International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 07 | July 2021 www.irjet.net p-ISSN: 2395-0072

# Watermarking of Medical Images: A Survey

**Pruthvi Dinesh[1], Varsha M.S[2], Ritu Patil[3]**

[1]*Student, Dept. of Electronics and Communication Engineering, K.S. Institute of Technology, Karnataka, India*
[2]*Student, Dept. of Electronics and Communication Engineering, K.S. Institute of Technology, Karnataka, India*
[3]*Student, Dept. of Electronics and Communication Engineering, K.S. Institute of Technology, Karnataka, India*

---

**Abstract -** *DICOM (Digital Imaging and communication of Medicine) images are extensively utilized in the medical imaging industry thus they must be widely studied, particularly the issue of data privacy and security. Accessing networks to transfer medical photographs subjects to a range of security threats. As a result, a reliable and secure technique for exchanging medical photographs over the Internet is required. The proposed approach embeds an encrypted watermark on DICOM images and also detects if a DICOM image is tampered or not.*

***Key Words***: DICOM, Infrared Rays, Security, Watermark, Tamper

## 1.INTRODUCTION

Digital information technology underpins today's health-care infrastructure. Medical data analysis systems have evolved significantly over the last several years as a result of rapid and significant advances in information and communication technology. The exchanging of datasets between hospitals across effective transmission lines is among the most important functions of a medical data management system. The DICOM standard for digital imaging and communication in medicine makes it easier to transfer digital image data between devices. Before saving a medical image in long-term storage, it is common to diagnose it, so the important parts of the image are already known. While recent advances in information and communication technology have provided new ways to access, manage, and also move medical images, they have also made it easier to manipulate and replicate them. It is widely believed that security precautions in medical information systems are urgently required.

Despite affecting the image for 7 at, digital watermarking can be used to encode messages invisibly. The watermarked image can still be DICOM compatible when used on medical imaging. DICOM file is made up of two different parts. One part is named as Header Data while another is named as Pixel Data. Patient records and clinical information are stored in header data, which is a textual data format. Pixel Data is a type of data that might be an image, a short video, or audio. The header data in DICOM has secrecy safeguards, but the picture pixel data does not. Data hiding approaches are basically used to interleave patient data along with medical images in order to solve the capacity problem by reducing storage and transmitting overheads. These data hiding tactics can also be utilised for authentication and tamper detection in order to determine the integrity and fidelity of pictures. This paper focuses mainly on embedding an encrypted watermark on DICOM images and also detecting if a DICOM image is tampered or not.

Section 2 presents literature survey. Section 3 presents comparison and challenges. Section 4 presents the proposed approach. Section 5 concludes the paper.

### 1.1 State of Art

Jeyamala Chandrasekaran et al. [1] made the encryption process to divide into three stages in this paper. The Sub imaging technique is used for permuting the input DICOM image. Using the input image for Modular Exponentiation, it develops a two-dimensional key array. Once the Key array is developed, Henon maps are used to permute or submit the key array for encrypting. Permuted Key arrays are XOR'ed with the bitwise sub images for encrypting processes. The exact inverse operation is done to decrypt the data. This paper only specifies the encryption/decryption of the DICOM image to ensure the security of the data.

Yin and Xin [2] for DICOM images, a quaternion-based lossless encryption method is suggested. The speed of Encryption and Decryption processes is concentrated. For encryption, the quaternion rotation algorithm is used. The proposed encryption scheme can also be used for encrypting textual data. The Feistal network scheme is modified and used in the suggested scheme. The Quaternion rotation formula is as shown in (1).

$$Prot=q.P.q-1 \quad (1)$$

The quaternion is denoted by q, while the vector portion is denoted by P. It is necessary to deconstruct a DICOM image into 2 separate Gray-tone images in order to encrypt it. The Quaternion rotation formula uses the two pictures acquired as input data.

