IFERP
ISSN (Online) 2394-2320
International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 9, Issue 9, September 2022

A Reversible Digital Image Watermarking Technique for Integrity and Authenticity of MR Images

[1] Manohar Gosul, [2] Nisarg Gandhewar

[1] Research Scholar, Department of CSE, Dr. A.P.J. Abdul Kalam University, Indore, Madhya Pradesh, India
[2] Professor, Department of CSE, Dr. A.P.J. Abdul Kalam University, Indore, Madhya Pradesh, India

Abstract— ***Digital Watermarking is the art and science of embedding information in existing digital content for Digital Rights Management (DRM) and authentication. Reversible watermarking is a class of (fragile) digital watermarking that not only authenticates multimedia data content, but also helps to maintain perfect integrity of the original multimedia "cover data". Watermarking of digital images is a well-known technique that is widely used for securing image contents. A successful watermarking method must be accurate, reversible, resilient, and robust against various attacks. The technical revolution associated with the implementation the development of digital technologies in medicine, has led to the emergence and active development of new directions in many areas of medicine. The authenticity and integrity of medical images has to be protected. Hence in this paper a reversible digital image watermarking technique for integrity and authenticity of MR (Magnetic Resonance) images is presented. Reversible watermarking is recognized as a robust approach to confirm the integrity and authenticity of medical images and to verify that alterations can be detected and tracked back.***

Index Terms— ***Digital watermarking, Reversible watermarking, medical images and Magnetic Resonance images***

I. INTRODUCTION

Image protection copyrights have become a matter of serious concern because of the reach and popularity of the Internet and the rapid development of multimedia technology. Furthermore, digital image copyrights have attracted progressively increasing attention. Nowadays, along with the improvements in technology, information security techniques have also been developed. Among these techniques, digital watermarking has emerged recently as a potential solution for protecting and securing digital images and their contents [1]. The technical revolution associated with the implementation the development of digital technologies in medicine, has led to the emergence and active development of new directions in many areas of medicine [2]. In most medical imaging domains, traditional diagnosis has mostly migrated to e-diagnosis workflows. Hospital Information Systems (HIS) and medical imaging platforms generate and manage digital images across many modalities including X-ray, Ultrasound, Magnetic Resonance (MR), Computerized Tomography (CT), etc. Images taken in a hospital are saved in the Picture Archiving and Communication Systems (PACS), and are typically managed within a digital workflow based on the Digital Imaging and Communications in Medicine (DICOM) standard.

The transmission of these medical images through, and across, hospitals, locations and administrative organizations, has become a common practice for many purposes within the digital medical workflow. These include diagnosis, treatment, training, distance learning and

medical consultation between clinicians and radiologists. In most cases, this is within the defined workflows of the PACS systems, but there are also many cases, both valid and occasionally nefarious, in which images and data are withdrawn from one system to be transferred to other institutions or people. During the process of production and exchange, medical images can be intentionally, or unintentionally, tampered with. Tampering these images could result in misdiagnosis [3]. This potentially has serious implications on the diagnosis of patients with possible life affecting impact outcomes, mortality, etc. Therefore, the ability to maintain the integrity and authenticity of these images has become significant, both within the internal systems and during their transfer to other systems.

Digital image watermarking is simply the digital watermarking of an image, which provides an alternative solution for ensuring tamper-resistance, the ownership of intellectual property, and reinforcing the security of multimedia documents. Any digital content, such as images, audio, and videos, can hide data. Digital content can easily be illegally possessed, duplicated, and distributed through a physical transmission medium during communications, information processing, and data storage.

Medical image watermarking approaches can be classified into three schools: conventional methods, Region of Interest (ROI), Region of Non Interest (RONI), and reversible approaches. The reversible watermarking techniques are used to avoid irreversible distortion in image by extracting the original image exactly at the receiver end. The reversible watermarking is a special application of digital watermarking [4]. Reversible image watermarking embeds the information into the carrier image on the premise of ensuring the visual quality. The purpose is to losslessly reconstruct the host image after the watermark is extracted. Therefore, compared with the traditional watermarking methods, the amount of embedding information is more demanding; hence, it has more extensive research and application value in the fields of judicial, military, medical, and other fields which ask for high-image authenticity and integrity. The basic goal of the reversible image watermarking algorithms is to achieve the maximum embedding capacity of effective information with less distortion.

