# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi dalam dua dekade terakhir telah membawa dampak besar terhadap cara manusia berinteraksi, berkomunikasi, dan berbagi informasi. Dengan adanya jaringan internet yang semakin luas dan cepat, pertukaran data digital dalam bentuk teks, gambar, audio, maupun video menjadi semakin mudah dan efisien. Namun, kemudahan ini juga diiringi dengan meningkatnya risiko terhadap keamanan data. Informasi yang dikirim melalui jaringan publik berpotensi disadap, dimodifikasi, atau bahkan dicuri oleh pihak yang tidak bertanggung jawab. Oleh karena itu, isu mengenai keamanan data digital menjadi salah satu fokus utama dalam bidang teknologi informasi modern (Alanzy et al., 2023).

Terdapat dua pendekatan utama dalam menjaga keamanan data digital, yaitu kriptografi dan steganografi. Kriptografi merupakan teknik pengamanan data dengan cara mengubah bentuk informasi menjadi kode atau ciphertext yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Metode ini berfungsi untuk menjaga kerahasiaan isi pesan, namun tetap memperlihatkan bahwa ada komunikasi yang sedang berlangsung. Sebaliknya, steganografi merupakan seni dan ilmu menyembunyikan pesan rahasia ke dalam media lain (seperti gambar, audio, atau video) sehingga keberadaan pesan tersebut tidak terdeteksi oleh pengamat (Rizqa et al., 2022). Dengan kata lain, jika kriptografi melindungi isi pesan, maka steganografi melindungi keberadaan pesan itu sendiri. Kombinasi antara kriptografi dan steganografi sering dianggap sebagai solusi yang efektif untuk meningkatkan keamanan komunikasi digital.

Salah satu teknik steganografi yang paling populer dan banyak digunakan adalah *Least Significant Bit* (LSB). Teknik LSB bekerja dengan mengganti bit paling tidak signifikan dari piksel dalam gambar untuk menyisipkan data rahasia.

Karena perubahan pada bit paling rendah tidak menyebabkan perubahan besar pada tampilan visual gambar, maka hasil citra steganografi (*stego image*) akan tampak identik dengan gambar aslinya bagi mata manusia (Set et al., 2025). Keunggulan metode LSB adalah prosesnya sederhana, mudah diimplementasikan, dan memiliki kapasitas penyimpanan pesan yang relatif besar.

Namun, metode ini memiliki kelemahan utama yaitu ketahanan terhadap serangan (*robustness*) yang rendah (Kautsar & Ikhsan, 2025). LSB sangat sensitif terhadap perubahan kecil pada gambar, seperti kompresi, rotasi, scaling, atau cropping. Perubahan-perubahan tersebut dapat menyebabkan sebagian atau seluruh pesan yang disembunyikan menjadi rusak dan tidak dapat diekstraksi kembali dengan benar. Hal ini berbeda dengan metode lain seperti *Spread Spectrum* yang lebih tahan terhadap gangguan namun memiliki kompleksitas yang lebih tinggi (Herri Setiawan et al., 2023).

Salah satu bentuk serangan yang sering terjadi terhadap gambar digital adalah *cropping attack*, yaitu pemotongan sebagian area gambar. Cropping bisa dilakukan secara sengaja untuk menghilangkan sebagian informasi atau secara tidak sengaja saat pengguna mengubah ukuran gambar. Dalam konteks steganografi, cropping dapat menghapus sebagian bit yang menyimpan data rahasia, sehingga pesan yang disembunyikan menjadi tidak utuh atau bahkan hilang seluruhnya (Qiao et al., 2023).

Untuk mengatasi kelemahan tersebut, diperlukan pendekatan yang tidak hanya mengandalkan penyembunyian pesan tetapi juga memperkuat keamanan isi pesan itu sendiri. Salah satu cara yang umum digunakan adalah mengombinasikan steganografi dengan algoritma enkripsi kriptografi seperti *Advanced Encryption Standard* (AES). AES merupakan algoritma kriptografi simetris yang sangat populer dan diakui keamanannya secara internasional. Dengan demikian, meskipun pesan rahasia berhasil diekstraksi oleh pihak yang tidak berwenang, isi pesan tersebut tetap tidak akan terbaca tanpa kunci AES yang benar (Firdaus & Rahmatulloh, 2025).

Kombinasi antara metode LSB dan AES membentuk pendekatan yang disebut LSB-AES, yang menawarkan dua lapisan keamanan. Pendekatan ini telah banyak diteliti dan terbukti mampu meningkatkan keamanan data tersembunyi. Namun, sebagian besar penelitian tersebut masih terbatas pada pengujian kualitas visual atau keberhasilan ekstraksi dalam kondisi ideal (Halim & Wulan Sri Lestari, 2023). Belum banyak penelitian yang secara khusus menganalisis sejauh mana metode LSB-AES mampu bertahan terhadap *cropping attack*, yaitu serangan yang secara fisik memotong sebagian piksel citra stego.

