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 for Tamper detection of Medical Images

Pruthvi Dinesh[1], Varsha M S[2]

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

Abstract - *Medical imaging techniques are widely used in the medical sector; therefore, they must be thoroughly investigated, especially in terms of security and data privacy. Using networks to send medical images exposes you to a variety of security risks. As a result, a safe and trustworthy method of transmitting medical images over the Internet is needed. The suggested method embeds a watermark in medical images and identifies whether the image is tampered or not.*

Key Words: Security, Watermark, Tamper

1.INTRODUCTION

The foundation of today's health-care infrastructure is digital information technology. Medical data analysis methods have evolved considerably in recent years as a result of rapid and significant developments in information and communication technologies. The exchange of datasets between hospitals over dependable transmission lines is one of the most important functions of a medical data management system. 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. Recent advancements in information and communication technology have made it simpler to modify and reproduce medical images while also providing new means to access, organize, and transport them. Security measures in medical information systems are commonly regarded to be urgently necessary. Images/messages can be encoded invisibly via digital watermarking. To ease the capacity constraint by decreasing storage and transmission costs, data hiding methods are employed to interleave patient data with medical images. These data hiding techniques may also be utilized for authentication and tamper detection in order to assess the integrity and fidelity of images. This paper focuses mainly on embedding a watermark on medical images and also detecting if that medical image is tampered or not. Section 2 presents the state of Art. Section 3 presents comparison and challenges. Section 4 presents the Methodology. Section 5 concludes the paper.

1.1 Literature Survey

Gull.S et al. [1] This paper presents the Fragile watermarking technique for tamper detection and localization in medical/general images. For a 1bit per pixel (1bpp) payload, it achieves an average PSNR of 51.26db. In embedding process logical AND, XOR operations are used to perform zero of every block of each pixel to set LSB and first intermediate significant bit (ISB). And for tamper localization embeds the bits stream into LSB into each UHB pixel. The watermarked images are divided into dimensions during extraction, and the two LSBs of each block are set to zero, followed by a logical XOR operation, which checks the computed mean and extracted logo data, ensuring that the block is not tampered if the values match. Here the pixel blocks are divided into 2 parts UPB (upper pixel block) and LPB (lower pixel block), Where these blocks are used to create two-bit streams that can be utilized for tamper detection and localization.

Seng, Woo et al. [2] In this paper multiple watermarking of medical images is presented, it consists of two parts, annotation part where this part can store the patient information with privacy and security, and fragile part is used to detect the tampering. Medical image which represents soft and hard tissue are used in this experiment. Here the watermarked images are measured in weighted PSNR. Off-the shelf image processing software is used to perform the attacks like noise insertion, JPEG compression and copy attack to find out the effectiveness of fragile watermark. In detection annotation part is detected separately which is similar to the embedding steps and fragile part is detected separately. So, this paper presents good visual quality of watermarked images.

J. M. Zain et al. [3] The primary goal of this article is to check the medical images' integrity and validity. This approach requires a secret key and a public chaotic mixing algorithm to recover and embed altered images. The main characteristics of this paper are Confidentiality, Reliability and Availability. Each block of 8x8 pixels is subdivided into 4x4 pixels, with each sub block being a 3-tuple watermark. This 3-tuple watermark is placed in the LSB of the 3x3 block. In detection if the sub blocks are tampered of the block 8x8 pixel block then mark it as tampered otherwise it is not tampered. Here the test image is watermarked with PSNR of 54.8db for one experiment and for another they watermarked image by adding the clone. This results in recovery of all tampered areas for spread tampered blocks.

O. M. Al-Qershi et al. [4] Here if there is no manipulation, the original medical images may be retrieved exactly from the watermarked image. If it is tampered ROI (Region of Interest), it can be recovered lossless. Reversible and Irreversible are the two techniques of watermarked images. This paper presents reversible ROI-based technique for

maintaining secrecy of patient's data and to verify authentication of ROI and to recover the tampered areas inside the ROI. Here the DE-based data hiding scheme is used. ROI of hash message is compared and calculated with the obtained one, if they are equal, then the image is said to be not tampered and if they are not equal the image is tampered and that tampered are will be recovered. In the watermarked images, pixel values inside ROI will be substituted by RONI for recovery and tamper localization. In hiding capacity and visual quality, it shows very good performance.

