IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Analysing The Technique Of Image Watermarking Based On Mordern Fuzzy Logic For Medical Images

[1] Ms. Kamalpreet Kaur

[1]Assistant Professor

[1]Department of Computer Science & Engineering,

[1]PCTE Institutes of Engineering & Technology, Ludhiana, India

Abstract: This article looks at using watermarking methods in medical images to make them safer and easier to manage. The idea is to protect trustworthiness, honesty, and safe sharing of health records. This paper looks at cases where watermarking has been used well in healthcare systems. Experts stress the main worry of keeping medical records accurate. This is tackled through a method called watermarking. Watermarking of medical images is an effective way to keep important health data safe and proved. It is extremely helpful for checking diseases and referencing information in the healthcare system. The document explains current health image marking methods, focusing on the Region of Non-Interest while keeping the key area safe. Important words are Medical Pictures, Region of Interest, Safety and Assaults. As nanoscience and nanotechnology progress, their use in medicine gets more common. Nano technology medical imaging gear gives clear and correct pictures of people's organs. This is key for finding out what is wrong in medicine. In the world of today's medicine and changing computers, scientists look at what is inside living things to find illness early and make science-based treatments. Medical pictures used in research often need to be shared or sent online for many uses like remote care. Telemedicine uses phone and computer science to give healthcare from far away, especially in places that do not have quick medical help. This way makes it easier for people in far-off countryside areas to get health advice. Putting a watermark on medical pictures is especially important for keeping the right information in check. Telemedicine systems often use parts of pictures called regions of interest and areas that are not important. The ROI is needed for doctors to make decisions about a patient's health. In this writing, the author talks about why watermarking medical pictures is important to keep information safe.

Index Terms - Medical Imaging, Region of Interest (ROI), Security, Threats, Digital Watermarking, Telemedicine, Data Integrity, Healthcare Information Protection.

I. INTRODUCTION

A significant change has come in society worldwide through the recent development of the digital revolution and internet revolution. Access to the internet and digital content or multimedia has become very easy nowadays for any kind of user. Therefore, an urgent requirement for the protection of intellectual property in digital media has been created. For the protection of this intellectual property, the best solution that has been created is digital watermarking (Kadian et al. 2021., p. 3236). However, nowadays the whole generation is living in the digital era and the domain of information. In this generation within a fraction of a second billions of data have been generated and also with new creation phase, delivery, and internet of data. Therefore, the duplicity of the data and fake creation of the digital even without the quality loss is possible easily. For this reason, the chances of the copying of the digital content have been increased.

Due to this reason, the requirement for prohibiting these kings of illegal copyrights of digital media during transmission has been created. The only solution to solve the problem includes the process of digital watermarking. Digital watermark applies to the graphics, text, logo, and audio and it has been hidden and not visible to the human eye (Megías et al. 2021., p. 10928). The rate of using digital media and digital content is rising nowadays due to the advancement of digital technology and internet networks globally. Alongside this, the availability of digital information has increased rapidly, and the process of storing, exchanging, and processing digital content has become simpler than ever.

On the other hand, despite these advantages, a modern set of issues concerning security such as the distribution of multimedia, unrestricted duplication, and manipulation have increased. Hence, content verification and owner protection have become an impactful issue. Moreover, this process is useful to ensure image integration, authentication, and content verification, especially in the medical field (Begum &Uddin, 2020., p.110). For this purpose which is to protect the integrity of the medical images advanced fuzzy technique has been applied for embedding the digital watermarks on the medical images.

Digital Watermarking

"Andrew Tirkel and Charles Osborne" invented the term "Digital Watermark" in the year December 1992. However, in 1993 the extraction of the steganography spread spectrum watermark and its embedding was first successfully demonstrated by Charles Osborne, Gerard Rankin, and Andrew Tirkel. This process is a type of the marker covertly implanted within thesignal based on noise-tolerant and they are video, audio, and image data. Using a digital watermark is the typical identification of the copyright of such signals. Digital watermarking refers to the process of embedding digital information into multimedia data which is digital. Digital watermarking can be classified into several categories such as visible watermarks, fragile watermarks, public watermarks, and invisible watermarks (Wazirali et al. 2021., p. 1744). However, the process of digital watermarking is divided into some stages such as embed, attack, and protection. In the first stage, the digital signal has been embedded with the digital watermark, and then in the second part, the transmitted media has been changed and becomes a threat to the watermarking system.

