ABSTRACT

The use of images, text and video has become inevitable in today’s rapidly advancing and growing digital world. It has been greatly assisted by the contributions of information technology in bringing about state of the art high speed and secure transmission and reception systems. Content transmission through e-mails, hard media like hard disk drives (HDD), compact discs (CD), digital video discs (DVD) etc., have made things simpler, safer and faster. Digital images can be captured easily with scanners, digital cameras and camcorders, and transmitted easily over the Internet. As a result, digital images appear widely in the internet and the World Wide Web (WWW). However, this advance has also brought the problem such as copyright protection for content providers. Many unauthorized activities like illegal tampering of data, illegal broadcast monitoring, attacks in an attempt to destroy the underlying content are becoming more prevalent. Digital watermarking is one of the proposed solutions for copyright protection of multimedia. Data hiding is an age old technique used to hide data in an image. Considerable researches are going on in this area to protect the hidden data from unauthorized access.

Apart from its normal applications, data hiding has had a new dimension since the introduction of tele based services like tele Medicine, tele diagnosis etc., which have introduced medical image processing to the arena of data hiding. With the advent of tele based services, numerous merits have been reported like cutting down of transportation time of patient to meet the doctor or hospital, cutting down of cost due to internet based transmission and reception and also efficient patient monitoring and treatment due to systematic and methodological secured storage of the patient information in the hospital’s data base for future access.
Data hiding takes many forms like visible, invisible, robust, fragile etc., since, the proposed word is focused towards an efficient algorithm to aid in hospital management of patient data, an invisible and robust data hiding scheme is proposed. The goal of this thesis is to establish a satisfactory tradeoff between the three optimality criteria namely robustness, visual imperceptibility and embedding capacity. This work also focuses on embedding multiple watermarks in the same cover image. The robustness of the watermarks is tested by exposing the watermarked image to various attacks and its performance is analyzed. The work also focuses on the behavior of both spatial and frequency domain techniques towards a noisy channel. This analysis would prove to be an effective platform upon which advanced data embedding in Medical Images can be accomplished.

Several works have been reported in the past in the area of data hiding introducing many techniques either as lone techniques or joint techniques in an attempt to achieve optimality and good results have been reported or studied. The contribution of this work consists of three main parts: An application-specific robust hybrid transform domain multiple watermarking schemes is introduced in the first part to mainly target the medical images and its performance over other existing techniques is justified. The second part of the work involves utilizing the embedding capacity enhancing properties of histogram based difference expansion technique and studying the impact of increasing payload with respect to image quality. The last part of the work involves integrating the first two phases or modules and testing the three optimality criteria after being exposed to a wide range of image processing operations equivalent to real time intentional and unintentional attacks.

Experimental results indicate that the reversible data hiding scheme out performs other approaches in the literature in terms of payload capacity and marked image quality. Results from the robustness evaluation also show that no major degradation in performance is noticeable which is highly desired in medical data embedding.
applications for medical data management. Significant conclusions have been made at the end of this entire work which could aid in further scope of data hiding to be taken to new heights.