Guo X et al. [5] In this paper the proposed scheme is used for local authentication information using only one lossless watermarking. It allows the user to easily adjust the precision of the localization and detects tampering. During detection, the derived watermark payload is validated using a region-based lossless watermarking method. The watermarked image can be utilized for diagnostic purposes as well as other medical applications. The reversible watermarking technique will be used to gather and implant the original information that was lost due to the irreversible watermarking system, which may cause substantial trouble in medical applications. Because the outside work of ROI is limited while embedding, watermarked images can be utilized securely in medical applications.

Al-Haj et al. [6] In this study, crypto-watermarking is used to assure the legitimacy, integrity, and confidentiality of medical images sent over public networks. This cryptography is adopted by DICOM (Digital Imaging and Communication in Medicine) standard to provide integrity and authenticity, so cryptographic watermarks like hash codes, digital signatures and cyclic redundancy codes will be used for implementation of integrity and authenticity. In embedding the bit pattern is inserted for three watermarks in RONI of each sub-band, the three watermark contains patient's information, hospital logo and the hash watermark. Here the inverse SVD and DWT (Discrete Wavelet Transform) is applied to produce the final watermarked image. In extraction verification of authentication will be done only if the received and expected watermark is matched. PSNR is used for better assessment as an imperceptibility object and obtained some values to it for X-ray, MRI images…etc.

Eswaraiah Rayachoti et al. [7] A unique block-based delicate medical image watermark approach is proposed in this study. It locates the tampering inside the ROI. The original ROI will be recovered when it is tampered. Here the most important point is ROI for making diagnosis and the ROI is represented by enclosed polygon. In this ROI pixels, RONI pixels and border pixels are segmented. So, this experiment can be used in multiple ROI areas. For embedding the three segment pixels are taken and the hash value should be calculated and divide the pixels in ROI and calculate the average of each block of ROI and then embed the LSB'S and encrypt the information using secret key. In extraction the encrypted watermarked medical images will be extracted and decrypts the extracted information from ROI. This uses only 8-bit authentication and complexity is less and uses simple calculation method less and uses simple calculation method for recovery of data and authenticity.

A. Shehab et al. [8] This paper presents the SVD (Singular Value Decomposition) based watermarking technique. SVD can be directly applied on the medical images. This experiment is tested on various attacks like text insertion, text removal, and copy paste attacks and effectively prevented these attacks. Cryptography technique and fragile watermarking technique is used for verification. The Arnold transform has been utilized for embedding process which provides reliability and security for hiding the medical images. FPR (False positive rate), FNR (False negative rate), TDR (Tamper detection rate), PSNR (Peak signal to noise ratio), and NCC (Normalized cross correlation) are calculated. For vector quantization attack self-recovery bits and authentication is used. It is highly reliable and efficient for attacked blocks.

R.F. Olanrewaju et al. [9] This technique is used for detection of the forgery watermarks of medical images, also detects and embeds mammogram using CVNN (Complex Valued Neural Network). For improvement of diagnosis, CVNN based technique is used. The mammogram medical images contain the diagnostics information of breast cancer and other breast abnormalities and also can be used for detection. In mammogram the diagnostic information should not include with embedding watermark. Because the watermarks are inserted in phase or magnitude of the image, some information may be lost while embedding. DCT, DWT, DFT is used to prevent the robust attacks while transfer of host image from spatial to frequency domain is done. This experiment gives good blind detection.

