Research Contribution

This work proposes an integrated, defense-in-depth security framework that jointly combines:

- **Entropy-aware hybrid encryption**
- **Post-quantum key encapsulation**
- **Frequency-domain, multi-channel steganography**

The **novelty is not any single algorithm**, but **how these components are *co-designed* and *orchestrated*** to address limitations of existing isolated solutions.

This integrated architecture is **not present in prior literature**, which typically treats encryption, steganography, and post-quantum security as **separate problems** rather than a unified pipeline.

2. Specific Novel Contributions

Contribution 1: Entropy-Driven Adaptive Encryption (New Design Choice)

Your system **dynamically selects the encryption strength based on Shannon entropy of the plaintext**, instead of applying uniform encryption.

- Low-entropy content → lightweight poly-alphabetic cipher
- High-entropy content → AES-256
- Session keys → Kyber768 (post-quantum safe)

Why this is new:

- Existing selective encryption focuses on *media semantics* (e.g., video frames, objects).
- Your work applies **information-theoretic entropy at the text/token level**, which is **lighter, deterministic, and content-agnostic**.

This directly addresses inefficiency and over-encryption in prior static systems.

Contribution 2: Post-Quantum Steganographic Pipeline (Rare in Literature)

While post-quantum cryptography is well studied, **embedding PQ-secured ciphertext inside a covert image channel** is still underexplored.

Your contribution:

- Uses **Kyber768 only for key encapsulation**, not bulk data
- Prevents *store-now-decrypt-later* attacks

- Keeps steganographic payload quantum-resilient **without heavy computational overhead**

Why this matters:
Most steganographic systems assume classical adversaries. Your work **explicitly anticipates quantum adversaries**, which is forward-looking and aligns with current cryptographic transition research.

Contribution 3: Split-Payload, Multi-Channel Frequency Embedding (Structural Novelty)

Your system **splits ciphertext into logical segments** (header, body, metadata) and embeds them **across RGB frequency channels**.

This provides:

- Reduced statistical detectability
- Fault tolerance if partial payload is corrupted
- Resistance against monolithic steganalysis

What's new here:
Prior work either:

- Embeds payload monolithically, or
- Uses multiple images (batch steganography)

Your approach performs **intra-image distribution across spectral channels**, which is **lighter than batch methods and more resilient than single-channel embedding**.

Contribution 4: Lightweight Texture-Adaptive Masking Without Deep Learning

Instead of CNNs or GANs:

- You use **DCT variance thresholding**
- Embed only in high-texture blocks
- Guarantee imperceptibility with deterministic rules

Why this is important:

- Avoids training cost and hardware dependency
- Suitable for real-time or constrained environments
- Still robust against modern steganalysis due to frequency-domain randomness

This positions your work as a **practical alternative to heavy generative steganography**.

Contribution 5: Deterministic, Key-Seeded Sparse Randomized Sampling

Your embedding locations are:

- Randomized
- Non-linear
- **Deterministically reproducible using the encryption key**

Novelty:
This tightly couples **cryptographic secrecy with embedding topology**, meaning:

- Without the key, both *content* and *location* are unrecoverable
- Improves resistance against pattern-learning steganalyzers