Then in the last stage, the detection of the watermark from the noisy signal has been done. On the other hand, based on the original data that is required for the extraction of watermarks the digital watermark can be classified into three categories such as non-blind, blind, and semi-blind schemes. However, in the semi-

blind process watermark and the keys to detect the watermark is required. In the non-blind scheme, the original image is required to extract the embedded watermark. Similarly, the blind scheme is applied when neither the original image nor the watermark is required during the extraction phase.

Digital watermarking methods can be classified into two classes based on the watermark embedding domain such as the transform domain and spatial domain (Gupta et al. 2022., p. 100520). Nowadays digital watermarking is essential as it protects the claim ownership and content as well as secures the digital assets with watermarks. Moreover, the embedding step of the digital marking process has three steps such as feature extraction from the primary content, then watermark creation from the message using a key and finally mixing the feature with the watermark. The decoding function is capable of decoding the hidden message from the watermark version by applying a decoding key.

Applications of Watermarking

Across a wide range of applications digital watermarks is successfully and broadly deployed in several types of projects. However, the main concern of this watermarking is the protection of the copyrights. This watermarking application is believed to be the most complex and this application also can be used in various applications such as ownership tracking, transaction tracking, broadcast monitoring, and copy control. The piece of watermarking is the process of superimposing a logo or piece of text on digital content.

There are several application areas of the digital watermarks and the application are illustrated precisely with the details of this technology that has been used. This study has highlighted some real-life uses and this links related to this useful information. These applications are:

1. Locating content online
2. Audience measurement
3. Content identification and management
4. Improved auditing
5. Content filtering that includes triggering of actions and blocking)
6. Broadcast monitoring
7. Authentication of objects and content (includes government IDs)
8. Communication of ownership and copyrights
9. Content protection based on the video and audio files
10. Document and image security
11. Forensics and piracy deterrence
12. Rich media enhancement for mobile phones

Fuzzy Logic

Based on the mathematical theory of fuzzy sets LotfiZadeh in 1965 declared that fuzzy logic is an extension of Boolean logic. The fuzzy logic is a generalization of the classical set theory. For reasoning, valuable flexibility has been provided by fuzzy logic and this also makes possible the work of taking account into uncertainties and inaccuracies (Athanassopoulos&Voskoglou, 2020., p. 875). The rules of fuzzy logic are set in natural language which is an advantage of the application of fuzzy logic for developing the process of

human reasoning. However, in fuzzy logic, membership functions divide components in the "range [0, 1], with 0 and 1 being no and full inclusion", while the other values are partial membership. Moreover, two aspects are worthy to be mentioned for understanding the reasons for the extensive development. The first one refers to a fuzzy set which is essential for modeling of all types of intermediate grades which mainly occurs within any types of concepts from any view of an application.

Then the second, aspect refers to a diversity of tools included within the fuzzy framework which enables the planner to identify the main concepts based on reality. A wide range of applications are present which range from different consumer products mainly as camcorder cameras, microwave ovens, and washing machines with the industrial processes such as medical instruments, portfolio selection, decision support systems, and process control. On the other hand, fuzzy logic refers to the process which is variable and allows multiple possible truth values to be processes by the same variables (Serrano-Guerrero et al. 2021., p. 107018). Problems with an imprecise and open spectrum of data attempt to be solved by fuzzy logic.

This also makes it possible to attain a range of accurate conclusions. Providing effective solutions to the most complex issues can be possible by using fuzzy logic and the system can easily modified for alter the performance or improve the performance. However, in the case of digital watermarking fuzzy logic can determine the strength of watermarking based on the edge sensitivity and contrast (Singh et al. 2023., p. 6251). Besides this, three fuzzy inference models are used to create the weighing factor for embedding the watermark. Similarly, the weighing factor is used in giving an input to the Fuzzy Inference System which is taken from the Human Visual System model.

LITERATURE REVIEW

The technique for the robust medical image is watermarking a process with a significant phenomenon that helps to identify accurate tapers and accurate detection through the region of insight and also covering the region of original interest (Bhatia &Almutairi, 2023., p. 15). This paper has followers with medical images with novel for the method of watermarking and this has been proposed through "integer wavelet transforms (IWT)". The integrity has effectively been verified for ROI, this identifies tampered precisely with different blocks present inside the ROI. Hence, through the respective proposed method, the medical image has been processed with two of the segments and those are in the areas of RONI and ROI region. The values of ROI are generated as hash, ROI recovery data and patient data are processed with embedded into the IWT and RONI. Furthermore, the result of the experiment has developed with the appropriate robustness method for watermarks and different information present inside RONI. This also performs to develop with appropriate detection; tempered areas become localized inside the areas of ROI original recovery.

