Chapter 25
Implementation of a Reversible Watermarking Technique for Medical Images

Ranit Karmakar
Tata Consultancy Services, India

Abhishek Basu
RCC Institute of Information Technology, India

ABSTRACT

Electronic health records (EHR) contain patients' medical as well as personal details. With the increased use of digital media, these data are stored and transferred through the electronic media all over the world. This makes it vulnerable to unauthorized people. Digital image watermarking can be a useful process of protecting these data from attacker but causes severe and unrecoverable damage to cover media. In the case of highly sensitive images like medical images, this might creates a problem during further diagnosis. In this chapter, a reversible data hiding algorithm is proposed which also is capable of holding a large chunk of data without affecting the cover media. The main cover image is first reconstructed and hidden behind a bigger media and then the extra pixels are used to hide encrypted forms of EHR data along with an authentication signature. As EHR data and the digital signature is passed through various encryption stages while encoding, it is made more secure. The algorithm is developed on the spatial domain adding some cautious measures which made it fragile as well.

INTRODUCTION

The history of imaging dates back in 1826 when a Frenchman Joseph Nicéphore Niépce was able to produce the first picture in the human history, a view through his window. Using the lithographic technique and 8 hours exposure to light, it was possible to capture the first image. Later that century a lot of work has been done for the improvement but it wasn't until late twentieth century when digital imaging was developed. This gave a cheaper and easier solution to the old film-based methods used in photography. In

DOI: 10.4018/978-1-6684-7544-7.ch025

the 1960s, the digital image processing has become a large area of interest in different research facilities around the globe, especially for the applications in satellite imagery, wire-photo standards conversion, medical imaging, videophone, character recognition, and photograph enhancement. However, the cost of processing was fairly high because of low-quality computer equipment available in that era. The scenario soon started changing with the advancement in computer science and in the 2000s, digital images and signal processing have become the most common form of image processing for different applications.

The internet boom of the late 90s and early 2000 allowed this digital media to float all around the globe in real-time. With improvements in technology and digital devices, the amount of digital data started increasing exponentially. A recent paper by IDC, Data Age 2025, predicts that by the year 2025, our world will have 163 ZB (Zetta Byte) of data, almost 10 times than what we have today. But most alarmingly, it suggests that 90% of this data will require some form of security and only about half of this will have it. So, security has become a big concern. For the purpose of securing digital images from different attacks and data theft, a new technique was introduced, named Digital Watermarking. The term digital watermarking was first coined by Andrew Tirkel and Charles Osborne in December 1992 and soon after in 1993 was demonstrated in their paper Electronic Water Mark. Although, watermarking content for IP protection is in use from 13th century, its application in digital media is relatively recent.

- **Digital Watermarking Life-Cycle:** The watermarking of a digital signal is distributed in three steps, Embedding, Attacking and Detecting. In the embedding stage, the watermark signal is embedded under the cover signal or host signal. After transmitting this signal, it may gone through some attacks such as compression, cropping, addition of noise etc. This is known as the attack stage. In the last stage, the watermark signal is tried to be recovered. If the recovered signal is unaltered, it proves that the host signal is not affected anyway. The digital watermarking can be classified in the following ways:
  - **Robustness:** A watermarking algorithm can be called as robust if it can withheld different attacks and transformations. Whereas a fragile watermarking algorithm is easily destroyed with slight modification on the mail signal.
  - **Perceptibility:** Perceptibility deals with the understanding of the signal. If the signal is perceptually indistinguishable even after applying the watermark, it is called perceptible.
  - **Capacity:** Differentiated in two different methods zero-bit and multiple-bit, as the name suggests, capacity determines the size of watermark signal that can be hidden under the host or cover signal.

One of the most widely used application of digital signal processing is on medical images. Medical images contain very sensitive data and can be easily manipulated. Without proper protection, these images are highly vulnerable. The information infrastructure system of modern health care is formed by HIS (Hospital Information System), and its special cases of RIS (Radiology Information System), PACS (Picture Archiving and Communication System). These digitization and recent developments in information and communication technology provide in fact new ways to store, access and distribute medical data. It introduces new practices for the profession, as well as the patient themselves by accessing to their own medical files. Over many advantages these techniques are vulnerable in protecting the Electronic Health Records (EHR), and highly personal documents shared in the open network. The systematized collection of patient and population electronically-stored health information in a digital format is known as Electronic Health Record (EHR), or Electronic Medical Record (EMR). Because