan segmentasi pesan, namun belum menyertakan digital signature atau autentikasi eksplisit. Kombinasi AES-GCM dan RSA dapat menutup celah tersebut.
20	A Secure Image Steganography Using Improved LSB Technique And Vigenere Cipher Algorithm	(Voleti et al., 2021)	Vigenere & LSB	Penelitian ini menggunakan Vigenere dan LSB. Keamanan dasar sudah tercapai namun tetap rentan karena Vigenere dapat dipecahkan dengan serangan klasik. Kriptografi modern tetap lebih unggul dalam menjaga kerahasiaan dan integritas data.

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
21	**Implementasi Kriptografi Hibrida AES-GCM Dan RSA Untuk Meningkatkan Keamanan Steganografi LSB (Usulan Penelitian)**	**(Muammar Farhan Londjo, 2025)**	**AES-GCM, RSA, dan LSB**	Penelitian ini menunjukkan bahwa kombinasi AES-GCM dan RSA dapat meningkatkan keamanan pesan yang akan disisipi ke dalam steganografi LSB. AES-GCM memberikan *confidentiality* dan *integrity* melalui autentikasi, RSA menyelesaikan masalah distribusi kunci. Hasil eksperimen membuktikan bahwa metode ini mempertahankan kualitas visual citra dengan nilai PSNR 46db pada citra berukuran 5000x3000 dengan plaintext berukuran 2857KB, nilai entropi meningkat secara signifikan, 100% meningkatkan ketahanan terhadap manipulasi ciphertext dan tahan terhadap serangan visual maupun statistik.

2.2.2 Matriks Penelitian

Tabel 2.5 Matriks Penelitian

No	Judul Penelitian	Ruang Lingkup penelitian																			
		Metode Enkripsi															Metode Steganografi				
		Base 64	Caesar Cipher	Hill Cipher	Playfair	Vigenere	OTP	Double XOR	AES	ElGamal	RC4	RSA	SSS	3DES	T-DES	Blowfish	DWT	EOF	FOF	LSB	DCS
1	Enhanced Security: Implementation of Hybrid Image Steganography Technique using Low-Contrast LSB and AES-CBC Cryptography (Jacinto et al., 2022)								✓											✓	
2	Analisa Keamanan Data Teks Dengan Menerapkan Kriptografi RSA dan Steganografi LSB (Ali Fitriani, 2020)											✓								✓	
3	Good Performance Images Encryption Using Selective Bit T-Des On Inverted Lsb Steganography (Sari et al., 2019)													✓	✓					✓	
4	Implementasi Kriptografi Algoritma RC4 Dan 3DES Dan Steganografi Dengan Algoritma EOF Untuk Keamanan Data Berbasis Desktop (Basim & Painem, 2020)										✓			✓				✓			

No	Judul Penelitian	Ruang Lingkup penelitian																			
		Metode Enkripsi															Metode Steganografi				
		Base 64	Caesar Cipher	Hill Cipher	Playfair	Vigenere	OTP	Double XOR	AES	ElGamal	RC4	RSA	SSS	3DES	T-DES	Blowfish	DWT	EOF	FOF	LSB	DCS
5	Enhanced Security: Implementation of Hybrid Image Steganography Technique using Low-Contrast LSB and AES-CBC Cryptography (Syahril & Jaya, 2019)										✓									✓	
6	Implementasi Steganografi LSB dengan Enkripsi Vigenere Cipher pada Citra (Laila & Sindar RMS, 2018)					✓														✓	
7	Steganografi Lsb Dengan Modifikasi Kriptografi: Caesar, Vigenere, Hill Cipher Dan Playfair Pada Image (Claudy Frobenius & Hidayat S H S, 2020)		✓	✓	✓	✓														✓	
8	Implementasi Kriptografi *Secret Sharing Scheme* dan Steganografi Audio Least Significant Bit (LSB*)* (Firjan Humaira et al., 2023)												✓							✓	