The main fundamental aspect or role of fuzzy logic is to provide grey shades between the off or on and also no or yes and is ideally helpful for the medical industry in terms of proving watermark to medical images (Anand& Singh, 2021., p. 75). The particular system does not significantly maintain the function of the membership system and rules control has been processed with determined. This phenomenon happened until the system became applied and also different output for this refers to the calculated table

as per current input. The major focus relied on the tuning process for volume and this is subjected to be one of the difficult steps for control application of fuzzy.

The new quantization method of two dimensions for watermarking digital images and this is particular paper has been processed with novel security for the appropriate techniques of watermarking reversible and was remarkably proposed for different medical images. Hence, for the phenomenon of maintaining a high level of security over cover images, this image is further partitioned into several blocks. Neighboring pixels become inherent with higher correlation. The particular aspects are remarkably useful in the areas of creating differences among fixed or steady point pixels and also its vertical fighter boring pixel, diagonal direction, and horizontal of that specific block (Kaur&Kaur, 2016., p. 6). These further differences based on Neighboring blocks are further used in the areas of space of data embedding. Hence, the global peak towards histogram differences is beneficial to developing or embedding a watermark. The embedded process of multiple iterations increases with the capacity for data or information hiding. The extraction has innovatively depicted through an inverse manner and also the original watermark and the original image can optimized as a result.

Grayslake images need to be processed with watermarking in real time instead of altering their respective content. The respective paper focused on a new domain watermarking spatial of the gray scale images and this was seen and proposed in its Implementation of VLSI. The VLSI implementation is processed without alternating its respective and real-time for a secret key (Singh et al. 2021., p. 30370). Furthermore, secret keys are generated with the help of watermark pixel searching values through host content images and a mark has been obtained in the location map through the secret key. Hence, the particular algorithm is known as PVSA- “Pixel Value Search Algorithm”.

The host image does not show any changes due to the aspects of the proposed algorithm. This mainly focuses towards high robustness for providing a signal to the processing attack. The extraction process of watermark has significantly become simple when host content has remarkably extracted through the approaches of key and also robustness has effectively evaluated for algorithm against different attacks signal process with the uses of MATLAB.

A novel secure has been proposed through this particular paper for different medical images. For the development of security by maintaining a higher level of cover images, these are partitioned into different blocks of images. Higher correlation is subjected to be inherent through respective neighboring pixels. The particular aspects further going to be used in the areas of developing differences between diagonal direction and horizontal, the fixed pixel point and vertical lighter boring pixel of the specific block. However, the differences among different neighboring pixels become useful for embedded data space. Hence, peak with a global approach for difference histogram further becomes useful for embedding watermark. Embedding multiple iterations increases the process of hiding the capacity of data. The extraction was appropriately done with the help of the original image, inverse manner and also the original watermark obtained as an effective result.

Different types of procedures and techniques are used for image processing watermarking and those are detection, attack and embedding approaches (Gupta et al. 2022., p. 24). In the process of embedding an algorithm performs for accepting data and host to become embedded and a significant procedure for

watermark signal. Furthermore, digital signal watermarks have remarkably transferred or also stored and are usually transmitted towards another person's end. The algorithm for water marketing has processed an innovative process for watermarking also known as hiding reversible data which guarantees recovery with the exact process for different original images. This happened after data embedded extracted from previous extract recovery images. The main remarkable advantages consist of domain frequency in respective proposed algorithms and are processed with high-capacity embedding. The main properties included in the image watermark are a number for defining relative importance. These properties are security, error probabilities, embedding capacity, robustness, inevitability, blindness, visibility and perceptual similarities.

The wavelet-based algorithm is subjected to a digital image invisible watermarking with a concept of multimedia security. The perspective paper is responsible for presenting the proposed algorithm for implementation, designing and also using a variety of MATLAB for R2014a of simulation based on bot both extraction and embedding of result and watermark that performs for showing performance improvement metrics (Kumar et al. 2023., p. 13). These metrics include SSIM, PSNR, MSE and Mean Correlation apart from other different “existing algorithms in the current literature”. The algorithm has considered the cover image with (256x256) also the binary image size watermark has been considered with (16x16). The modern generation has processed with security lacking for having access to intelligent access software availability and internet access. This phenomenon creates conflict in the transmission of communication channels. Thus, the most effective process for data security consists of the techniques of digital watermarking and also steganography (Megías et al. 2021., p. 11). The image of digital watermarking complie4d with two important properties and those are robustness and imperceptibility. Host image is subjected to be less degraded visually than more imperceptible algorithm. Furthermore, the robustness is focused towards image attack processing.