Siau-Chuin Liew et al. [10] This paper proposes a simultaneous digital watermarking approach for multi-frame medical images. The time required for parallel watermarking is significantly less than that required for sequential watermarking. The major goal here is to keep the patient's information private and secure, as well as to avoid image manipulation. The tampered region can be retrieved by obtaining the image's original pixel values. Parallel processing on multicores was implemented to save time, and the watermarking operation is now completed concurrently. Imperceptibility, elapsed time and robustness to tampering are the three important performance metrics. When the performance of hardware and software is inadequate, a capacity and capability problem develop in the sequential watermark process. To improve the speed of multi-frame watermarking process time the parallel watermark process is used.

1.2 Comparison and challenges

SL.NO	METHODOLOGY	ADVANTAGES	DISADVANTAGES
[1]	Fragile watermarking technique used for Tamper detection.	Lesser computational complexity, High image fidelity and better payload.	Correction of detected tampered areas cannot be done.
[2]	For privacy management and tamper detection, many watermarking methods are used.	It stores the patient information with security and privacy and helps to reduce storage space.	Stored information can be destroyed using malicious attack technique.
[3]	Watermarking method for detecting and recovering tampered medical images.	Integrity Verification and Authentication of Medical Image.	Case study in school cannot be done and also patient's confidential information cannot be disclosed.
[4]	ROI-based technique of watermarking for medical images.	It helps to hide patient's data with high capacity.	Multiple-ROI concept cannot be added for more practicable in medical informatics.
[5]	Region-based lossless watermarking scheme of medical images.	It can be used for diagnostic purpose and it makes algorithm simple and sensitive.	The authentication information could not be retrieved by the watermark decoder.
[6]	Crypto-watermarking algorithm which uses multiple watermarks.	It provides confidentiality, authenticity and integrity for the medical images.	Multi-slice and multi-frame cannot be handled.
[7]	Block based fragile medical image watermarking technique.	Provides high quality watermarked medical images.	It is unable to decrease embedding distortion and restore pixels within ROI.
[8]	SVD based fragile watermarking of sensitive medical images.	Copy and paste attacks, content removal attacks, and text addition attacks are all prevented.	Detection on other tampering issue cannot be done, such as image resize and rotate operations.
[9]	Detecting forgery in medical watermarked images using CVNN.	Good blind detection can be done.	This can't test the effect of various activation function list.
[10]	Digital watermarking on multi frames medical image.	Speeds up multi frames watermarking processing time.	It cannot be applied for MRI scan and nature images.

2. PROPOSED APPROACH

The Algorithm used for Watermark Embedding is Modification of Discrete Cosine Transform Coefficients. The method for including the Watermark picture in the Cover Medical Image is as follows.

1. First, the scaling factor is defined. It must be more than zero; nevertheless, the higher the value, the less visible the image becomes.
2. Read the medical image called the Host Image, which is of the Unsigned Integer Type. (HI)

3. Convert that image which is Unsigned Int type into **double** type. **(Host_image)**

Normally, the double function is employed to improve the image's accuracy.
Frequency data is converted to double precision using double. Because Frequency data does not support symbolic values, it must be converted.
If users try to insert a watermark straight into an Unsigned integer host image, there is a risk losing some information, whether it's from the host image or the watermark image.
But this **double** data type cannot be displayed using normal image processing applications. So, at the end we will be converting back **double** data to unsigned integer format.

4. Discrete Cosine Transform is to be used.

The average value of the spatial host image will be stored as the first Pixel of the frequency domain of the image.
In frequency domain, just a little amount of time is required for high frequencies, and changes occur quickly. Low frequencies, on the other hand, take more time and the effects are more gradual.

5. Using the Procedure of Discrete Cosine Transform we obtain the PSNR (Peak Signal to Noise Ratio) value.
6. The PSNR (Peak Signal to Noise Ratio) is calculated by comparing the Spatial domain used before the Discrete Cosine Transform alteration to the Spatial domain used after the Discrete Cosine Transform modification.

The watermarked picture is deemed to be corrupted if the PSNR value is less than 0.99. The watermarked image is considered to be not corrupted if the value is higher than 0.99.

7. Obtain Discrete Cosine Transformed Image (DCT_H)

Parallelly, Watermark Image will be read which will be in the Unsigned Integer Type and Display it (W).

