Steganography is defined as the invisible communication between two communicating parties. For hiding communicated data many carrier file formats are present but the most commonly used are images. The data can be hidden by using Least Significant Bit (LSB), k-Modulus Method (k-MM), Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). The LSB and k-MM algorithms are implemented under spatial domain in which secret data is directly embedded in the bits of cover image whereas the DCT and DWT algorithms are under transform domain in which firstly images are transformed and then the message is embedded in the image. The comparison and performance of these techniques depend upon different parameters: MSE (Mean Squared Error), PSNR (Peak Signal to Noise Ratio), BER (Bit Error Rate), Capacity. This paper explains the different Steganography techniques for hiding the information in an image.

References

Exploring the Techniques of Data Embedding in Images: A Review


Index Terms

Computer Science

Security
Keywords

LSB  DCT  DWT  MSE (Mean Squared Error)  PSNR (Peak Signal to Noise Ratio)
BER (Bit Error Rate)

Steganography.