In medical domains, if an image is modified during the workflow process a collapse in trust regarding the validity of the images is formed. Potentially, any small change to the image could lead to misdiagnosis or uncertainty, with possible life-threatening consequences or legal implications. Consequently, retrieval of the original data from the modified image is essential. Reversible or lossless watermarking approaches fulfill this requirement in that they guarantee the extraction of the watermark and full retrieval of the unmodified original image. Therefore, fully reversible watermarking techniques, which can completely recover both the original unmodified image and the embedded watermark are developed in this paper to provide privacy and integrity of MR images.

II. LITERATURE SURVEY

Xiang Hou, Lianquan Min, and Hui Yang et. al., [5] presents A Reversible Watermarking Scheme for Vector Maps Based on Multilevel Histogram Modification. To protect the security of vector maps, we propose a novel reversible watermarking scheme for vector maps based on a multilevel histogram modification. The experimental results show that the proposed algorithm has good invisibility and is completely reversible.

Mohammad Shahab Goli, Alireza Naghsh et. al., [6] has introduced a New Method Robust against Crop Attack in Digital Image Watermarking Using Two-Step Sudoku. In this method, the watermark image is scattered in two sudoku table layouts with different solutions and is watermarked in the host image. Using this method, the watermark image is repeated 81 times in the host image, and to this effect the watermark image can be reconstructed using other segments when cropped by the attacker.

Zhengwei Zhang, LifaWu, Yunyang Yan, Shaozhang Xiao and He Sun et. al., [7] presents An improved reversible image watermarking algorithm based on difference expansion. To improve the visual quality and the embedding rate of the existing reversible image watermarking algorithm, an improved reversible image watermarking algorithm based on difference expansion is proposed. First, the watermark information is divided into groups, and the information value of each group is calculated.

Khalil Shekaramiz, Alireza Naghsh et. al., [8] presents Embedding and Extracting Two Separate Images Signal in Salt & Pepper Noises in Digital Images based on Watermarking. Since the salt & pepper noises are placed randomly throughout the image, the pixels' information of the two separate images can be replaced into the salt & pepper noises peer to peer, and then this embedded information in noises is extracted in other applications, and noises from these three images will be removed.

Irshad Ahmad Ansari, Millie Pant & Chang Wook Ahn et. al., [9] presents Artificial bee colony optimized robust-reversible image watermarking. The present study is focused on the development of lossless watermarking method that can fulfill five basic requirements (robustness, reversibility, invisibility, security and capacity) of ideal lossless watermarking scheme maximally.

R. Lakshmi Priya and V. Sadasivam et. al., [10] presents Protection of Health Imagery by Region Based Lossless Reversible Watermarking Scheme. The scheme combines hashing, compression, and digital signature techniques to create a content dependent watermark making use of compressed region of interest (ROI) for recovery of ROI. The experiments were carried out to prove the performance of the scheme and its assessment reveals that ROI is extracted in an intact manner.

LLukman Çerkezi, Gökçen Çetinel et. al., [11] presents RDWT and SVD Based Secure Digital Image Watermarking Using ACM (Arnold Cat Map). In this study, digital image watermarking method based on Redundant Discrete Wavelet Transform (RDWT) and Singular value Decomposition (SVD) is proposed. By exploiting the complexity property of the chaotic signals, which is the main reason of using them in the security applications, the robustness and the invisibility of the proposed method is improved.

Anu Bajaj et. al., [12] presents Robust And Reversible Digital Image Watermarking Technique Based On RDWT-DCT-SVD. Hybrid image watermarking technique is proposed in this paper which takes the advantages of different transforms like RDWT, DCT (Discrete Cosine Transform), SVD and trigonometric functions. To measure the effectiveness of the method, the correlation based extraction mechanism is used with the tolerance level of 0.8 for robustness.

