A REVIEW ON BIOMEDICAL IMAGE WATERMARKING

Amulya K[1], DR Sudha M S[2], Amulya B R[3], Akriti Raj[4], Kavya M R[5],Chandana R[6]

[13456] Student, [2]Asso.Professor, Department of Electronics and Communication and Engineering,
Cambridge Institute of Technology, KR Puram, Bengaluru-36

ABSTRACT

This paper explores the use of watermarking in healthcare settings, particularly in the context of online operations during the COVID-19 pandemic. It addresses the importance of safeguarding medical image data from online manipulation and presents a detailed review of security and privacy protection using watermarking techniques. The paper discusses the prerequisites of medical image watermarking systems, classifies Medical Image Watermarking Techniques (MIWT), and presents existing schemes along with their limitations to highlight the need for further research and development in this area.

Keyword : - *Medical image watermarking, Framework of typical watermarking system, Digital Health, Data Integrity.*

1. INTRODUCTION

The introduction provides a comprehensive overview of the paradigm shift in healthcare enabled by the ubiquitous presence of computer networks and electronic medical records. This transformation has not only facilitated seamless access to medical images worldwide but has also revolutionized diagnostic processes, significantly reducing the incidence of misdiagnoses. However, this digitalization has brought forth a critical concern: ensuring the security and integrity of patient information against unauthorized access and tampering.

In response to this imperative, the focus shifts to digital watermarking as a robust solution. Watermarking involves the clandestine embedding of data, known as a watermark, into medical images, ensuring their authenticity and integrity. This introductory section then navigates through the intricate landscape of watermarking methodologies, highlighting their classification based on various dimensions.

One such dimension of classification revolves around the embedding information concept, categorizing watermarking algorithms into spatial or transform domain techniques. Spatial domain methods entail the direct insertion of watermark information into the pixel values of the host image, boasting simplicity and high embedding capacity. However, they may exhibit vulnerabilities to noise or loss compression attacks. Conversely, transform domain methods embed watermarks onto transformed versions of the original image, each with its unique strengths and weaknesses.

The discussion further extends to the classification of watermarking methods based on human perception, distinguishing between visible and invisible watermarking techniques. While visible methods, such as overt logos, serve purposes like content or copyright protection, invisible watermarks remain imperceptible to viewers, serving critical functions such as authentication, integrity verification, and copyright protection without altering the visual appearance of the image. Additionally, a hybrid approach integrating robust and fragile techniques is explored, offering a comprehensive suite of security features to encompass authentication, integrity verification, and copyright protection simultaneously.

2. LITERATURE SURVEY

The literature survey delves into various studies and implementations of watermarking techniques for data authentication, emphasizing their significance in modern communication systems. Several approaches have been explored, including Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Hadamard Transform (DHT), each with its unique advantages and challenges.

M S Sudha et al. [1] & T C, Thanuja presented a FPGA Implementation of DTCWT and PCA Based Watermarking Technique and an International Journal of Reconfigurable and Embedded Systems.

Lim, Hyun et al. [2] utilized DCT and Least Significant Bit (LSB) techniques for invisible watermarking in digital cameras, achieving faster embedding compared to software implementations.

Tamilvanan et al. [3] improved robustness and perceptibility using DWT and LSB techniques, implemented on FPGA.

Sonjob Deb Roy et al. [4] presented a hardware implementation of real-time invisible watermark insertion into compressed video streams using DCT, addressing challenges such as power consumption and quality degradation.

Enas Dhuhri Kusuma et al. [5] discussed DCT-based image compression using Hardware Descriptive Language (HDL), highlighting power consumption concerns.

Pankaj U. Lande et al. [6] introduced a watermarking algorithm in DHT domain, emphasizing the need for high-speed applications.

Rajesh Kannan Megalingam et al. [7] implemented image watermarking methods in spatial domain and DCT using Matlab, Verilog HDL, and FPGA, comparing performance metrics such as Peak Signal to Noise Ratio (PSNR).

S. Sowmya et al. [8] explored FPGA implementation of enhancement techniques during transmission, with varying RAM requirements and minimum period durations.

P. Karthigaikumara et al. [9] discussed fragile and semi- fragile watermarking techniques, addressing resource utilization and power consumption issues by employing robust invisible watermarking with DWT.

