Journal of Namibian Studies, 35 (2023): 127-139 ISSN: 2197-5523 (online)

Special Issue on Engineering, Technology and Sciences

Dual Watermarking With Logo And Electronic Patient Record For Enhanced Security In Medical Image Security

Joseph Deril K. S. , Dr. Rajendra Singh Kushwah

Department of Computer Application, Sri Satya Sai University of Technology & Medical Sciences, Sehore, M.P., India.

ABSTRACT

Protecting private medical pictures while also facilitating their widespread distribution and use has made secure watermarking a vital component of modern healthcare informatics. Algorithms for Dual watermarks on medical images are presented in this work. Two watermarks, one for the company logo and one for the EHR. Space is conserved, attachments are avoided, network traffic is reduced, etc. The results demonstrate that the suggested system's accuracy will improve and that it provides a high PSNR value. Telemedicine, medical research, legal and forensic applications, increased security, and improved partnerships are just few of the areas that may benefit from the use of secure medical image watermarking.

Keywords: Patient, Medical Image, Scan, Logo, Electronic.

I. INTRODUCTION

Medical image watermarking is a crucial and evolving field within the broader domain of medical imaging and healthcare informatics. In an era characterized by digitalization and the seamless sharing of medical data, ensuring the confidentiality, integrity, and authenticity of sensitive medical images has become a paramount concern. Secure medical image watermarking stands at the intersection of information security and medical imaging, offering innovative solutions to address these challenges. As healthcare systems around the world increasingly transition towards digital medical imaging, the need for robust security measures to safeguard patient information has never been more critical. Medical images, such as X-rays, MRIs, CT scans, and ultrasounds, form the foundation

of clinical diagnoses and treatment planning. These images contain highly sensitive information, often linked to a patient's identity, medical history, and potentially life-altering diagnoses. Consequently, the unauthorized access, alteration, or theft of medical images poses significant risks to patient privacy and the integrity of healthcare systems.

Moreover, secure medical image watermarking addresses the issue of image authenticity and integrity. In the medical field, ensuring that an image has not been altered or manipulated is vital for accurate diagnoses and treatment planning. By watermarking medical images with information about their source and history, healthcare professionals can verify the authenticity of the image and detect any unauthorized changes. This not only enhances patient safety but also bolsters the credibility of medical research and legal documentation based on these images.

In addition to privacy and authenticity concerns, secure medical image watermarking plays a pivotal role in data management and traceability. As medical images traverse complex healthcare ecosystems, tracking their origin and usage becomes increasingly challenging. Watermarking provides a means to trace the journey of an image from its source to its final destination. This traceability is invaluable for auditing and compliance purposes, ensuring that medical images are handled in accordance with data protection regulations and institutional policies.

Furthermore, secure medical image watermarking extends its influence beyond patient care and research to legal and forensic applications. In legal cases involving medical malpractice, personal injury claims, or insurance disputes, medical images often serve as crucial evidence. Watermarking ensures the integrity of these images, making it possible to verify their authenticity and history in a court of law. Similarly, in cases of forensic investigation or post-mortem examinations, watermarking can play a pivotal role in preserving the credibility of autopsy images and other critical evidence.

II. DUAL WATERMARKING TECHNIQUE

Dual watermarking is a technique used to embed two separate watermarks within a single digital media, such as images or videos. These two watermarks serve different

purposes and can offer enhanced security, authentication, and traceability. Dual watermarking can be particularly useful in various applications, including copyright protection, content authentication, and secure data transmission. Here, we'll discuss the concept of dual watermarking and its applications:

1. **Primary Watermark**: The primary watermark typically serves as the primary objective of embedding information into the digital media. This watermark could be a logo, copyright information, or any other data that needs to be protected or authenticated. For example, in a video, the primary watermark may be a logo or copyright text that proves ownership.

2. **Secondary Watermark**: The secondary watermark is an additional layer of embedded information, often used for a different purpose than the primary watermark. It may contain metadata, information about the content, or tracking information. In the context of medical image security, the secondary watermark could be used to embed electronic patient records or other relevant data.

Applications of Dual Watermarking

1. **Copyright Protection**: In multimedia content, dual watermarking can help protect the copyright of the content owner. The primary watermark can be the copyright logo or text, while the secondary watermark may contain information about the content's owner, creation date, or usage rights. This allows content owners to prove ownership and trace unauthorized use.