Arijit Kumar Pal, Nilanjan Dey, Sourav Samanta, Achintya Das, Sheli Sinha Chaudhuri et. al., [13] presents A Hybrid Reversible Watermarking Technique for Color Biomedical Images. In this present work a reversible watermarking method (Odd-Even Method) is used for watermark insertion and extraction in a bio medical image with large data hiding capacity, security as well as high watermarked quality.

Neeraj Bhargava, M.M. Sharma, Abhimanyu Singh Garhwal and Manish Mathuria et. al., [14] presents Digital Image Authentication System Based on Digital Watermarking. The complete system consists of two functions, one for hiding information inside image and other for detecting information from image. In this approach,

IFERP
ISSN (Online) 2394-2320
International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 9, Issue 9, September 2022

digital watermarking performed using Discrete Wavelet Transform (DWT) and analyzed its results.

Koushik Pal, Goutam Ghosh, Mahua Bhattacharya et. al., [15] presents Reversible Digital Image Watermarking Scheme Using Bit Replacement and Majority Algorithm Technique. In this paper an indigenous approach is described for recovering the data from the damaged copies of the data under attack by applying a majority algorithm to find the closest twin of the embedded information.

III. REVERSIBLE DIGITAL IMAGE WATER MARKING TECHNIQUES

A reversible digital image watermarking technique for integrity and authenticity of MR images is presented. The block diagram of presented technique is shown in Fig. 1. For a secure communication model, the digital image watermarking process consists of a watermark embedding part and a watermark extraction part.

In the watermark embedding part, at first, the cover image is pre-processed, and then, its entropy is evaluated to find the integrating capacity information of the image. Then, using an optical image encoding method, the encoder embeds a watermark image into the high entropy value of the host image by using a secret key. Then, the system achieves the amplitude and phase shaping information of a laser beam and generates the watermarked image. In the watermark extraction step, the watermarked image is pre-processed. After that, the system extracts the amplitude and phase shaping information of the laser beam patterns. Then, the entropy of these beam patterns is evaluated. A high entropy value is selected for extracting the watermark, in order to ensure better integrity and authenticity.

Magnetic resonance (MR) spectroscopy is a non-invasive diagnostic test for measuring biochemical changes in the brain, especially the presence of tumors.

MRI (Magnetic Resonance Imaging) uses a strong magnetic field and radio waves to create detailed images of the organs and tissues within the body. In this approach brain MR images are used. The scheme segments images into two parts; the Region of Interest (ROI) and the Region of Non Interest (RONI). Watermark data is encoded into the ROI using reversible watermarking. A selected subset of samples within a dataset identified for a particular purpose. In computer vision, the ROI defines the borders of an object under consideration to perform some operation on it and RONI indicates the background of image.