8. Convert that image into **double** type. **(Watermark)**

Using the following procedure, obtain the Discrete Cosine Transform of the Watermark Embedded Host Image.

DCT_WI=DCT_H * (1 + Scaling Factor * Watermark)

On a double-type watermark image that will be saved as a tiff file, use the Inverse Discrete Cosine Transform. Tagged Image File Format (TIFF) is a variable-resolution bitmapped image format. Tiff files are normally of high quality and takes more storage.

9. Convert the double type into unsigned integer type and display
10. Get the Unsigned Integer Type Peak Signal to Noise Ratio of the watermark image and the Host Image.

(PSNR)Peak Signal to Noise Ratio and (SSIM)Structural Similarity Index Measures are obtained after the embedding of Watermark to the Host image.

The Algorithm used for Watermark Extraction is based on getting the Discrete Cosine Transform Coefficients of the Watermarked Images. The technique for recovering the Watermark image is known as the Reverse process of Watermark embedding. If the watermark image extracted is same as that of while embedding, the image is said to be not tampered. If the watermark image extracted is not same as that of while embedding, the image is said to be tampered
The following is the procedure for extracting the Watermark image from the Integrated Medical Image.

1. Read the original image and the watermarked image.

These images are already in double type and this needs to be converted to unsigned integer type to display

2. The Discrete Cosine Transform of the Watermarked Image and the Original Image are required to extract the Watermark from the Watermarked Image.

The Extracted Watermark is obtained by dividing the quotient of the Discrete Cosine Transform of the Watermark Image and the Host Image by the scaling factor.

Ex_W= ((DCT_WI / DCT_HI) - 1) / scale

3. Convert the retrieved Watermark to an unsigned integer type in order to display it, as double type formats do not allow data to be displayed.
4. Compare the original image to the watermarked image to see whether the image has been tampered with. If the image is blurred, flipped or rotated, then the image is said to be tampered.

SSIM (structural similarity index measures) is performed for watermark and extracted watermark image to find whether the image is tampered or not tampered.