2. **Content Authentication**: Dual watermarking ensures the authenticity of digital media. The primary watermark provides immediate authentication, while the secondary watermark can carry information about the content's integrity, ensuring that it has not been tampered with during transmission or storage.

3. **Traceability**: Dual watermarking can be used to trace the distribution and usage of digital media. The secondary watermark can contain tracking data that

helps monitor how and where the content is being used, providing valuable insights into its distribution.

4. **Medical Image Security**: In the context of medical images, the primary watermark can be a hospital or clinic logo, ensuring that the image's source is verified. The secondary watermark can embed electronic patient records or metadata, allowing for traceability and securely linking the image to the patient's information.

5. **Forensics and Digital Investigations**: Dual watermarking can play a role in digital forensics and investigations by providing a way to authenticate digital evidence. The primary watermark may indicate the source or chain of custody, while the secondary watermark can contain additional case-related information.

6. **Multimedia Communication Security**: In secure communications, dual watermarking can be used to verify the source and integrity of multimedia content, ensuring that it has not been tampered with during transmission.

It's important to note that the success of dual watermarking techniques relies on their robustness to various attacks and their ability to maintain the confidentiality and integrity of the primary and secondary watermarks. Researchers and practitioners continue to develop and refine dual watermarking methods to enhance their effectiveness in different applications while addressing security concerns.

III. REVIEW OF LITERATURE

Hurrah, Nasir et al., (2020) A very resilient digital image watermarking system suitable for the copyright protection of medical photographs is suggested. Before being embedded in a medical picture, the watermark is given an extra layer of protection via the use of encryption methods. Adjusting the values of the singular matrix's diagonal coefficients in the SVD domain accomplishes the embedding. The coefficients are adjusted after a watermark bit of a binary logo determines the adjustment factor. In order to get the singular matrices, we choose the

coefficients in the middle frequency range of a DCT block and arrange them in a two-by-two grid. Different image processing processes, such as adding noise, filtering, and manipulating the geometry of a picture, have been used to evaluate the suggested scheme's performance. This concludes that the technique is very resistant to both independent and coordinated assaults. The suggested methodology is shown to be superior than state-of-the-art methods in terms of resilience, security, payload, and undetectability via comparison. As a result of its advantages, the suggested method may be used in contexts where copyright protection and user privacy are particularly important. An emerging use for this technology is in electronic healthcare, where it may be used to prevent data corruption in medical imaging, safeguard electronic patient records, and guarantee the safety of transmitted files. Future updates to the system will include a tamper localization module for identifying the precise location of any forging attempts.

Aparna, Puvvadi & Kishore, P.V.V. (2019) Patient data security is an essential component of any credible medical image management system. The confidentiality of patients' medical records is a top priority for all healthcare facilities. The privacy and integrity of patients' medical records are protected using digital watermarking, which also raises patients' health literacy. It is recommended that crypto-watermarking be used in a secure patient medical information exchange system to prevent unauthorized access to sensitive data. There are two stages to the proposed system: (i) embedding and (ii) extraction. In this study, we discuss a safe method for exchanging medical images, electronic health records (EHRs), and facial images across healthcare facilities. At first, the three inputs are encrypted together and all the data matches up. To make the crypto-watermarking method more robust, the returned bit stream is compressed before being added to the cover image. The identical procedures are repeated when it's time to get rid of the drug. Experimental findings are conducted using a variety of medical images with EHR, and the effectiveness of the suggested technique is evaluated using the peak signal-to-noise ratio.

Allaf, Abdelhay & M'hamed, Aït Kbir (2019) In this study, we discuss the use of watermarking techniques to medical

imaging, and we emphasize the importance of these methods for security reasons, since watermarking is widely regarded as an excellent means of shielding patients' private information during the transmission of medical pictures and other telemedicine data. This document is developed in two sections. The first is devoted to a general introduction to picture watermarking, including a discussion of the three most crucial watermarking criteria (invisibility, capacity, and resilience). We also provide a broad outline of watermarking, including its two primary stages and the many assaults that may be mounted against them. In addition, we provide a categorization of watermarking methods according to criteria such insertion domain, human perception, and detection approaches, and conclude with a presentation of certain metrics and benchmarks for evaluating the effectiveness of watermarking. We also discuss a literature overview of watermarking methods for medical images and their applications, with a focus on integrity verification, authentication, and data concealment, which we'll cover in the second section. We also discuss the significance of watermarking in contemporary medical treatment, as well as the notion of telemedicine and telehealth.

Singh, Amit. (2017) For telemedicine and other future uses, this book details methods and algorithms for watermarking medical images. In order to safeguard the veracity of transmitted medical data, this book focuses on medical picture watermarking. First, the concept of digital watermarking is laid forth, along with its salient features, unique applications, various watermarking attacks, and industry-standard benchmarking resources. The benefits and drawbacks of several watermarking methods for medical images, both in the spatial and transform domains, are discussed in detail in this book. The authors have created innovative and enhanced watermarking algorithms for telemedicine applications, which are more secure, have a greater embedding capacity, and a higher perceptual quality. The solutions proposed may be used to address a major worry in telemedicine: the theft of patients' personal information and problems with managing their medical records. This book offers a good framework for comprehending the medical picture watermarking paradigm for researchers in the area and advanced-level students. Those working in the industry, as well as those

developing new applications that need safe and robust watermarking, will find this book to be an invaluable resource.

Swaraja, K. (2017) Authentication and image integrity in the medical field are starting to become serious problems. To address this issue, this work proposes a unique region-based blind fragile lossless reversible watermarking approach for medical photos. When inserting the watermark into the projected scheme, the least significant bits are used. Compressing the region of interest (ROI) to create a content dependent watermark, the strategy combines compression, hashing, and digital signature methods to extort ROI. Simulations were run to prove the method's efficacy, and the results show that the ROI is extracted in a complete fashion, and the PSNR values reached lead to the insight that the easily available scheme suggests healthier security for medical imageries.

Sharma, Abhilasha et al., (2015) The security of patient information is a top priority in the medical industry for the advancement of telemedicine. There must be a safe and reliable method for sending medical pictures online. The suggested watermarking strategy makes use of the DWT and DCT, two well-known methods in the transform domain. When a medical picture is embedded, it is first segmented into a ROI and an NROI. For the purpose of authenticity checking, the same cover media item may have many image and text watermarks inserted in both the ROI and NROI. After encrypting the text watermark using the Rivest-Shamir-Adleman (RSA) technique, we embed the encrypted EPR data into the NROI region of the cover medical image to make it more secure. The effectiveness of the suggested technique is tested against signal processing assaults, and it is shown to provide the intended result without significantly lowering the quality of the extracted watermark or the watermarked image's perceived quality.

Mahmood, Ahmed et al., (2013) Protecting patients' privacy during medical picture transmission requires the use of security measures. To ensure privacy and authenticity during transmission, encryption and watermarking are necessary. A strong encryption algorithm that can withstand a variety of assaults is a must for the development of cryptographic protocols. The suggested

strategy is grounded on number theory, namely the Chinese remainder theorem. This method not only delivers a high degree of security but also is resilient against several threats. For the watermarking process, the medical picture is segmented into a ROI and a ROB, or backdrop. The area of interest (ROI) must remain unchanged since it contains crucial data in the form of pixel values. To insert the watermark to the ROI, the suggested watermarking method involves segmenting the medical picture into blocks and then moving the blocks about. After then, the same amount of blocks are taken out of the ROB. Since the ROI is unaffected and the picture size is kept the same, this method is termed lossless. It is also resistant to cropping and noise-based watermarking attempts.

IV. PROPOSED MODEL

The following diagram illustrates how the suggested system might function in practice.

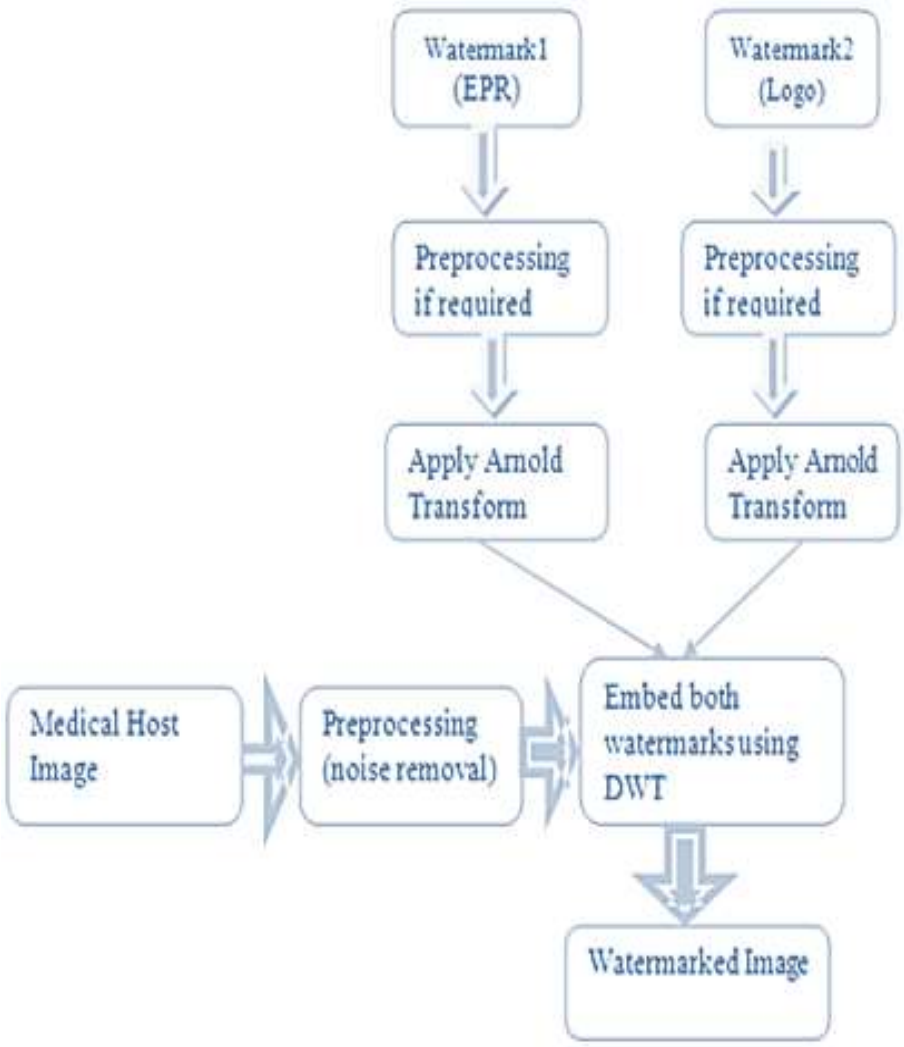

Figure 1: Proposed model

V. RESULTS AND DISCUSSIONS

Below, we provide the results of one such collection. The same discovery pattern was seen in every subsequent image. Figures 3-5 show the cover image, watermark1 and watermark2, and the extracted image and its PSNR value, respectively.

Grayscale images at a host resolution of 512 pixels on the horizontal and vertical are seen in Figure 2.

Figure 2: Original MRI image

Figure 3 Watermark

The logo serves as watermark1 in Figure 3, with EPR serving as watermark2. The program was put through its paces on several generic and gray scale test photos.

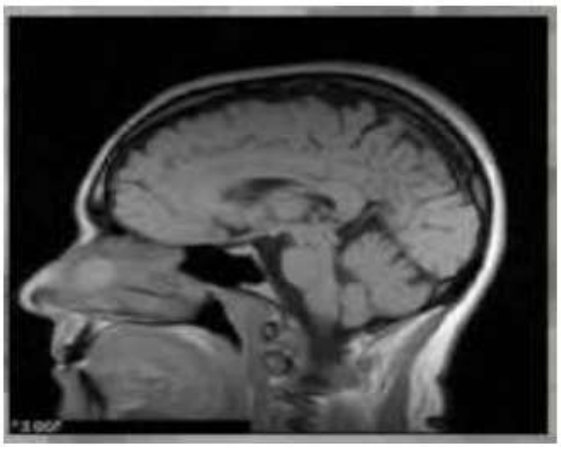

Figure 4: Watermarked Image

Figure 5: Extracted image of watermark 1 and watermark 2

Table 1: CT scan and MRI Imaging

Type of Imaging	**CT Scan Imaging**	**MRI Imaging**
Size	512x512	512x512
MSE	0.2989	0.1372
Peak Signal to Noise Ratios	53.37db	56.76db

VI. CONCLUSION

Secure medical image watermarking stands as a vital bridge between healthcare and information security. It addresses the pressing need to protect sensitive medical images while enabling their efficient and secure utilization. This technology not only safeguards patient privacy by anonymizing images but also ensures the authenticity and integrity of critical diagnostic data. Its diverse applications in telemedicine, research, and legal contexts underscore its transformative potential in elevating the standards of healthcare practices and data protection. As the healthcare landscape continues to evolve in the digital era, secure medical image watermarking remains a cornerstone technology, offering assurance, traceability, and reliability in the handling of invaluable medical image assets.

REFERENCES: -

1. Hurrah, Nasir & Parah, Shabir & Sheikh, Javaid. (2020). A Secure Medical Image Watermarking Technique for E-Healthcare Applications. 10.1007/978-3-030-15887-3_6.

2. Aparna, Puvvadi & Kishore, P.V.V.. (2019). A Blind Medical Image Watermarking for Secure E-Healthcare Application Using Crypto-Watermarking System. Journal of Intelligent Systems. 29. 10.1515/jisys-2018-0370.
3. Ayu, Media & Mantoro, Teddy & Priyatna, I Made. (2019). Advanced watermarking technique to improve medical images' security. TELKOMNIKA (Telecommunication Computing Electronics and Control). 17. 2684. 10.12928/telkomnika.v17i5.13292.
4. Allaf, Abdelhay & M'hamed, Aït Kbir. (2019). A Review of Digital Watermarking Applications for Medical Image Exchange Security. 10.1007/978-3-030-11196-0_40.
5. Assini, Imane & Badri, Abdelmajid & Safi, Khadija & Sahel, Aicha & Abdennaceur, Baghdad. (2018). A Robust Hybrid Watermarking Technique for Securing Medical Image. International Journal of Intelligent Engineering and Systems. 11. 169-176. 10.22266/ijies2018.0630.18.
6. Al-qdah, Majdi. (2018). Secure Watermarking Technique for Medical Images with Visual Evaluation. Signal & Image Processing : An International Journal. 9. 01-09. 10.5121/sipij.2018.9101.
7. Singh, Amit. (2017). Medical Image Watermarking:Techniques and Applications.
8. Swaraja, K.. (2017). Protection of medical image watermarking. Journal of Advanced Research in Dynamical and Control Systems. 9. 480-486.
9. Sharma, Abhilasha & Singh, Amit & Ghrera, S.P.. (2015). Secure Hybrid Robust Watermarking Technique for Medical Images. Procedia Computer Science. 70. 778-784. 10.1016/j.procs.2015.10.117.
10. Indira Joshi, Dr. V. N. Pawar. (2014). Secure Medical Image Watermarking. International Journal of Research in Advent Technology, Vol.2, No42, April 2014 E-ISSN: 2321-9637.
11. Mahmood, Ahmed & Hamed, Tarfa & Obimbo, Charlie & Dony, Robert. (2013). Improving the Security of the Medical Images. International Journal of Advanced Computer Science and Applications. 4. 10.14569/IJACSA.2013.040922.
12. S.Rameshkumar, A.Umamageswari & G R, Suresh. (2013). Performance Analysis of Secure Medical Image Communication with Digital Signature and reversible Watermarking. EURASIP Journal on Image and Video Processing. 4. 647-651. 10.21917/ijivp.2013.0093.
13. Nyeem, Hussain & Boles, Wageeh & Boyd, Colin. (2012). A Review of Medical Image Watermarking Requirements for Teleradiology. Journal of digital imaging : the official journal of the Society for Computer Applications in Radiology. 26. 10.1007/s10278-012-9527-x.
14. Nassiri, Boujemaa & Latif, Rachid & Toumanari, Ahmed & Maoulainine, F.. (2012). Secure transmission of medical

images by watermarking technique. Proceedings of 2012 International Conference on Complex Systems, ICCS 2012. 1-5. 10.1109/ICoCS.2012.6458577.

15. Rao, Namuduri & Kumari, V.. (2011). Watermarking in Medical Imaging for Security and Authentication. Information Security Journal: A Global Perspective. 20. 148-155. 10.1080/19393555.2011.561154.