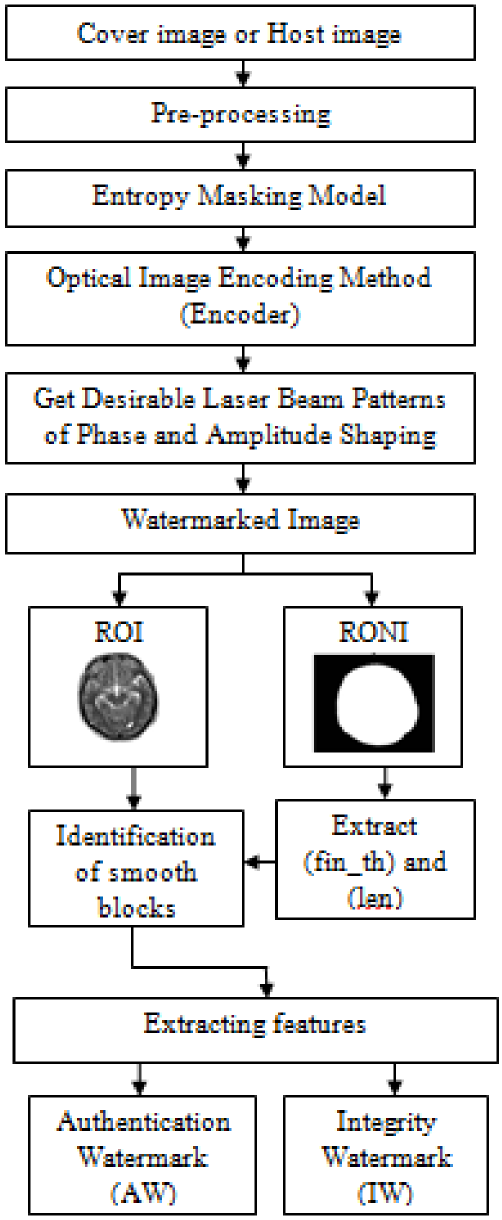

Fig. 1: BLOCK DIAGRAM OF PRESENTED REVERSIBLE DIGITAL IMAGE WATERMARKING TECHNIQUE

In addition to the image raw data, DICOM (Digital Image and Communications in Medicine) defines a structure for describing the image. This structure is located in the image's header and called metadata. DICOM metadata comprises tables of attributes which record key information including time of image acquisition, device parameters, imaging conditions, diagnosis result, and essential patient details such as the name, ID number, age, gender, weight, and height. Some metadata fields are changed each time the image is distributed whilst others remain constant. Therefore, only information related to the patient and image (i.e. the constant data) must be used to ensure the authenticity.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 9, September 2022

The Digital Signature (DS) of the original medical image is calculated utilizing the Message Digest (MD5) algorithm. The MD5 is a cryptographic hash function that generates a 128-bit Message Authentication Code (MAC). Any change to the image, either intentional or accidental, leads to change in the hash code. Comparing the base and retrieved codes enables identification of image manipulation. In this research, the DS of the entire image is computed and encoded into the medical image to offer strict integrity watermark (IW).

Most medical images have a large smooth area, which is defined the regions that have little significant difference between the adjacent pixels intensity values, compared to the other images. Embedding the watermark into these regions is less noticeable to the human eye. Consequently, the watermark was encoded in smooth areas inside ROI to decrease the degradation of the watermarked image. If adopting one of the existing techniques to determine the smooth regions, then when trying to identify the smooth regions to extract the encoded data, some of the identified smooth blocks will not precisely match the original blocks. Consequently, there is no guarantee that all pixels employed to discover the watermark will be similar to those utilized in the hiding process. This leads to the inability of the algorithm to extract the encoded data and recover the original image precisely.

A simple new algorithm is presented to determine the smooth regions inside the ROI of the medical image, such that when applying this algorithm to the watermarked image, it generates the same smooth blocks used at both embedding and extraction. This enables a precise extraction of the embedded data in the watermarked image without the need for any additional information (e.g. location map). The algorithm segments the ROI into non-overlapping blocks of 3 × 3 pixels which are separately evaluated and classified as either smooth or non-smooth blocks. The len and fin_th values are extracted. len is the length of the watermark data, fin_th is the final threshold used to identify the smooth blocks.

The watermarked image is segmented into ROI and RONI. After the image has been segmented to ROI and RONI and the smooth blocks inside ROI have been identified, the generated watermark data can be encoded. Smooth blocks inside ROI are then identified. Watermark is extracted from the identified smooth blocks. The watermark is compared to the recalculated watermark of the extracted image to verify the authenticity and integrity of the image.

The extracted watermark is decompressed using the RLE (Run Length Encoding) method. It is divided into two watermarks; the authentication watermark (AW), and the integrity watermark (IW). These watermarks are compared to the recalculated metadata and DS of the extracted DICOM image to confirm authenticity and integrity of the image. This can be achieved by calculating the number of error and correct bits between the extracted and recalculated watermarks.

IV. RESULT ANALYSIS

In this section, the result analysis of a Reversible digital image watermarking technique for authenticity and integrity of MR images is discussed. This work ensures the authenticity and integrity of MR images. Authenticity and integrity of the pixel data and header information of the watermarked image are confirmed, if and only if, the embedded watermark and original image can be retrieved correctly and exactly matched.

Manipulations of the image data also corrupts the embedded watermark resulting in a mismatch between original and retrieved watermarks. The original image, watermark image and extracted images are shown in Fig. 2.