Selain aspek keamanan, faktor kapasitas penyimpanan juga menjadi aspek penting dalam penelitian steganografi. Kapasitas mengacu pada seberapa besar jumlah data rahasia yang dapat disembunyikan di dalam media penampung tanpa menurunkan kualitas visual citra secara signifikan. Dalam metode LSB, semakin banyak bit yang digunakan untuk menyembunyikan pesan, semakin besar kapasitasnya (Ren & Wu, 2024). Namun hal ini juga meningkatkan risiko penurunan kualitas gambar dan mempermudah deteksi. Oleh karena itu, penelitian ini juga berfokus pada analisis kapasitas penyimpanan pesan dalam metode LSB-AES.

Penelitian mengenai Analisis Kapasitas dan Ketahanan Steganografi LSB-AES terhadap *Cropping Attack* ini menjadi penting karena dapat memberikan kontribusi dalam pengembangan metode keamanan data digital yang lebih kuat dan efektif. Dengan melakukan analisis terhadap kapasitas penyimpanan serta ketahanan terhadap serangan pemotongan gambar, penelitian ini diharapkan mampu memberikan gambaran komprehensif mengenai kelebihan dan keterbatasan metode LSB-AES berdasarkan berbagai temuan penelitian sebelumnya..

## 1.2 Identifikasi Masalah

Berdasarkan uraian pada latar belakang, dapat diidentifikasi beberapa masalah yang mendasari penelitian ini, yaitu:

1. Keamanan data pada jaringan publik rentan terhadap serangan jika hanya mengandalkan satu lapisan perlindungan.
2. Metode steganografi LSB murni memiliki ketahanan (*robustness*) yang rendah, di mana manipulasi fisik seperti *cropping* dapat merusak struktur bit pesan secara permanen.
3. Penggunaan enkripsi AES membutuhkan integritas data yang tinggi untuk proses dekripsi, yang bertolak belakang dengan dampak serangan *cropping* yang menghilangkan data.
4. Kurangnya analisis empiris mengenai ambang batas persentase *cropping* yang menyebabkan kegagalan total proses dekripsi pada kombinasi metode LSB-AES.

### 1.3 Rumusan Masalah

Berdasarkan identifikasi masalah di atas, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana merancang dan mengimplementasikan aplikasi steganografi teknik LSB yang dikombinasikan dengan algoritma enkripsi AES pada citra digital untuk mengamankan kerahasiaan pesan?
2. Berapa kapasitas maksimum pesan yang dapat disisipkan tanpa menurunkan kualitas visual citra di bawah standar kelayakan (PSNR > 30 dB) yang umumnya dijadikan acuan kualitas citra stego?
3. Bagaimana pengaruh serangan *cropping* dengan variasi posisi dan rasio pemotongan tertentu terhadap tingkat keberhasilan dekripsi pesan (*decryption success rate*) pada data yang dienkripsi AES?
4. Bagaimana dampak serangan *cropping* terhadap kualitas citra hasil steganografi (*stego-image*) yang tersisa berdasarkan parameter objektif *Peak Signal-to-Noise Ratio* (PSNR) dan *Mean Squared Error* (MSE)?

### 1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Menghasilkan implementasi perangkat lunak steganografi LSB dengan pengamanan enkripsi AES-256.
2. Menganalisis kapasitas tampung pesan 10 KB pada citra berukuran 512x512 piksel terhadap nilai *imperceptibility* (PSNR) guna membuktikan efektivitas kualitas visual citra *stego*..
3. Mengevaluasi pengaruh lokasi geometris pemotongan piksel (*Top-Left* vs *Center*) terhadap integritas *Initialization Vector* (IV) dan dampaknya terhadap keberhasilan dekripsi algoritma AES.
4. Mengevaluasi penurunan kualitas visual citra stego pasca-serangan cropping dengan mengukur parameter objektif Peak Signal-to-Noise Ratio (PSNR) dan Mean Squared Error (MSE).

### 1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Penelitian ini dapat menjadi referensi tambahan dalam bidang keamanan data digital, khususnya mengenai kombinasi steganografi dan kriptografi.
2. Penelitian ini dapat menjadi acuan bagi pengembang sistem keamanan informasi dalam menerapkan metode LSB-AES untuk melindungi data rahasia.
3. Hasil analisis dapat membantu menentukan batas kapasitas optimal dan ketahanan metode LSB-AES terhadap serangan cropping untuk aplikasi nyata.
4. Penelitian ini dapat memberikan kontribusi dalam pengembangan metode steganografi yang lebih tangguh terhadap manipulasi citra digital.

### 1.6 Batasan Masalah

Untuk memfokuskan penelitian ini agar lebih terarah, maka batasan masalah yang diterapkan adalah sebagai berikut:

1. Media penampung (*cover image*) yang digunakan adalah citra digital berformat BMP atau PNG agar tidak terjadi kompresi lossy.
2. Teknik steganografi yang digunakan adalah *Least Significant Bit* (LSB).
3. Algoritma enkripsi yang digunakan adalah *Advanced Encryption Standard* (AES) dengan kunci simetris.
4. Serangan yang diuji dalam penelitian ini terbatas pada cropping attack dengan variasi ukuran pemotongan tertentu.
5. Analisis yang dilakukan meliputi kapasitas penyimpanan pesan, ketahanan terhadap cropping, dan kualitas citra yang diukur menggunakan nilai PSNR dan MSE.