ABSTRACT

In healthcare industry like teleradiology, telesurgery and telediagnosis, traditional diagnosis is being replaced by e-diagnosis, with the development of latest technologies in the areas of communication and computer networks. The requirement of these applications is to exchange the medical images in digital format from one location to another in a secured manner.

The objective of the research is to provide secure communication of medical images through the wired and wireless media. In the initial phase of the research work, one level security is achieved by embedding patient's information using different watermarking schemes. In the second phase for further enhancing the security of medical image transmission and retrieval, two level security is achieved by joint watermarking and encryption methods.

ROI of medical image, contains all important information. From diagnosis point of view, ROI should not be altered by any further operations and need reversibility. ROI is subjected to reversible

watermarking and NROI undergoes robust watermarking. So, three level security is performed which increases the reversibility and robustness of the medical image when compared to two level security.

The effectiveness of the data integrity and authenticity is evaluated by computing the speed of the data transmission by various transmission protocols. If the transmission speed is less, the data is less prone for attacks. The medical images are subjected to ten different attacks. The performance of the different security algorithm is investigated by some quality measures.

In the initial phase of research work, multiscale approach to medical image watermarking is performed using three approaches. In the first approach, a fragile image authentication scheme based on multiple watermarking is proposed for Digital Imaging and Communications in Medicine (DICOM) images using Discrete Wavelet Transform (DWT). The robustness of the method is enhanced through a form of hybrid coding, which includes repetitive embedding of BCH (Binary Coded Hexadecimal) encoded watermarks. In the second approach, double watermarks such as Electrocardiograph (ECG) signal and Patients demographic text ID is watermarked by wavelet and Embedded Zero tree Wavelet (EZW) algorithm. The third approach is based on hash function, Independent Component Analysis (ICA) and Integer Wavelet Transform (IWT).

The major drawback of one level security is that the medical image during transmission cannot withstand various attacks. In this research, an attempt is made to provide two level securities for medical images using watermarking and encryption. Watermarking is performed by using a new non-tensor product wavelet filter banks, which has the ability to reveal singularities in different directions. A natural image is taken as an original image because it avoids the attention of the attackers and the medical image is taken as a watermark image.

In Tri level security, medical images are partitioned by three different partitioning techniques. This increases the reversibility and robustness of the medical image when compared to two level security. In the first approach, the partitioning technique segments the medical image into background and foreground. From the foreground image, Digital Envelope (DE) is generated and embedded into the background of the image. Finally, the embedded images are encrypted. The TAF value is calculated between embedded DE and extracted DE. The original PSNR and TAF values calculated. It is then transmitted separately to the receiver. Then the digital signature, TAF and PSNR values calculated from the received decrypted image and it is compared with the original values.

In second approach, the medical images are partitioned into two parts ROI and NROI. ROI is subjected to reversible watermarking and

NROI undergoes robust watermarking. Then the watermarked images are encrypted. This assures that the content of the original ROI image is not altered. In NROI region, robust watermarking is done in the wavelet domain.

In third approach, the medical image is partitioned into six shares using Shamir's secret sharing method. Then the shared images are embedded into six different natural images, which do not attract eaves' droppers' attention. Then the embedded natural images are encrypted by a self adaptive wave algorithm. Then the speed of transmission of images is measured by different protocols with wired and wireless media.

In this research work, four different modules are proposed with different methodologies of watermarking and encryption algorithms to enhance the security of medical images. One level security provides confidentiality and integrity, but watermarked medical images cannot withstand various attacks. In joint watermarking and encryption, method provides security, authentication and integrity and can also withstand various attacks. This method alters the ROI and makes it irreversible. From the diagnosis point of view, this method fails. Three level security increases the reversibility and robustness of the medical images. The effectiveness of the data integrity and authenticity is evaluated by computing the speed of the data transmission by various transmission protocols.