National Conference on Recent Advances in Engineering, Technology, Science, Management and Humanities (NCRAETSMH – 2025)

23rd February, 2025, Nagpur, Maharashtra, India.

CERTIFICATE NO : NCRAETSMH /2025/C0225103

A Study of Steganography with Cryptography to Determine for Secure Communication

Maid Mukund Devidasrao

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

ABSTRACT

Steganography and cryptography are two powerful techniques used together to enhance secure communication. Cryptography transforms data into an unreadable format using encryption algorithms, ensuring that only authorized users can access it. However, encrypted data can attract attention from attackers. To address this, steganography hides encrypted data within digital media, such as images, audio, or video, making it undetectable to unauthorized parties. Combining both methods strengthens security. First, cryptographic techniques like AES (Advanced Encryption Standard) or RSA encrypt the message. Then, steganographic methods, such as Least Significant Bit (LSB) substitution, Discrete Cosine Transform (DCT), or Discrete Wavelet Transform (DWT), embed the encrypted data within a carrier file. This dual-layer security ensures that even if the hidden data is detected, decryption requires a key, making unauthorized access nearly impossible. For wireless communication, where data transmission is vulnerable to interception, this hybrid approach provides robust security against eavesdropping and cyber threats. Modern advancements integrate artificial intelligence (AI) and blockchain to further enhance security and detect anomalies. As cyber threats evolve, the fusion of steganography with cryptography remains a crucial strategy for safeguarding sensitive information in digital and wireless communication networks.