ABSTRACT

Data hiding has emerged as a major research area due to the phenomenal growth in internet and multimedia technologies. Securing data transmitted over the internet becomes a challenging issue caused by the advancement in data digitization and communication networking over the past decade. Data hiding schemes have been increasingly adopted to protect digital media content. Data hiding involves concealing confidential data within another seemingly innocuous host media or cover media such as text, video, audio, images, and compression coding. The embedded data can then be used as authentication codes for protecting intellectual copyrights or as confidential data for sharing information. Steganography will be chosen if secure communication is the objective; in addition, Watermarking should be considered if copyright protection is the objective. However, in those techniques, permanent destruction of the cover media is normally inevitable, even after the embedded data is extracted. Some trivial applications like medical diagnosis, geographic maps, military maps and remote sensing insist on restoring the cover image perfectly. Hence, reversible data hiding techniques are used to restore the cover media without distortion in such sensitive applications.

The reversible data hiding techniques can be broadly classified according to the domain in which the secret payload is embedded as spatial domain, frequency domain and compressed domain techniques. The spatial domain techniques modify the intensity values of the pixels in the cover image, whereas the frequency domain techniques modify the frequency coefficients of the cover image. The compressed domain techniques embed the secret data into the compressed codes of the original cover images.
A good reversible data hiding scheme is characterized by the possession of attributes like reversible, imperceptible, high payload capacity and robustness. By reversible, it is meant both the extraction of the payload as well as the restoration of the host image perfectly from the stego image. Secondly, the imperceptible factor ensures the stego image resemblance against the cover/host image. The payload capacity measures the maximum size of the payload that can be embedded into a given host image without or with minimal perceptible distortions. Finally, robustness count for the ability to sustain the secret payload against both intentional and unintentional attacks. In this research work, three algorithms have been proposed to enhance imperceptibility, robustness, embedding capacity and reversibility of the reversible data hiding techniques.

The first algorithm embeds data into cover image in spatial domain using edge-oriented Gaussian weighted predictor. The proposed algorithm utilizes the information redundancy that exists in the color channels to estimate the edges. The edge detectors namely, Sobel, Laplacian of Gaussian and Canny are used for detecting edges in cover images. Among these detectors, the canny detector provides more space to embed data at the cost of large variations in the pixel values. Hence it offers less PSNR compared to other detectors. However, it provides an optimal solution to the edge detection problem, especially in the presence of noise. The prediction error is weighted using Gaussian function. Genetic algorithm is used to optimize the prediction parameters. The performance of edge-oriented Gaussian weighted predictor (GWP) is compared with Median edge detection (MED) predictor and Gradient adjusted predictor (GAP). As the edge-oriented GWP provides sharper prediction error, the payload capacity is higher compared to other predictors. The data embedding is performed by expanding the GWP if the prediction error lies within pre-defined threshold; otherwise, histogram shifting method is used to embed data. The embedded payload is highly
imperceptible as the Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) are higher.

The second algorithm focuses on the two optimality criteria, namely robustness and reversibility. The frequency domain strategy is applied due to its superior performance over the spatial domain techniques in certain important aspects like robustness and reversibility towards signal processing and image processing operations. Accordingly, the rotation, scaling and translation properties of the Radon transform and reversibility property of integer lifting transform have been joined together in a hybrid formation. The performance of this combination is also examined and compared with the other existing works in literature. As the Radon transform performs rotation, scaling and translation operations on the cover image, it changes the locations of the secret bits. Hence, it is very difficult to detect the embedded data without taking the inverse Radon transform and subsequently it increases the security of the embedded payload.

The integer lifting wavelet transform guarantees complete reversibility as they produce integer wavelet coefficients. As the approximate coefficients contribute to visual perception of the image, the secret data is embedded in detail coefficients. The original bits in the selected bit plane are compressed using arithmetic coding to provide space for embedding the payload bits. The middle bit planes are used for embedding as they provide a balanced trade-off between embedding capacity and visual quality of the embedded image. The performances of various orthogonal and bi-orthogonal wavelet families in the lifting domain under fixed and varying secret payload are investigated. As the proposed framework embeds data in red, green and blue channels, it can work well for a variety of images with different distribution of colors. When the image intensity is projected at different
angles in radon domain, the perceptual quality of the embedded image also gets changed.

The third algorithm aims to increase the payload capacity as well as robustness as opposed to the former belief that robustness would have to be compromised for better payload. Robustness of data hiding techniques can be enhanced if the properties of the cover image could be properly used. Hence, the cover image has been transformed into time-frequency domain using Fractional Fourier Transform (FrFT) and the optimal pixel locations for hiding the secret data are found by using Firefly algorithm. The optimal locations are found by using the multi-objective function which is the combination of SSIM and Bit Error rate (BER). The objective function for firefly algorithm is fixed in such a way that both quality and robustness of the embedded image are within an acceptable value. The histogram shifting technique is used to embed secret data in the optimal pixel locations. The quality of test images is analyzed under varying payload at constant as well as varying fractional order (rotation angle). It is found that using FrFT, high visual quality as well as robustness can be obtained for the same amount of embedding rate as that of other transforms.

When the embedded images are transmitted through a communication channel, they get corrupted due to various intentional and unintentional attacks. From the simulation results, it has been observed that all the three proposed algorithms are more robust and reversible against various attacks as they have lower bit error rate and higher normalization coefficient.