**Paper Title:**

Privacy-Preserving Image Watermark Embedding Method Based on Edge Computing

**Paper Link:** https://ieeexplore.ieee.org/document/9712284

1.Summary

**1.1 Motivation/purpose/aims/hypothesis:**

The motivation behind this research arises from the pressing need to address privacy and latency challenges in outsourced image watermark embedding within cloud computing. With the traditional reliance on centralized cloud processing posing privacy risks, the motivation is to introduce edge computing to minimize data exposure, ensuring a secure and efficient watermark embedding process.

**1.2 Contribution:**

This research contributes a novel watermark embedding method that integrates perturbing encryption with homomorphism, edge computing, and a secure framework for singular value decomposition. The primary contribution lies in providing a practical solution to privacy concerns and latency issues associated with cloud-centric approaches. The proposed method not only preserves user privacy but also minimizes response latency, aligning with the evolving landscape of cloud and edge computing.

**1.3 Methodology:**

The methodology involves the integration of perturbing encryption techniques with homomorphism, leveraging edge computing for decentralized processing. The secure framework for singular value decomposition ensures that the original image matrix cannot be recovered by the edge server. This combination forms a robust watermark embedding method that operates efficiently in an outsourced environment while preserving privacy.

**1.4 Conclusion:**

The paper presents a timely and relevant solution to the challenges of privacy and latency in outsourced image watermark embedding. The proposed method, as demonstrated through experiments, surpasses comparable schemes in encryption/decryption time and ciphertext expansion. The integration of edge computing ensures a secure watermarking operation, making it superior to traditional cloud-based approaches.

2. Limitations

**2.1 First limitations / Critique:**

The first limitation lies in the intricate balance between privacy and computation efficiency. Striking an optimal equilibrium is essential to avoid compromising either aspect, requiring a nuanced approach in the design and implementation of the watermark embedding method.

**2.2 Second limitations / Critique:**

The second limitation pertains to the adaptability of the proposed method to dynamic and resource-constrained environments. Ensuring seamless integration and efficient operation in diverse settings remains a challenge that warrants exploration.

**3. Synthesis:**

The paper navigates the complex terrain of privacy, latency, and efficiency in the context of outsourced image watermark embedding. By introducing edge computing and overcoming the outlined limitations, the proposed method synthesizes a practical and robust solution that not only preserves user privacy but also aligns with the evolving landscape of digital content processing.