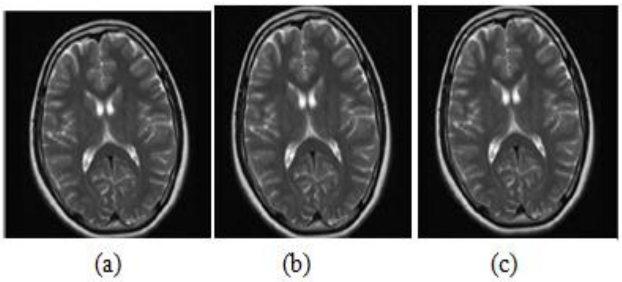

Fig. 2: (a) ORIGINAL IMAGE, (b) WATERMARKED IMAGE and (c) EXTRACTED IMAGE

The Fig. 2 indicates the Example of the original MR images and their corresponding watermarked, extracted and the difference between the original and extracted images. There is no visible difference between the original and watermarked images and no numerical difference between the original and extracted images.

PSNR (Peak Signal to Noise Ratio) and BER Bit Error Rate are used to assess reversibility and ability to recover the embedded watermark after applying image processing operations simulating both intentional and unintentional modifications.

Peak Signal to Noise Ratio (PSNR): It is a basic measure used to estimate the distortion amount between the original and watermarked images. A higher PSNR value indicates lower distortion.

$$PSNR(I_o, I_w) = 10 \times log_{10} \frac{MAX_I^2}{MSE} \ldots \quad (1)$$

Where MAX_I represents the highest possible pixel value of the input images and MSE is the Mean Squared Error between the original and watermarked images.

Bit Error Rate (BER): It is expressed as

$$BER = \frac{Number\ of\ Error\ bits}{Total\ number\ of\ watermark\ bits} \quad (2)$$

The PSNR of presented techniques is very high compared to other reversible watermarking techniques and the BER values are approximately equal to zero. This indicates that the embedded watermark can be recovered at the extraction without any loss. If the image has very less noise and without errors then the image authenticity and integrity will be very high. The authenticity and integrity of presented system is shown in Below Fig. 3.

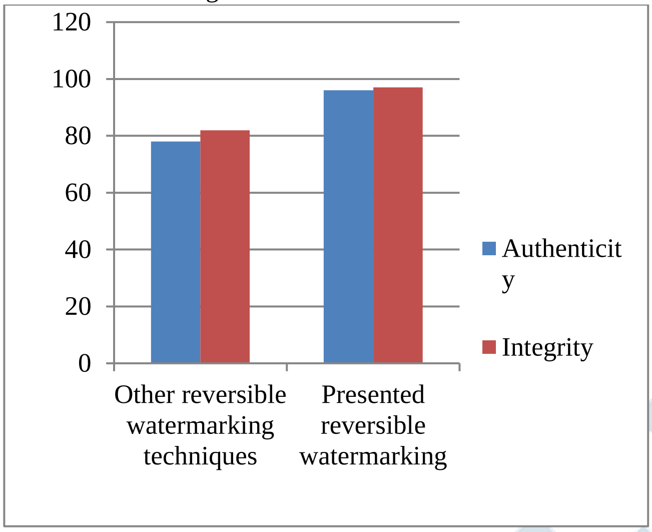

Fig. 3: AUTHENTICITY AND INTEGRITY COMPARISION GRAPH

Therefore, this reversible digital image technique has higher integrity and authenticity for MR images compared to earlier techniques.

V. CONCLUSION

In this paper a reversible digital image watermarking technique for integrity and authenticity of MR images is presented**.** This approach segmented as two parts namely: ROI and RONI. For a secure communication model, the digital image watermarking process contains a watermark embedding part and a watermark extraction part. In the water embedding part, the image data is preprocessed and its entropy is evaluated. the watermark data in each smooth block are selected from the ROI. The exact original images are retrieved after extracting the embedded watermark successfully. Based on the methodology of the optical image encoding technique, which hides the data in the difference values of pixels pairs, the proposed scheme encodes the watermark into the smooth blocks inside ROI. Experimental results indicate that this technique achieves superior performance in terms of distortion level, PSNR and BER compared to other esssssssarlier methods. So, this reversible digital image watermarking technique effectively improves the integrity and authenticity of MR images.