Sareh Mortajez et al. [3], for encryption, the DICOM image is encrypted employing the Logistic Mapping Technique. The secret key is obtained while encrypting using the pixel data of the DICOM image. Permutation of the position of pixels is done based on the Pseudo-Random Sequences and Confusion Strategy of Periodicity. Permuted image pixels are

coded using the XOR operator and the logistic system sequences. Once the secret key is obtained, Two Chaotic sequences are created by the Logistic Mapping Technique. They obtain a new Sequence of elements using the ascendingly arranged Chaotic sequence according to the elements positioned in the Primary Sequence. Using Periodical permuted strategy, the obtained sequence is applied to permute image pixel data. The original chaotic Sequence is obtained using the permuted data of rows and columns. Initial values for the diffusion process are used to obtain Logistic System generated Chaotic Sequence. For decryption, the inverse process of the proposed encryption is followed for decrypting. i.e., using the idea of the reverse process for encryption.

Yin Dai et al. [4] suggested that Chebyshev maps and Logistic maps are been combined. To achieve maximum security, it was decided to encrypt a single image twice using two distinct kinds of encoding. It is mentioned that the height and width of the input image are first calculated. The encrypted image is then created by conducting a point-to-point XOR operation between the image and the chaotic sequence. The image is first embedded using the Logistic mapping process, and then it is encrypted again using the Chebyshev mapping method. The diagnostic image is used as the input image in the encryption procedure. However, the Cipher image is used as the input image in the Decryption Process. The concept of encrypting and decrypting in this paper is mainly based on the dimensions of image and the Chaotic sequence that is needed to be determined.

Q. N. Natsheh et al. [5] In this paper, to encrypt the multi-frame DICOM images, either the first image is used as an XOR key to encrypt the following images in the multi-frame, or a particular number of bits of a grayscale random image is used as an XOR key to encrypt the multi-frame DICOM images that are created based on the frame size. Each key block will be used to encrypt a huge number of plaintext blocks during decryption. Each frame will be converted to plain text once the key image is split into key blocks with twice the number of bytes. The goal of this article is to reduce the amount of time it takes to encrypt and decode data.

J. M. Zain et al. [6] presented a watermarking scheme in which the original image is recovered from the watermarked image. Initially, the Region of Interest (ROI) is defined around a small rectangle that is obtained from the ultrasound image. Later, The SHA-256 method is used to generate a hash value for the whole image. The SHA-256 algorithm has the benefit of being a one-way hash function, which means it can create the hash value for a given image but not the image for a given hash value. The computed hash value is then encoded in the LSB of the image's Region of Non-Interest (RONI). The watermark is extracted and the LSB values are read during tamper detection. The flipping function is then used. The retrieved image is now subjected to the SHA-256 method, which yields a hash value. If the embedded hash value matches the retrieved hash values, the picture is genuine, meaning it has not been tampered with.

A. Kannammal et al. [7] used the image in this article which is the Haar Wavelet Transformed in the spatial domain. The wavelet transformation is used to get the image texture characteristics. The ECG signals are encoded with a secret key using their texture characteristics. The Inverse Haar Wavelet Transform is used to obtain the watermarked image once it is embedded. The document solely covers the encryption of the watermark; it does not discuss the process of embedding the watermark into the DICOM image.

Osamah M. Al-Qershi et al. [8] used region of interest idea in this article throughout the embedding process. The image is characterized by a polygon, which is then split into blocks, each of which is labelled with an area of interest and a region of non-interest. To conserve RONI capability, the region of interest is compressed using the Lossy comparison approach. The average is then computed and utilised to identify any tampering. The patient's information is compressed and concatenated. Four neighbouring pixels are used to divide the region of interest. Using the DE method, the pixels are scanned and implanted. The data is then compressed using Huffman coding. The side information necessary to begin the extraction step is encoded in border blocks using the DWT technique. The location of the ROI is listed in the side information. While extracting, the inverse procedure is carried out.

