Term	What It Means
AES (Advanced Encryption Standard)	A symmetric encryption algorithm that uses the same key for encryption and decryption. AES-256 is extremely secure and fast for large data.
ECC (Elliptic Curve Cryptography)	An asymmetric encryption method. It provides strong security with smaller key sizes (256-bit ECC ≈ 3072-bit RSA). Used for secure key exchange.
DWT (Discrete Wavelet Transform)	A mathematical transform that decomposes an image into frequency bands (LL, LH, HL, HH). Embedding data in high-frequency bands makes it less noticeable.
DCT (Discrete Cosine Transform)	Converts spatial domain data (pixels) into frequency domain. Modifying mid-frequency coefficients hides data while preserving image quality.
ACO (Ant Colony Optimization)	A bio-inspired optimization algorithm that mimics ants finding paths. Used here to adaptively choose the best embedding positions in an image.
Chaotic Pseudo-Random Generator	Uses chaotic mathematical maps (e.g., Logistic Map) to generate random embedding positions, adding unpredictability.
Huffman Coding	A compression algorithm that reduces data size by assigning shorter codes to frequent elements. Saves space for more payload.
PSNR (Peak Signal-to-Noise Ratio)	Measures image quality. Higher PSNR (>50dB) means changes are imperceptible to human eyes.
SSIM (Structural Similarity Index)	Measures similarity between original and stego image. SSIM > 0.98 means almost no perceptible difference.
NPCR (Number of Pixels Change Rate)	Tests robustness by checking how much the image changes when slight modifications are made. High NPCR means stronger security.
UACI (Unified Average Changing Intensity)	Measures average intensity changes between original and modified images. High UACI means better resistance to attacks.

Our proposed framework addresses these gaps with a **hybrid system**:

✅ **Hybrid AES-ECC Cryptography:**

- AES-256 encrypts the message or file for high-speed security.
- ECC encrypts the AES key to securely exchange it between sender and receiver.

✅ **Huffman Compression:**

- Reduces the size of encrypted payloads to allow higher capacity embedding.

✅ **Adaptive DWT+DCT Embedding:**

- DWT decomposes the image into sub-bands.
- DCT operates on high-frequency bands to embed data.
- **ACO** or **chaotic maps** adaptively choose embedding locations, making detection by CNN/GNN steganalyzers very difficult.

✅ **High-Performance Targets:**

Metric	Target Value
PSNR	> 50 dB
SSIM	> 0.98
Payload Capacity	30–50% of image size
Encryption Time	≤ few seconds
Robustness (NPCR/UACI)	Very High

✅ **Functional Application:**
Supports **secure text messaging and file transfer** in a **/16 LAN network (Windows OS)**, scalable for internet/server deployment.

Feature	Existing Solutions	Limitations	Your Proposed System
Encryption	AES-only or no encryption.	AES protects payload, but key exchange often insecure.	✅ **Hybrid AES-256 + ECC** for secure payload encryption and key exchange.
Embedding Technique	Simple LSB (Least Significant Bit), DWT or DCT only.	Vulnerable to steganalysis and visual/statistical attacks.	✅ **Adaptive DWT+DCT** multi-transform embedding for higher security.
Embedding Positions	Fixed or predictable pixel positions.	Easier for CNN/GNN steganalyzers to detect patterns.	✅ **ACO or Chaotic Pseudo-Random** embedding to randomize positions.
Payload Capacity	~10–20% of image size.	Limited capacity due to fear of noticeable changes.	✅ **30–50% of image size** with Huffman compression optimization.
Robustness	Poor against compression, noise, cropping.	Attacks degrade hidden data integrity.	✅ Resistant to **compression, noise, and cropping** due to transform-domain embedding and adaptive placement.
Support for File Transfer	Text-only or static payloads.	Does not support embedding full files.	✅ Supports **secure text messaging and file transfer** (small files embedded covertly).
Network Application	No support for LAN/Internet covert communication.	Mostly offline stego tools.	✅ Designed for **/16 LAN network (Windows OS)**, scalable to Internet/server.