Wael Wasfya et al. [10] focused on increasing speed and accuracy in fast image processing algorithms, leveraging FPGA's DSP slice module for efficient computation.

Mohammad-Reza Keyvanpoura et al. [11] emphasized the importance of wavelets for watermarking, particularly in designing authentication algorithms resilient to variances and directionalities.

Overall, the literature survey provides a comprehensive overview of the diverse methodologies employed in watermarking techniques for data authentication, highlighting their strengths, challenges, and potential areas for improvement.

3. METHODOLOGY

Basic Concepts in Watermarking Scheme:

In understanding watermarking, it's essential to contextualize it within the broader domain of data security systems, alongside cryptography and steganography. Cryptography serves as a means of securely transmitting messages by encoding them in a manner that only authorized individuals can decipher. However, once decrypted, the message loses its protection, highlighting a key limitation compared to watermarking.

On the other hand, steganography, originating from the Greek words meaning "covered" and "writing," involves concealing a secret message within a cover work. Despite some similarities with watermarking, notable differences exist:

Objective: Steganography aims to embed unrelated messages covertly, whereas watermarking integrates information directly related to the cover work.

Visibility: Steganographic messages remain invisible, contrasting with watermarking, where the embedded data can be visible or invisible.

Goal: Steganography conceals messages to evade detection, while watermarking focuses on embedding data securely to prevent removal or alteration.

Considering these aspects, watermarking emerges as the preferred choice for safeguarding digital images. Additionally, encrypting the data before watermark embedding adds an extra layer of protection.

Further Elaboration:

Watermarking, by embedding data directly into digital assets, offers a robust solution for protecting intellectual property and ensuring content authenticity. It provides a means of tracing ownership, preventing unauthorized use, and verifying data integrity. The combination of watermarking with encryption enhances data security, making it challenging for malicious actors to tamper with or remove embedded information.

By understanding the intricacies of watermarking alongside cryptography and steganography, stakeholders can devise comprehensive strategies for safeguarding sensitive digital assets and maintaining data integrity in an increasingly interconnected world.

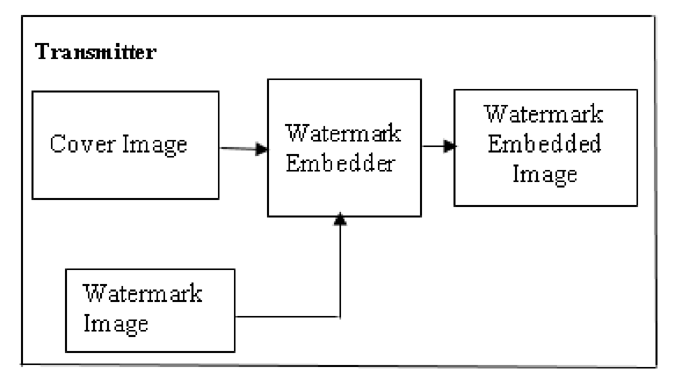

Fig -1 Watermarking system framework in Transmitter

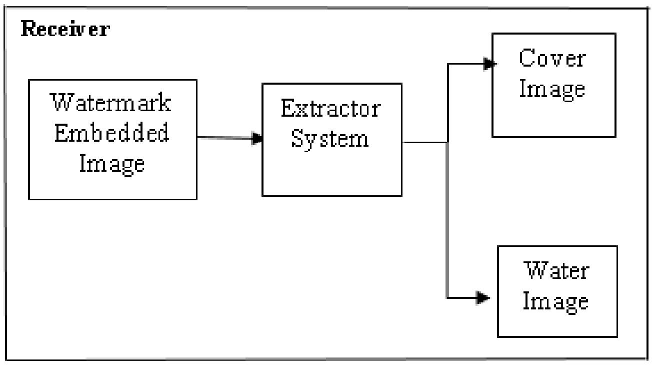

Fig -2 Watermarking system framework in Receiver

A typical watermarking system consists of several key components aimed at embedding and extracting watermarks from digital content for authentication purposes. Here's a breakdown of each part:

Embedding: The original image and watermark are processed by the embedding algorithm to produce a watermarked image.

Distribution: This step involves making the watermarked image accessible to others, such as customers or publication on the internet.
Attacks: Watermarked images may undergo intentional or unintentional modifications by third parties, which can compromise the integrity of the watermark.
Extraction: The process of retrieving hidden information from the watermarked image. Extraction algorithms can be categorized as non-blind, semi-blind, or blind, depending on the availability of side information.
Detection: Evaluates the quality of watermarked images and the accuracy of extracted watermarks by measuring the similarity between the extracted and original ones.