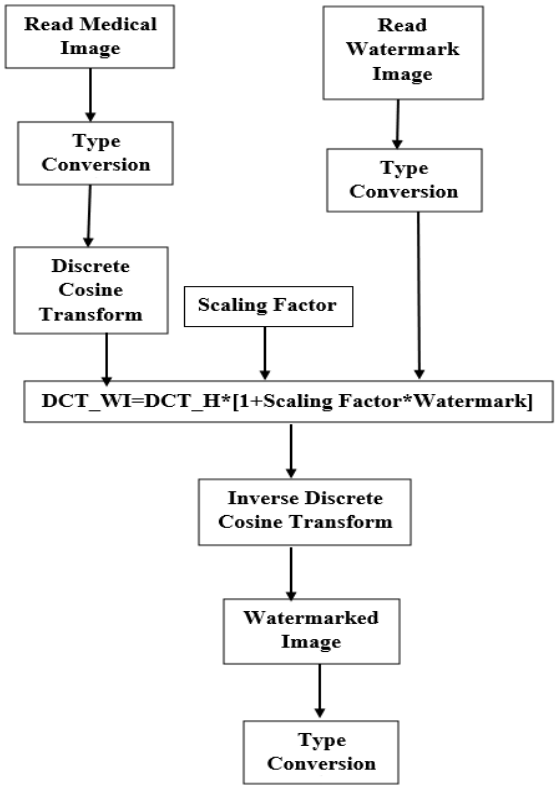

Fig. 1: Embedding Flowchart

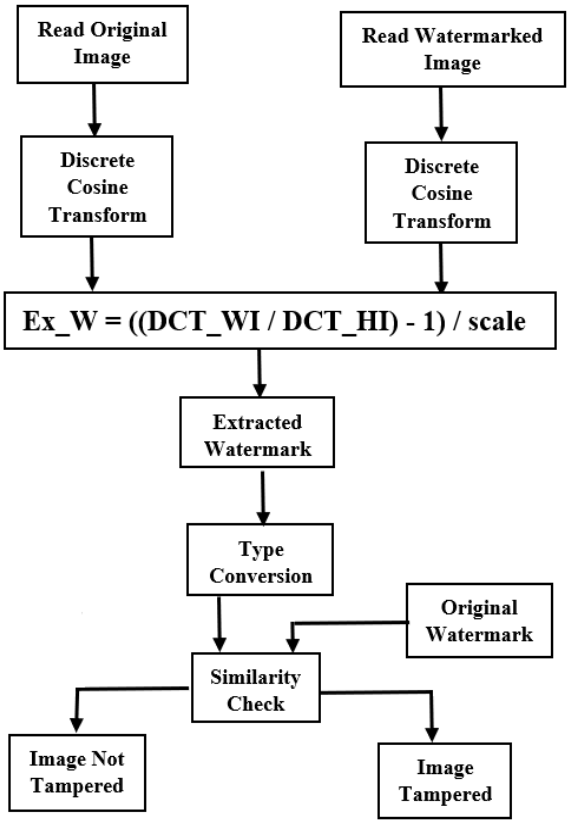

Fig 2: Extraction Flowchart

3. CONCLUSIONS

Medical imaging techniques must be extensively assessed since they are widely used in the medical profession, particularly in terms of data security and privacy. `The proposed technique in this paper focuses on the reliability and security of transmitting medical images. Here, an encrypted watermark is included on medical images. Detecting whether or not the medical image has been manipulated with is also a priority.

Using DCT for embedding, the medical image is secured. By using inverse DCT for extracting medical images is said to be tampered or not.

REFERENCES

[1] Gull, S., Loan, N.A., Parah, S.A. et al. An efficient watermarking technique for tamper detection and localization of medical images. J Ambient Intell Human Comput 11, 1799–1808 (2020).

[2] Seng, Woo & Du, Jiang & Pham, Binh. (2005). "Multiple Watermark Method for Privacy Control and Tamper Detection in Medical Images". Proc. APRS Workshop on Digital Image Computing Pattern Recognition and Imaging for Medical Applications.

[3] J. M. Zain and A. R. M. Fauzi, "Medical Image Watermarking with Tamper Detection and Recovery, "2006 International Conference of the IEEE Engineering in Medicine and Biology Society, 2006, pp. 3270-3273

[4] O. M. Al-Qershi and B. E. Khoo, "ROI-based tamper detection and recovery for medical images using reversible watermarking technique," 2010 IEEE International Conference on Information Theory and Information Security, 2010, pp. 151-155, doi: 10.1109/ICITIS.2010.5688743.

[5] Guo X, Zhuang TG. Lossless watermarking for verifying the integrity of medical images with tamper localization. J Digit Imaging. 2009;22(6):620-628. doi:10.1007/s10278-008-9120-5

[6] Al-Haj, A., Mohammad, A. & Amer, A. Crypto-Watermarking of Transmitted Medical Images. J Digit Imaging 30, 26–38 (2017)

[7] Eswaraiah Rayachoti and Sreenivasa Reddy Edara, "Block Based Medical Image Watermarking Technique for Tamper Detection and Recovery", https://arxiv.org/abs/1412.6143

[8] A. Shehab et al., "Secure and Robust Fragile Watermarking Scheme for Medical Images," in IEEE Access, vol. 6, pp. 10269-10278, 2018, doi: 10.1109/ACCESS.2018.2799240.

[9] R.F. Olanrewaju, Othman. O. Khalifa, Aisha- Hassan Hashim, Akram M. Zeki and A.A. Aburas International Islamic University Malaysia (IIUM) P.O Box 10, 50728, Kuala Lumpur, Malaysia

[10] Siau-Chuin Liew,[1] and Jasni Mohd. Zain[1,] "Parallel Digital Watermarking Process on Ultrasound Medical Images in Multicores Environment", https://doi.org/10.1155/2016/9583727