Farhad Rahimi et al. [9] mainly concentrated on ROI (Region of Interest) and RONI (Region of Non-Interest) for watermark encrypting. A blind and Dual watermarking scheme is used under the contourlet domain. RONI is defined as the black area inside an image. It uses the watermark which is embedded in the singular values of contourlet sub bands and is automatically selected for ROI. It is selected by the two vectors obtained by calculating the rows and columns by using the edges of the Image. A Rectangle is formed using the automatically generated ROI. To obtain the watermarked Image, the contourlet domain and lowpass sub bands are used for embedding. Before embedding the Rectangles into the image, they are split into blocks. In the extraction process, the inverse of the contourlet domain and lowpass sub bands are employed.

Chun Kiat Tan et al. [10] employs dual-layer watermarking, which uses a reversible watermarking scheme to embed the patient's medical data and other source information into the image. Initially, the image is preprocessed to remove underflow and overflow situations, guaranteeing that the image chosen is suitable for watermarking. After that, the preprocessed image is watermarked with the source information by splitting it into 2*2 non-overlapping blocks and applying a random location signal. Using the location signal to locate the estimator during data extraction, the image is again split into 2*2 non-overlapping blocks. To protect the random location signal, public-key cryptography is employed, which encrypts the message using a pair of codes (known as the public and private key) as the first layer of watermarking. The watermark scheme in this paper uses RSA program developed by Rajatasereekul and

Kiettrisalpipop that is available online. The second layer of watermarking involves the embedding of CRC bits using the same watermark embedding procedure. CRC is the error checking code that forms the tamper detection information of the medical image. The image is initially separated into 16x16 non-overlapping pixel blocks and Cyclic Redundancy Code (CRC). Later each CRC code is included within a separate block. The image is split into 16x16 blocks again during the extraction phase, with each CRC block obtained from the watermarked image compared against the CRC block of the restored image. If both CRCs do not match, the block is considered to be tampered, and tamper localization is achieved.

## 3. CONCLUSION

In the medical industry DICOM images are extensively used but the issue of data privacy and security must be widely studied. In this Paper, The various works focused on detecting whether the DICOM image is tampered or not are presented

## REFERENCES

[1] Q. N. Natsheh, B. Li, A. G. Gale ,"Security of multi-frame DICOM images using XOR encryption approach", International Conference On Medical Imaging Understanding and Analysis 2016, MIUA 2016, 68 July 2016, Loughborough, UK

[2] Yin Dai, Xin Wang , "Medical Image Encryption Based on a Composition of Logistic Maps and Chebyshev Maps", International Conference on Information and Automation Shenyang, China, June 2012

[3] Sareh Mortajez, Marziyeh Tahmasbi, Javad Zareia, Amir Jamshidnezhad," A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images", Informatics in Medicine Unlocked, Volume 20,2020,100396,ISSN 2352-9148.

[4] JeyamalaChandrasekaran1 and S.J.Thiruvengadam, "A Hybrid Chaotic and Number Theoretic Approach for Securing DICOM Images"

[5] J.B. Lima, F. Madeiro, F.J.R. Sales," Encryption of medical images based on the cosine number transform", Signal Processing: Image Communication, Volume 35,2015, Pages 1-8, ISSN 0923-5965

[6] J. M. Zain, L.P Baldwin, M. Clarke," Reversible watermarking for authentication of DICOM images", Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Conference · February 2004

[7] A. Kannammal, K. Pavithra , S. SubhaRani , "Double Watermarking of Dicom Medical Images using Wavelet Decomposition Technique", European Journal of Scientific Research ISSN 1450-216X Vol.70 No.1 (2012), pp. 46-55

[8] Osamah M. Al-Qershi and Bee Ee Khoo," Authentication and Data Hiding Using a Hybrid ROI-Based Watermarking Scheme for DICOM Images", Journal of Digital Imaging, Vol 24, No 1 (February), 2011: pp 114Y125.

[9] JeyamalaChandrasekaran1 and S.J.Thiruvengadam, "A Hybrid Chaotic and Number Theoretic Approach for Securing DICOM Images"

[10] Farhad Rahimi and Hossein Rabbani," A dual adaptive watermarking scheme in contourlet domain for DICOM images ", Rahimi and Rabbani BioMedical Engineering OnLine 2011, 10:53 http://www.biomedical-engineering-online.com/content/10/1/53