Each part plays a crucial role in the watermarking process, ensuring the authenticity and integrity of digital content. A typical watermarking system encompasses these components, as depicted in Fig -1 and Fig -2

Advantages of Medical Image Watermarking:

Incorporating medical image watermarking offers several advantages:

Memory and Bandwidth Saving: Integrating both the medical image and electronic patient report (EPR) reduces the substantial bandwidth typically required for telemedicine applications.
Detachment Avoidance: Integrating the EPR with medical images mitigates the risk of detachment or misplacement, ensuring that patient information remains correctly associated with the corresponding medical image.
Confidentiality: Watermarking techniques allow the patient report to be concealed within the medical image, safeguarding it from unauthorized access.
Security: Watermarking prevents tampering with patient information and medical images by hiding the EPR within the medical image, enhancing protection against unauthorized modifications [11].
Requirements of Medical Image Watermarking:
In addition to the basic requirements of a typical watermarking system, specific features are necessary for medical watermarking:
Imperceptibility: The watermark should be invisible, ensuring minimal visual difference between watermarked and original images, measured using metrics like SSIM or PSNR.
Reversibility: The watermarking method should be reversible to ensure exact recovery of the original image after extracting the watermark.
Integrity Control: The system should verify that the image hasn't been modified without authorization.
Authentication: Ability to identify the image source and verify that it belongs to the correct patient.

Medical image watermarking methods serve two main objectives: to control integrity and authentication, and to conceal electronic patient record (EPR) information. These methods can be categorized based on their applications: authentication, data hiding, or a combination of both.

4. CONCLUSIONS

Throughout this study, we've delved into various watermarking techniques and methodologies, aiming to understand their strengths, weaknesses, and applications in the medical field. Our investigation has shed light on the intricate components of watermarking systems, the challenges posed by different types of attacks, and the diverse requirements for effective medical image watermarking.

Overall, our study underscores the significance of medical image watermarking in preserving data integrity, confidentiality, and security. As technology continues to evolve, so too must our approaches to safeguarding sensitive medical data, ensuring that patient privacy and healthcare standards are upheld to the highest degree.

5. REFERENCES

[1]. M S Sudha & T C,Thanuja presented a FGPA Implementation of DTCWT and PCA Based Watermarking Technique.International Journal of Reconfigurable and Embedded Systems(IJRES)12.19(2017):8252-8256

[2]. Lim, Hyun utilized DCT and Least Significant Bit (LSB) techniques for invisible watermarking in digital cameras, achieving faster embedding compared to software implementations. Vol.2.IEEE,2003.

[3]. Tamilvanan improved robustness and perceptibility using DWT and LSB techniques, implemented on FPGA.

[4]. Sonjob Deb Roy presented a hardware implementation of real-time invisible watermark insertion into compressed video streams using DCT, addressing challenges such as power consumption and quality degradation.1051-8215,IEEE,2012

[5]. Enas Dhuhri Kusuma discussed DCT-based image compression using Hardware Descriptive Language (HDL), highlighting power consumption concerns. IEEE 2010.

[6]. Pankaj U. Lande introduced a watermarking algorithm in DHT domain.”FPGA Implementation of Image Adaptive Watermarking using Human Visual Model”,Volume 9,Issue 1,October 2009.

[7]. Rajesh Kannan Megalingam implemented image watermarking methods in spatial domain and DCT using Matlab, Verilog HDL, and FPGA, comparing performance metrics such as Peak Signal to Noise Ratio (PSNR).

[8]. S.Sowmya explored FPGA implementation of enhancement techniques during transmission, with varying RAM requirements and minimum period durations.

[9]. P. Karthigaikumara discussed fragile and semi-fragile watermarking techniques, addressing resource utilization and power consumption issues by employing robust invisible watermarking with DWT. 266-273.

[10]. Wael Wasfya focused on increasing speed and accuracy in fast image processing algorithms, leveraging FPGA's DSP slice module for efficient computation.

[11]. Mohammad-Reza Keyvanpoura emphasiz explored FPGA implementation of enhancement techniques during transmission, with varying RAM requirements and minimum period durations. 238-242.