Chapter 7
Digital Watermarking Strategies for Healthcare Data Security: A Comprehensive Review and Analysis

Aditi Kumari
Dr. B.C. Roy Engineering College, India

Harshek Madhukar
Dr. B.C. Roy Engineering College, India

Shagufa Ali Haider
Dr. B.C. Roy Engineering College, India

Anandaprova Majumder
https://orcid.org/0000-0003-1676-6206
Dr. B.C. Roy Engineering College, India

Sumana Kundu
https://orcid.org/0000-0003-0731-8284
Dr. B.C. Roy Engineering College, India

ABSTRACT

This chapter extensively delves into the realm of digital image watermarking, encompassing comparisons with analogous information security methodologies, elucidations of watermark embedding and extraction procedures, discussions on watermark attributes and applications, overviews of prevalent watermarking tactics, and a concise recapitulation of secure watermarking approaches. The primary focus of this discourse lies in advanced strategies for shielding healthcare data using digital watermarking techniques, with special emphasis on the integration of discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD). Recognizing the inherent challenges in safeguarding medical data amidst the dynamic healthcare landscape, the investigation explores multifaceted watermarking algorithms. Leveraging foundational principles from DWT, DCT, and SVD, the study amalgamates prior research and provides comparative evaluations of the efficacy of these methodologies through tabular representations.

DOI: 10.4018/979-8-3693-2109-6.ch007

INTRODUCTION

In contemporary healthcare practices, the seamless transfer of medical images between different medical centers has become imperative for the exchange of knowledge and experiences. This process not only facilitates patient follow-up when transitioning between centers but also ensures the continuity of patient research studies, even if the patient relocates to a new medical facility (Annaby, M. H et.al, 2018). When medical images are transmitted between centers, the paramount concern is safeguarding patient information from unauthorized manipulation. This is a top priority for electronic medical centers, necessitating the implementation of robust security measures (Med Sayah Moad et.al, 2022).

Digital watermarking (Young M.M. et.al., 1998), as a technique for embedding and extracting information within medical data, has garnered significant attention. In order to thwart potential attackers from extracting or manipulating the watermark, it is crafted in alignment with the objectives of the watermarking program, adding complexity and uniqueness to its content (Ali Al-Haj et.al, 2021). A watermark can take the form of noise, a message, or a picture. The use of watermarks has been suggested as an additional security measure, enabling users to access file content while maintaining robust protection through an imperceptible mark.

Digital watermarking involves embedding a private "mark" or signature or picture or message within a digital document without compromising its quality as shown in Fig.1. This concealed information, which may take various forms, must be both imperceptible and resistant to legal or illicit attempts to manipulate or remove the mark from the document (Yousefi Valandar M, 2020).

Traditional watermarking techniques can be broadly classified into two categories based on their insertion domains: those operating in the spatial domain and those in the frequency domain (Borra S, 2019). Spatial domain techniques modify signal values to insert the mark, depending on the representation space (Salah E, 2021). In contrast, frequency domain techniques are commonly preferred for their resilience against various attacks and their intricate nature (Thanki R, 2017). In these techniques, the mark is inserted by modulating the coefficients of the chosen frequency transform to correspond to the watermark bits. Commonly utilized transforms in watermarking algorithms include the discrete cosine transform (DCT), discrete wavelet transforms (DWT), and discrete Fourier transforms (DFT). Frequency domain watermarking techniques offer increased information hiding capacity and resilience against compression, filtering, and noise addition attacks. Furthermore, they provide an acceptable level of imperceptibility, making them a preferred choice for securing digital content (Ahmadi SBB, 2020).

The digital watermarking algorithms (E. Ganic et.al., 2005 and F. Cayre et.al., 2005) are chosen for their distinct characteristics, including frequency localization, energy compaction, and matrix decomposition, making them well-suited for enhancing the security and robustness of medical data protection.

OBJECTIVE OF USING DIGITAL WATERMARK IN HEALTHCARE

The main objective of using watermark in healthcare is to ensure integrity, authenticity and traceability of digital medical information. The main reasons of using digital watermarking in healthcare data protection are: