Integration of digital watermarking technique into medical imaging systems

Qasim, A, Aspin, R and Meziane, F

http://dx.doi.org/10.1109/DESSERT.2019.8770051

Integration of Digital Watermarking Technique into Medical Imaging Systems

Asaad F. Qasim
Computing, Science and Engineering
University of Salford
Greater Manchester, UK
a.qasim@edu.salford.ac.uk

Rob Aspin
Computing, Science and Engineering
University of Salford
Greater Manchester, UK
r.aspin@salford.ac.uk

Farid Meziane
Computing, Science and Engineering
University of Salford
Greater Manchester, UK
f.meziane@salford.ac.uk

***Abstract*—This paper presents the process of integrating digital watermarking technique into medical imaging workflow to evaluate, validate and verify its applicability and appropriateness to medical domains. This is significant to ensure the ability of the proposed approach to tackle security threats that may face medical images during routine medical practices. This work considers two key objectives within the aim of defining a secure and practical digital medical imaging system: current medical digital workflows are deeply analyzed to define security limitations in Picture Archiving and Communication Systems (PACS) of medical imaging; the proposed watermarking approach is then theoretically tested and validated in its ability to operate in a real-world scenario (e.g. PACS). These have been undertaken through identified case studies related to manipulations of medical images within PACS workflow during acquisition, viewing, exchanging and archiving. This work assures the achievement of the identified particular requirements of digital watermarking when applied to digital medical images and also provides robust controls within medical imaging pipelines to detect modifications that may be applied to medical images during viewing, storing and transmitting.**

Keywords—Medical Imaging, Digital Watermarking, Picture Archiving and Communication Systems, Integrity, Authentication.

I. INTRODUCTION

Picture Archiving and Communication Systems (PACS) act as integrated systems for managing, archiving and exchanging medical images. The propagation of PACS is associated with the development of various digital acquisition equipment that contributed to reducing the maintenance issues and improving the performance of services provided by radiology departments. Acquisition devices create digital images across various modalities [1], which are, typically, managed within the digital medical workflow based on Digital Imaging and Communications in Medicine (DICOM) standard [2]. A generic PACS infrastructure (Fig. 1) comprises three main components, connected by a high-speed communication network, including acquisition devices, repositories, and viewing workstations [3]. Acquisition gateway acts as a buffer between the acquisition devices and the PACS to collect medical images, which are produced from various manufacturer specifications, and transform them to DICOM format. PACS server acts as interface for receiving, accumulating, storing and transferring medical images [4].

In modern healthcare systems, a hierarchical scheme can be considered as a pyramid with the general PACS at its top and hospitals at the base. Images generated in a hospital are archived in the local PACS and then transmitted to a higher PACS, which gathers data arrived from similar departments. These images remain in this system for several hours, usually staying for the night, during which time their integrity is not preserved strictly. The images are then transferred to a hierarchically upper PACS until they arrive the top-PACS to be collected and permanently archived in tapes, physical drives or optical disks. This process is defined as consolidation [5]. For security reasons, the authorized archive is conducted offline, while accessible images are saved on the top-PACS discs. In most circumstances, it is challenging to predict the security problems for each intermediate system, and the images could be intentionally or accidentally tampered. This signifies the first critical situation. Furthermore, the images are not immediately consolidated when arriving the top-PACS but after approximately 24/36 hours, which allows PACS technicians to manipulate the image's pixels and header as well as image's header data, if required, for addressing potential defects that may appear in the images. This issue represents the second critical situation, which enables malicious manipulations to be applied to the images prior to the consolidation operation. The detection of image manipulation in the top-PACS is difficult due to the authorized archive is done offline and the available images are not quickly accessible. The separation between the legal archive (secured images) and the available images (used by clinicians) points out the third crucial case of PACS scenario. Manipulations of medical images in the top-PACS can be detected later, but it might be too late for patients' safety [6].

Transmission of medical images through, and across, hospitals, located at various locations, has become a common practice for many purposes including diagnosis, treatment, consultations, transferring to another hospital or clinic, and patient images request [7]. Many cases of manipulations on the medical images can be performed, but the concern is how they can be revealed? By merely viewing the images, detecting some sensible alterations, that comprise fully counterfeit abnormalities, would be unattainable [8]. Therefore, the capability to ensure the authenticity and integrity of digital medical images has become crucial, both within the local hospitals' systems and through their exchange to other systems. Integrity of images can be achieved by encrypting the images during sharing. Authentication requires additional techniques to determine whether integrity and/or confidentiality of the images has been breached [9].

Digital watermarking is recognized as an efficient technique for protecting medical images and detect applied alterations. Three objectives can be achieved by using digital watermarking: data hiding; integrity; and authentication [4]. Many approaches have been proposed for applying digital watermarking to medical images but there is no study on the experimentation of watermarking in an operational PACS workflow. Therefore, this research proposes an approach for integrating digital watermarking into PACS infrastructures to ensure its applicability and suitability.

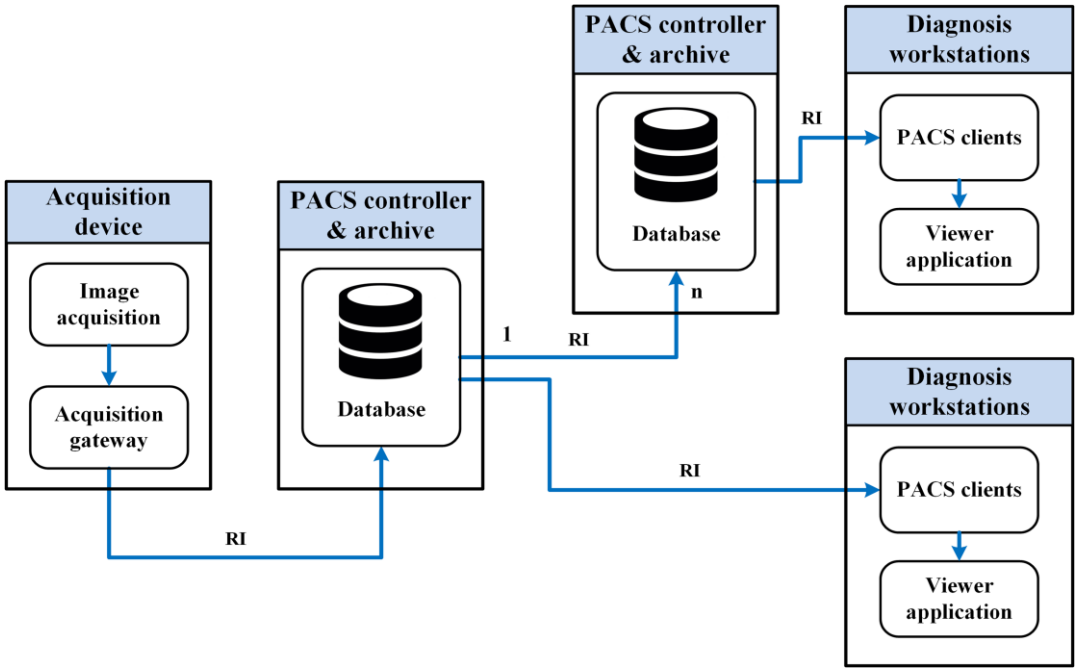

Fig. 1: A generic PACS infrastructure which comprises three main components connected by a high-speed communication network including acquisition devices, archive server, and diagnosis workstations. Acquisition gateway works as a buffer between acquisition devices and PACS to perform various objectives. RI denotes row images produced by the acquisition devices. Internal PACS may connect to a different number of PACS (1 to n) within or outside the internal system.

II. Design and Evaluation Requiremnents

On the practical side, there is a reluctance in using digital watermarking in medical domains due to most proposed watermarking approaches not considering the requirements of medical imaging workflow. Therefore, defining the design and evaluation criteria, of medical image watermarking, is fundamental to verify the appropriateness of the proposed watermarking technique for medical imaging workflow. The design and evaluation parameters for medical image watermarking are mainly related to its substance components; watermark creation, embedding, and extraction. A definitive review article [10], often cited in the literature, has defined four requirements that must be considered when applying digital watermarking to medical imaging including imperceptibility, reversibility, integrity and authentication.

Imperceptibility is the highest requirement of watermarking systems. A digital watermark is defined as imperceptible if the original and modified images are visually indistinguishable, which is significant for the secrecy and confidentiality of the encoded data. Reversibility ensures the retrieving of original images after extracting the encoded data successfully. Integrity refers to the ability to ensure that images have not been manipulated, while authentication denotes the ability to verify that images belong to the correct patient [6].

We have proposed a novel reversible watermarking technique to verify the authenticity and integrity of medical images to ensure that manipulations can be revealed and tracked [11]. The exact original images can be retrieved after extracting the watermark successfully. The proposed method delivered highly imperceptible watermarked images evaluated through clinical assessment based on relative Visual Grading Analysis (VGA) to define the amount of change that can be applied to medical images without noticeable distortion [12]. This developed security measure, therefore, assists the detection of image alterations, by a reversible and imperceptible technique, that may establish enhanced trust in the medical workflow.

III. Integration of Proposed Watermarking Approach in Medical Imaging Systems

After the proposed watermarking approach has been designed, developed and evaluated in terms of achieving all the identified medical imaging requirements, it is essential to integrate the approach into medical systems or PACS infrastructures (Fig. 2). The proposed scheme can be introduced into the PACS workflow as follows:

Acquisition Phase

- Acquisition gateway receives the raw images from acquisition machines and transform them into standard DICOM format.
- Watermark data is encoded into the raw images as soon as they are received from the acquisition gateway. Each image is watermarked independently.
- Watermarked images are verified to ensure their integrity before they are being transferred to the PACS server.

Archiving Phase

- Local PACS receives the watermarked images from the acquisition phase and verify the integrity and authenticity of these images before archiving.
- Each PACS includes two databases; one for storing the verified images and another for storing the

unverified images. The watermarked images are archived in one of these databases according to the verification result.

- The watermarked images are also verified when received by another internal or external PACS.

Viewing Phase

- The watermarked images are downloaded from the database of verified images when requested by a radiologist.
- Watermark data is extracted and validated, and original unmodified images are retrieved.
- Original images are shown to the radiologist alongside the verification report. This gives the clinician the certainty of being viewing images that have not been manipulated (neither by an attacker nor by the watermarking technique).
- In case of urgent requests, watermarked images are shown to the radiologist and the verification process is managed independently. The radiologist is immediately notified if the verification process reveals a manipulation.

IV. Validation of the Proposed Medical Imaging Workflow

Validation of watermarking approaches is a challenging issue that has not been widely investigated in the literature. There is no current standard on the usage of watermarking in medical imaging and development of a watermarking approach for a healthcare provider depends on its infrastructure and its related entities. Ethical and legislative concerns about modifying image are decreasing the applicability of digital watermarking for medical images. Therefore, this work concentrates on designing a framework for validating the applicability of the proposed watermarking technique to medical environments. To achieve this, security threats that may face medical images during their exchanging over medical pipelines require to be identified first. This is essential to ensure the ability of the proposed approach to tackle the determined security risks and provide a secure environment for medical imaging workflow. We have conducted an in-depth survey to analyze the security flaws in medical imaging systems. The process of integrating the proposed watermarking technique into medical environments is then clarified and validated. Two studies have been found; one related to manipulation of medical images within PACS database [5] and another study related to tampering with medical images during transmission [13]. In addition, two potential security issues have also been identified in this research. The first issue related to manipulation of images after capturing process and before transmission to PACS. The second issue related to the modification of images in the workstations when the images are requested for examinations. This section comprises two main parts: the security hazards that may face the medical images during routine practices are reviewed; and the ability of the proposed approach to tackle these threats is then discussed to provide a protected workflow for medical imaging.

A. Security Threats in Medical Imaging Workflow

Despite the many advantages that modern healthcare systems offer, they are vulnerable to a wide range of risks. Security threats can take place on each level of medical imaging workflow including image acquisition, transmission, viewing, and archiving (Fig. 3).

Scenario One (S1) – Acquisition Phase

Acquisition devices capture digital images of patients according to the required examination. The captured images are gathered by the acquisition gateway and stored in a cache before transmission to PACS for archiving and using for medical investigations. During this time, the images can be accidentally or intentionally manipulated which can, therefore, impact the originality of the image data utilized for diagnosis purposes.

Scenario Two (S2) – Transmission Phase

Most healthcare providers concentrate on protecting images within their data centers, but there are also many circumstances in which the images are subjected to manipulation, through exchange, within the hospital's internal network or when transmitted to another hospitals or clinicians. This is a critical issue where accidental or malicious operation can be applied to manipulate the images.

Scenario Three (S3) – Viewing Phase

Medical images are downloaded from PACS database to diagnosis workstations when requested for medical examinations. These images can be modified and re-archived in the PACS database or re-send to another user. In this case, there is no ability to detect the manipulations as there is no verification system neither in PACS controller nor in the diagnosis workstations.

Scenario Four (S4) – Archiving Phase

This is the most serious scenario of security threats which can be applied to PACS database where medical images are archived for short-term or permanently. These threats need to be identified first to provide a secure platform for medical imaging workflow that can address these threats. To achieve this, a research paper has been considered as a case study to identify security risks that may face medical images stored in the PACS database [5]. This aids in analyzing the PACS workflow and understanding the security requirements derived from the medical side to determine a suitable approach for integrating the proposed watermarking technique into medical domains. The selected research declares three main critical situations that may face medical images inside PACS.

- *Critical Situations 1 (CS1)*: Medical images inside PACS can be manipulated either intentionally or inadvertently due to the difficulty of predicting security matters for each intermediate system.
- *Critical Situations 2 (CS2)*: PACS technicians, which have access to image pixels as well as metadata, can manipulate the images before the consolidation process.
- *Critical Situations 3 (CS3)*: In case of modifying medical images in top-PACS, it will be impossible to automatically discover the manipulation in hospital systems, which requested the images, because authorized archives are stored offline and images are not quickly accessible.

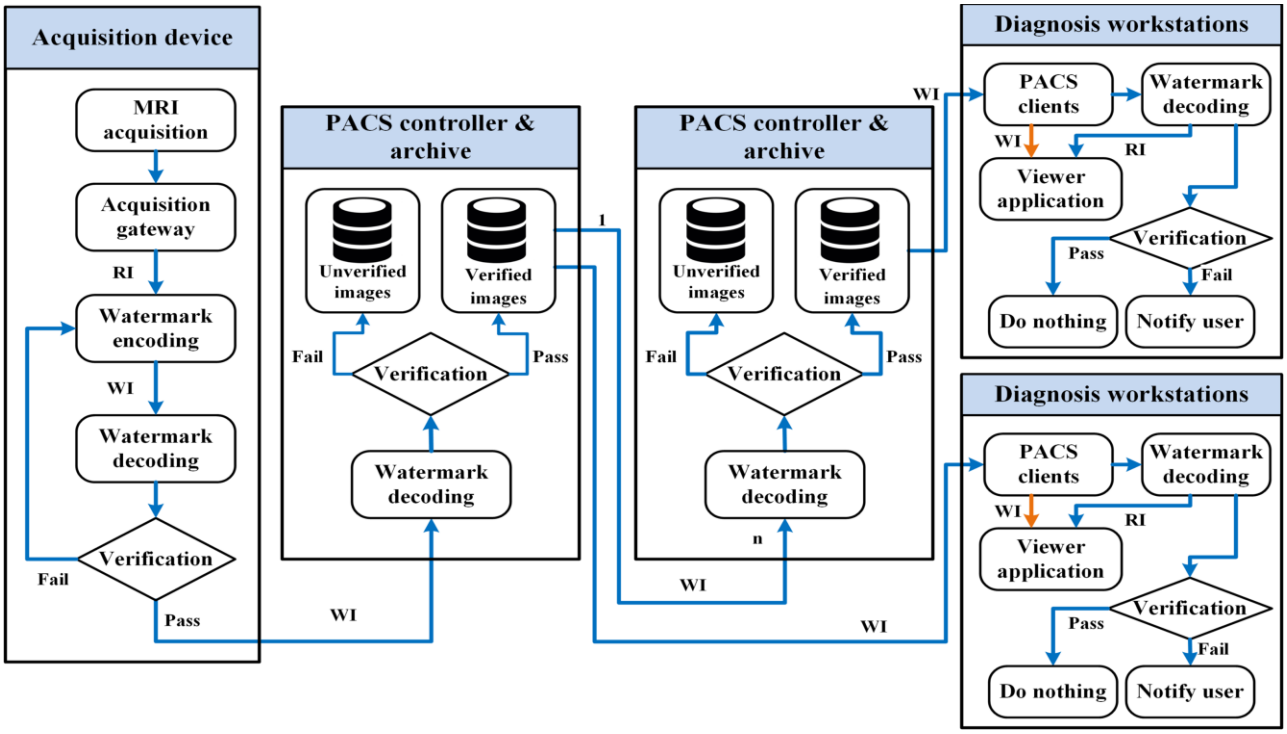

Fig. 2: Integration of the proposed watermarking approach into PACS infrastructures. Watermark data is encoded into the raw images (RI) as soon as they are received from the acquisition gateway. Watermarked images (WI) are verified before archiving and during viewing to confirm their integrity and authenticity.

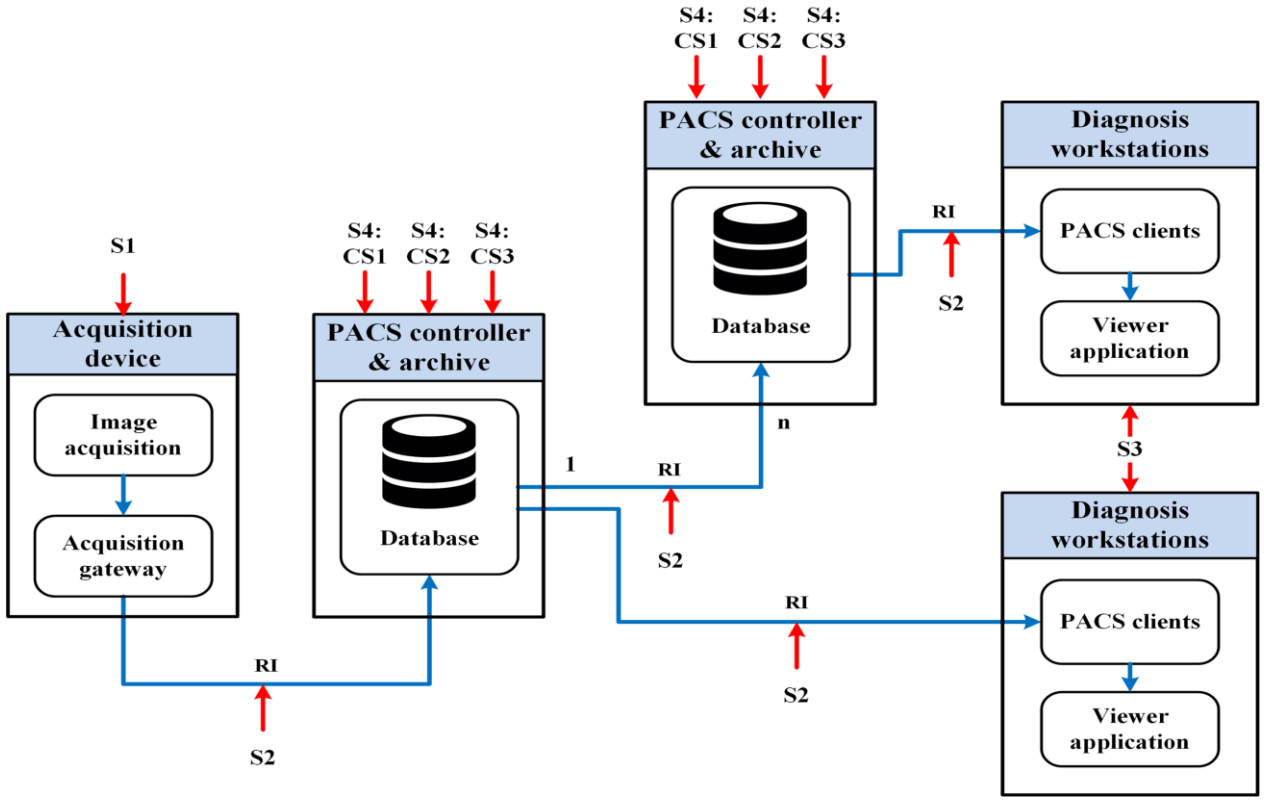

Fig. 3: Security threats that may face medical imaging during routine medical practices. Various scenarios can be applied to manipulate medical raw images (RI) within medical imaging workflow during acquisition, transmission, viewing and archiving.

B. Validation of the Proposed Integration Process

To verify the applicability of the proposed watermarking approach within the digital medical imaging workflow, its ability to deal with the identified security threats need to be tested and verified. The ability of the approach to detect manipulations of medical images during routine medical practices, for each identified scenario of security threats, has been examined and validated (Fig. 2).

Scenario One (S1) – Acquisition Phase

The proposed approach suggests encoding watermark data into medical images as soon as they are captured in the acquisition phase. After watermarked images are transferred to PACS server, they are verified instantly to verify their validity and integrity to detect manipulations that may applied during the acquisition process. The proposed approach stores both the verified and manipulated images in two different databases to allow the database administrator to conduct the required investigations.

Scenario Two (S2) – Transmission Phase

The integrity of watermarked images is verified with each transmission before they are stored in the PACS database or shown to viewers. Any manipulation to images during transmission can be immediately detected. The manipulated images are inserted into the database, which is dedicated for the unverified images, when received by local/external PACS. In the workstations, the diagnosis phase, the manipulated images are shown to clinicians alongside a notification demonstrating that the displayed images are unauthorized and have been tampered.

Scenario Three (S3) – Viewing Phase

Matching to the transmission phase, modification of images, that may happen during the viewing phase at diagnosis workstations, can be discovered when re-archived in the PACS or re-sent to another workstation for viewing.

Scenario Four (S4) – Archiving Phase

Watermarked medical images, which are saved permanently inside the PACS database, may face three critical situations (CS1, CS2, CS3). The proposed approach can address all these critical situations by detecting modifications during transmission to another local/external PACS or when requested for viewing at diagnosis workstations.

V. Conclusion

Modern healthcare systems act as integrated platforms for capturing, transmitting and storing medical images. During routine medical practices, many operations can be applied to these images through which the image data is modified intentionally or unintentionally. Despite its efficiency in ensuring the integrity and authenticity of medical images, there is a hesitation of accepting the digital watermarking technique in the medical fields due to most existing watermarking approaches not taking into account the essential requirements of medical imaging workflow.

In this research, these essential requirements of medical imaging have been identified and the proposed watermarking approach, developed to detect both intentional and accidental manipulations, has been integrated into medical imaging systems to provide a secure platform for medical image workflow. This has been theoretically validated because of the reluctance of using digital watermarking in medical domains due to the ethical and legal concerns about modifying patients' images. To accomplish this, security threats, drawn from case studies and this research, that may face medical images during the routine medical practices has been identified to verify the ability of the approach to address these threats through detection of intentional and unintentional manipulations of medical images during acquisition, transmission, viewing, and archiving.

For future work, we recommend verifying the applicability of the proposed watermarking approach to operating in a real operational PACS, where medical images are produced, exchanged and archived, to ensure its validity and suitability.

Acknowledgment

The authors would like to thank the ministry of higher education and scientific research/Iraq, for providing scholarship support to the first author of this paper.

References

[1] T. M. Godinho, L. M. Silva, and C. Costa, "An automation framework for PACS workflows optimization in shared environments," in *10th Iberian Conference on Information Systems and Technologies (CISTI)*, Aveiro, Portugal, 2015, pp. 1-7.

[2] O. S. Pianykh, *Digital imaging and communications in medicine (DICOM): a practical introduction and survival guide*, 2nd ed ed.: 2nd ed. Springer. Berlin, Germany, 2009.

[3] H. Huang, *PACS and imaging informatics: basic principles and applications*: John Wiley & Sons, 2011.

[4] S. c. Liew and J. M. Zain, "Experiment of tamper detection and recovery watermarking in picture archiving and communication systems," *Journal of Computer Science*, vol. 6, p. 794, 2010.

[5] M. Fontani, A. De Rosa, R. Caldelli, F. Filippini, A. Piva, M. Consalvo, *et al.*, "Reversible watermarking for image integrity verification in hierarchical pacs," in *Proceedings of the 12th ACM workshop on Multimedia and security*, Roma, Italy, 2010, pp. 161-168.

[6] A. F. Qasim, F. Meziane, and R. Aspin, "Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review," *Computer Science Review*, vol. 27, pp. 45-60, 2018.

[7] N. A. Memon, A. Chaudhry, M. Ahmad, and Z. A. Keerio, "Hybrid watermarking of medical images for ROI authentication and recovery," *International Journal of Computer Mathematics*, vol. 88, pp. 2057-2071, 2011.

[8] H. Nyeem, W. Boles, and C. Boyd, "A review of medical image watermarking requirements for teleradiology," *Journal of digital imaging*, vol. 26, pp. 326-343, 2013.

[9] K. Pushpala and R. Nigudkar, "A novel watermarking technique for medical image authentication," in *Computers in Cardiology*, Lyon, France, 2005, pp. 683-686.

[10] S. M. Mousavi, A. Naghsh, and S. Abu-Bakar, "Watermarking techniques used in medical images: a survey," *Journal of digital imaging*, vol. 27, pp. 714-729, 2014.

[11] A. F. Qasim, R. Aspin, F. Meziane, and P. Hogg, "ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images," *Multimedia Tools and Applications*, 2018.

[12] A. F. Qasim, R. Aspin, F. Meziane, and P. Hogg, "Assessment of perceptual distortion boundary through applying reversible watermarking to brain MR images," *Signal Processing: Image Communication*, vol. 70, pp. 246-258, 2019.

[13] P. Selvam, S. Balachandran, S. P. Iyer, and R. Jayabal, "Hybrid transform based reversible watermarking technique for medical images in telemedicine applications," *Optik-International Journal for Light and Electron Optics*, vol. 145, pp. 655-671, 2017.