

## ABSTRACT

In today's Internet era, secure data communication is vital and indispensable. Image steganography is one of the most popular and widely used techniques to protect valuable information from illegitimate access. The quality of the stego image obtained from any steganographic scheme is inversely proportional to its data hiding capacity. This poses a challenge for the prospective researcher to balance a good trade-off among the quality of stego image, embedding capacity and robustness. Moreover, it is not only the extraction of the secret message from stego image but, the reconstruction of the original image from stego is also of paramount importance for many human centric applications such as tactical communication, health care, e-governance, commercial security, and intellectual property rights etc. In the last two decades, researchers around the globe have tried to resolve these problems to some extent but have not achieved a significant level of success. In order to overcome these issues, some new image steganographic schemes have been designed in spatial domain. These schemes maintain a good balance between stego image quality, embedding capacity and robustness.

Two single image based steganographic schemes have been designed and implemented using graph neighbourhood, and pixel value difference. These schemes produce good quality stego image along with high embedding capacity. To increase the embedding capacity, robustness and to achieve reversibility, some dual image based steganographic schemes have been designed using graph neighbourhood and weighted matrix. In these schemes, the use of dual image and image interpolation techniques help to increase the data hiding capacity, improve visual quality and enhance the security.

To strengthen the robustness under compressed environment, some novel steganographic schemes have been developed in transform domain using Discrete Cosine Transform and Discrete Wavelet Transform. To encounter the extent of distortion to the coefficient of transform domain, a weighted matrix is introduced to maintain good trade-off between quality and robustness.

Further, some standard steganalysis techniques have been used to examine the proposed methods and tested under some steganographic attacks to analyze the robustness of the schemes because designing a new scheme is not enough, rather the analysis of its impact in terms of security and robustness is very much important that would determine whether it can be advocated globally or not.