No	Judul Penelitian	Ruang Lingkup penelitian																			
		Metode Enkripsi															Metode Steganografi				
		Base 64	Caesar Cipher	Hill Cipher	Playfair	Vigenere	OTP	Double XOR	AES	ElGamal	RC4	RSA	SSS	3DES	T-DES	Blowfish	DWT	EOF	FOF	LSB	DCS
9	Implementasi Algoritma OTP Dan Steganografi EOF Dalam Penyisipan Pesan Teks Pada Citra (Arief et al., 2022)						✓											✓			
10	Implementasi Penyisipan Pesan Teks Terenkripsi Menggunakan Kriptografi ElGamal pada Citra Digital Menggunakan Steganogarafi LSB (Saragih et al., 2023)									✓										✓	
11	Implementasi Steganografi LSB dengan Enkripsi Base64 Pada Citra dengan Ruang Warna CMYK (Al Isfahani & Nugraha, 2020)	✓																		✓	
12	Teknik Algoritma ElGamal Dan Steganografi *First Of File* (FOF) Untuk Penyisipan Pesan Dalam Citra (Hidayat et al., 2022)									✓									✓		

No	Judul Penelitian	Ruang Lingkup penelitian																			
		Metode Enkripsi															Metode Steganografi				
		Base 64	Caesar Cipher	Hill Cipher	Playfair	Vigenere	OTP	Double XOR	AES	ElGamal	RC4	RSA	SSS	3DES	T-DES	Blowfish	DWT	EOF	FOF	LSB	DCS
13	Implementasi Algoritma Caesar Cipher Dan Steganografi *Least Significant Bit* Untuk File Dokumen (Yusup et al., 2020)		✓																	✓	
14	Pengamanan Teks Terenkripsi Dengan Algoritma RC4+ Dan Steganografi DCS Pada Citra Digital (Lase, 2021)										✓										✓
15	Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Kombinasi Multi Bit LSB Dengan Hill Cipher (Hamrul et al., 2022)			✓																✓	
16	A Secure Image Steganography using LSB and Double XOR Operations (Ahmed & Ahmed, 2020)							✓												✓	
17	Secure Mobile Computing Authentication Utilizing Hash, Cryptography and Steganography Combination (Alotaibi et al., 2019)								✓											✓	

No	Judul Penelitian	Ruang Lingkup penelitian																			
		Metode Enkripsi															Metode Steganografi				
		Base 64	Caesar Cipher	Hill Cipher	Playfair	Vigenere	OTP	Double XOR	AES	ElGamal	RC4	RSA	SSS	3DES	T-DES	Blowfish	DWT	EOF	FOF	LSB	DCS
18	Hide Image And Text Using LSB, DWT And RSA Based On Image Steganography (Bhargava & Mukhija, 2019)											✓					✓			✓	
19	Image Steganography Using LSB and Hybrid Encryption Algorithms (Alanzy et al., 2023)								✓							✓				✓	
20	A Secure Image Steganography Using Improved LSB Technique And Vigenere Cipher Algorithm (Voleti et al., 2021)					✓														✓	
21	**Implementasi Kriptografi Hibrida AES-GCM Dan RSA Untuk Meningkatkan Keamanan Steganografi LSB (Usulan Penelitian)**								✓			✓								✓	

Kebaruan penelitian ini terletak pada kombinasi yang belum dieksplorasi sebelumnya yaitu menggabungkan algoritma enkripsi **AES-GCM 256 bit, RSA 4096 bit, dan Steganografi LSB**. Pendekatan ini menawarkan keamanan berlapis yang lebih kuat dibandingkan penelitian sebelumnya yang hanya menggunakan satu algoritma enkripsi atau tidak mengamankan kunci enkripsi secara terpisah. Kombinasi ini menghasilkan sebuah solusi yang lebih aman untuk melindungi pesan rahasia dalam citra digital, baik dari serangan kriptografi maupun deteksi steganografi.