10

Storage and Transmission of Cardiac Data with Medical Images

U. Rajendra Acharya, P. Subbanna Bhat, U. C. Niranjan, Sathish Kumar, N. Kannathal, Lim Choo Min and Jasjit Suri

The landscape of healthcare delivery and medical data management has significantly changed over the last years, as a result of the significant advancements in information and communication technologies. Complementary and/or alternative solutions are needed to meet the new challenges, especially regarding security of the widely distributed sensitive medical information. Digital watermarking is a technique of hiding specific identification data for copyright authentication.

The DICOM standard is one method to include demographic information, such as patient information and X-ray exposure facilities, in image data. The DICOM standard is a standard that can be used regularly to record demographic information onto the image data header section. Regarding DICOM format images, information on patients and X-ray exposure facilities can be obtained easily from them. On the other hand, general-purpose image formats, such as the JPEG format, offer no standard that can be used regularly to record demographic information onto the header section.

Digital watermark technologies [1–8] can be used to embed demographic information in image data. Digital watermarking have several other uses, such as fingerprinting, authentication, integrity verification purposes, content labeling, usage control and content protection [9, 10]. The efficient utilization of bandwidth of communication channel and storage space can be achieved, when the reduction in data size is done. Recently, Giakoumaki *et al*, have presented a review of research in the area of medical-oriented watermarking and proposed a wavelet-based multiple watermarking scheme. This scheme aimed to address critical health information management issues, including origin and data authentication, protection of sensitive data, and image archiving and retrieval [11]. Their experimental results on different medical imaging modalities demonstrated the efficiency and transparency of the watermarking scheme.

The digital watermarking technique is adapted in this chapter for interleaving patient information with medical images, to reduce storage and transmission overheads. The text data is encrypted before interleaving with

images to ensure greater security. The graphical signals are compressed and subsequently interleaved with the image. Differential pulse code modulation and adaptive delta modulation techniques are employed for data compression as well as encryption and results are tabulated for a specific example. Adverse effects of channel induced random errors and burst errors on the text data are countered by employing repetition code, Hamming code and R-S code techniques.

10.1 Concept of Interleaving

With the present trend of using internet as a medium to transmit images and patient data, it is of utmost importance to preserve authenticity of patient information. Exchange of data between hospitals involves large amount of vital patient information such as bio-signals, word documents and medical images. Therefore, it requires efficient transmission and storage techniques to cut down cost of health care. Interleaving one form of data such as 1-D signal, or text file, over digital images can combine the advantages of data security with efficient memory utilization [12]. In this present chapter, the watermarking technique is adapted for interleaving text and graphical signals with medical images (Fig. 10.1).

The watermarking techniques are divided into two basic categories:

- Spatial domain watermarking, in which the least significant bit (LSB) of the image pixels are replaced with that of the *watermark* (authentication text).
- Frequency domain watermarking, in which the image is first transformed to the frequency domain by discrete fourier transform (DFT), discrete cosine transform(DCT) and then the low frequency components are modified to contain the authentication text [13,14]. Since high frequencies will be lost by compression or scaling, the watermark signal is applied to the lower frequencies or applied adaptively to frequencies that contain important information of the original picture. Since watermarks applied to the frequency domain will be dispersed over the entirety of the image upon inverse transformation, this method is not susceptible to defeat by cropping as in the spatial domain.

Many authors have proposed the schemes to protect the ownership rights through the watermarking [12,15–19]. Swanson *et al*, have proposed the robust

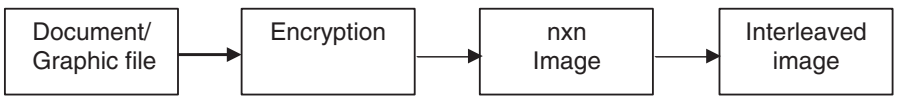

Fig. 10.1. Scheme for data storage