International Conference on Engineering, Trends in Engineering,
Science, Humanities and Management (ICETESHM – 2024)
31st March, 2024, Karlo Bagh, New Delhi, India.

CERTIFICATE NO: ICETESHM /2024/ C0324315

An Overview of Existing Image Steganography for Wireless Communication

Maid Mukund Devidasrao

Research Scholar, Ph.D. in Electronics,
Mansarovar Global University, Bilkisganj, Sehore, M.P.

ABSTRACT

Image steganography is a crucial technique for secure wireless communication, allowing confidential data to be embedded within images to prevent unauthorized access. Traditional methods include Least Significant Bit (LSB) substitution, discrete cosine transform (DCT), and discrete wavelet transform (DWT), each balancing capacity, imperceptibility, and robustness. LSB is widely used due to its simplicity and high payload capacity but is vulnerable to attacks like statistical analysis. Transform domain techniques such as DCT and DWT provide better resistance against compression and noise but often compromise embedding capacity. Recent advancements integrate deep learning and chaotic encryption to enhance security and detectability. Convolutional neural networks (CNNs) and generative adversarial networks (GANs) are now employed to automate and optimize steganographic embedding, improving imperceptibility and robustness. In wireless communication, where bandwidth and security are major concerns, adaptive steganographic techniques that consider network conditions are being developed. Challenges include ensuring resilience against steganalysis, maintaining high image quality, and reducing computational overhead. Future research focuses on hybrid models combining artificial intelligence with traditional techniques to enhance efficiency and security. As wireless communication expands, robust image steganography will play an essential role in securing sensitive information while ensuring minimal transmission disruption.