REFERENCES

[1] Khalid M. Hosny, Mohamed M. Darwish, “Reversible Color Image Watermarking Using Fractional-Order Polar Harmonic Transforms and a Chaotic Sine Map”, Circuits, Systems, and Signal Processing, 2021 Springer, doi.org/10.1007/s00034-021-01756-z

[2] Xiaoyi Zhou, Yue Ma, Qingquan Zhang, Mazin Abed Mohammed and Robertas Damaševičius, “A Reversible Watermarking System for Medical Color Images: Balancing Capacity, Imperceptibility, and Robustness”, Electronics 2021, 10, 1024, doi.org/10.3390/electronics10091024

[3] Nisar Ahmed Memon And Ali Alzahrani, “Prediction-Based Reversible Watermarking of CT Scan Images for Content Authentication and Copyright Protection”, IEEE Engineering In Medicine And Biology Society Section, 2020, doi: 10.1109/ACCESS.2020.2989175

[4] Zhengwei Zhang, Mingjian Zhang, and Liuyang Wang, “Reversible Image Watermarking Algorithm Based on Quadratic Difference Expansion”, Hindawi Mathematical Problems in Engineering, Volume 2020, Article ID 1806024, 8 pages, doi.org/10.1155/2020/1806024

[5] Xiang Hou, Lianquan Min, and Hui Yang, “A Reversible Watermarking Scheme for Vector Maps Based on Multilevel Histogram Modification”, Symmetry 2018, 10, 397; doi:10.3390/sym10090397

[6] Mohammad Shahab Goli, Alireza Naghsh, “Introducing a New Method Robust Against Crop Attack in Digital Image Watermarking Using Two-Step Sudoku”, 3rd International Conference on Pattern Recognition and Image Analysis (IPRIA 2017) April 19-20, 2017

[7] Zhengwei Zhang, LifaWu, Yunyang Yan, Shaozhang Xiao and He Sun, “An improved reversible image watermarking algorithm based on difference expansion”, International Journal of Distributed Sensor Networks 2017, Vol. 13(1), DOI: 10.1177/1550147716686577

[8] Khalil Shekaramiz, Alireza Naghsh, “Embedding and Extracting Two Separate Images Signal in Salt & Pepper Noises in Digital Images based on Watermarking”, 3rd International Conference on Pattern Recognition and Image Analysis (IPRIA 2017) April 19-20, 2017

[9] Irshad Ahmad Ansari, Millie Pant & Chang Wook Ahn, “Artificial bee colony optimized robust-reversible image watermarking”, Multimed Tools Applications, 2016 Springer, DOI 10.1007/s11042-016-3680-z

[10] R. Lakshmi Priya and V. Sadasivam, “Protection of Health Imagery by Region Based Lossless Reversible Watermarking Scheme”, Hindawi Publishing Corporation The Scientific World Journal, Volume 2015, Article ID 489348, 10 pages, doi.org/10.1155/2015/489348

[11] LLukman Çerkezi, Gökçen Çetinel, “RDWT and SVD Based Secure Digital Image Watermarking Using ACM”, 2016 IEEE, 978-1-5090-1679-2/16

[12] Anu Bajaj, “Robust And Reversible Digital Image Watermarking Technique Based On RDWT-DCT-SVD”, IEEE International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), August 01-02, 2014

[13] Arijit Kumar Pal, Nilanjan Dey, Sourav Samanta, Achintya Das, Sheli Sinha Chaudhuri, “A Hybrid Reversible Watermarking Technique for Color Biomedical Images”, 2013 IEEE International Conference on Computational Intelligence and Computing Research, 978-1-4799-1597-2

[14] Neeraj Bhargava, M.M. Sharma, Abhimanyu Singh Garhwal and Manish Mathuria, “Digital Image Authentication System

Based on Digital Watermarking", 2012 International Conference on Radar, Communication and Computing (ICRCC), December, 2012. pp.185-189

[15] Koushik Pal, Goutam Ghosh, Mahua Bhattacharya, "Reversible Digital Image Watermarking Scheme Using Bit Replacement and Majority Algorithm Technique", Journal of Intelligent Learning Systems and Applications, 2012, 4, 199-206, doi:10.4236/jilsa.2012.43020