A comprehensive manner of surveys has been processed based on watermark techniques of digital images. The particular paper image is processed with additional ads for watermark information for the prospective host image in the form of video audio or logo. The main target or objective for watermark images is to deliver more copyright protection, data integrity, ownership identification and also content authentication fully (Begum &Uddin, 2020., p. 11). This is not for only modification relating to content protection but also for content authentication and data integrity. Watermark recruitment is processed with high imperceptibility, capacity, security, and strong robustness which vary according to a different application. The spatial domain for techniques is simple and has to operate with low complexity and further cannot embed with more bit number but they are also not resistant towards different types of geometric attack. Frequency transformation domain techniques are considered with both the aspects of geometric and also attacks of image process but on the other hand, when the frequency is totally corrupted then the also the robustness is also decreases. Furthermore, it is not capable for embedding more bits as the quality is degraded.

In the resilient inversion attack medical image scheme for zero-watermarking authentication fuzzy technology benefitted immensely. This paper significantly focuses towards resilience attacks for the inversion system of zero-watermarking and through the transforms of hybrid contoured singular

decomposition value domain with authentication of medical images (Singh et al. 2021., p. 30370). However, this "respective scheme preserves the fidelity of the host image" despite introducing a triangular number and artifact for generating the functional number. Hu's invariant images are responsible for conform attacks and the system performs evaluations with different modalities and medical images quick responses which contain different data of pat emits with code watermark. The demonstration of the result or outcome has been processed with system robustness against the ambiguity attack. This signifies an appropriately secured exchange of medical images between several remote radiologists.

Hybrid watermarking for medical images with ROI recovery and authentication and a scheme for a hybrid watermarking process with the approaches of multimedia data in the areas of digital video and digital images is proposed and utilized with processing transform images and also comprehensive sensing for achieving security and fragility with multimedia data or information. The main advantage of this particular fuzzy technology is to provide proposed solutions for DICOM strong security medical images with a combination of ROI zero-watermarking and RONI with non-zero watermarking.

Digital watermarking through a dual reversible process is a pivotal process of authentication and recovery of medical diagnostic images. The paper has demonstrated various ranges of tampering detection based on specific regions of the brain. Apart from that, the paper also proposes extracting methods to recover from the impact of reversible digital watermarking and quad-tree decomposition purposes (Gong et al. 2020.,p.79). All these proposals are evaluated for enhancing medical image authentication through the process of medical diagnostic procedures. At first, quad-tree decomposition has been discussed in this study. The quad-tree decomposition is generally used to separate the original image into parts which contain different types of characteristics such as parts with high homogeneity and other computer pixel's linear interpolation. These parts are salient parts of recovery features (Wang et al. 2022.,p.198). There is also another part which is integral to the recovery feature which is first-layer watermarking.

The invertible integer transformation is a tool that can be used to embed as a recovery mark within any given content. This is a highly effective tool for security measurement. Besides that, there is another feature called a logistic chaotic map that can be used to examine the part's reference pixel to evaluate the original author. The second layer of watermarking is another part of quad-tree information and this watermarking offers critical security measurements which are characterised by LSB replacement (Evsutin,Melman&Meshcheryakov, 2021.,p.179). The last stage in this watermarking technique is the authentication phase. In this stage, the hidden and embedded watermark is extracted as well as the source of code of the image.

These are the comprehensive stages of tampering detection to authenticate the sources by revealing various ranges of embedded features. Besides that, the tempering detection method can sophisticatedly determine which area of a given file is tempered and manipulated by checking region by region. These divided parts can be recomputed to understand the level of tampering applied by differentiating the tampered one from the original one. As the author, in this method, the authentication can proceed by checking the tempered file through the restored image by checking the visual quality of the given file and unearthing the embedded content within a file. Optical 3D watermarking is also an important process

which involves watermarking of the digital image for telemedicine. 3D watermarking involves embedding a 2D elemental image array in the process of a lenslet array (Yuan et al.2023., p.295). Through this process, the watermark from a host image requires an inverse process of embedding or EIA.

Later, the EIA can be in a complex procedure called computational integral imaging reconstruction to regenerate the 3D watermark. Through this process, the data regarding the watermark of the original file can be carefully retrieved. Hence, this watermarking method is highly effective extract the result of authenticity through the 3D watermarking process. Another aspect of the tampering recovery process is ROI segmentation with multilevel authentication (Ravichandran et al. 2021.,p.1355). This process is a complicated process which involves identifying tampering with an image which contains an average peak ratio based on signal of noise is 48.7 decibels. In this way, the area of tampering is highly identifiable through the incorporation of ROI segmentation and a multilevel authentication process (). It has been found that this process allows users to locate 50% of overall tampering.

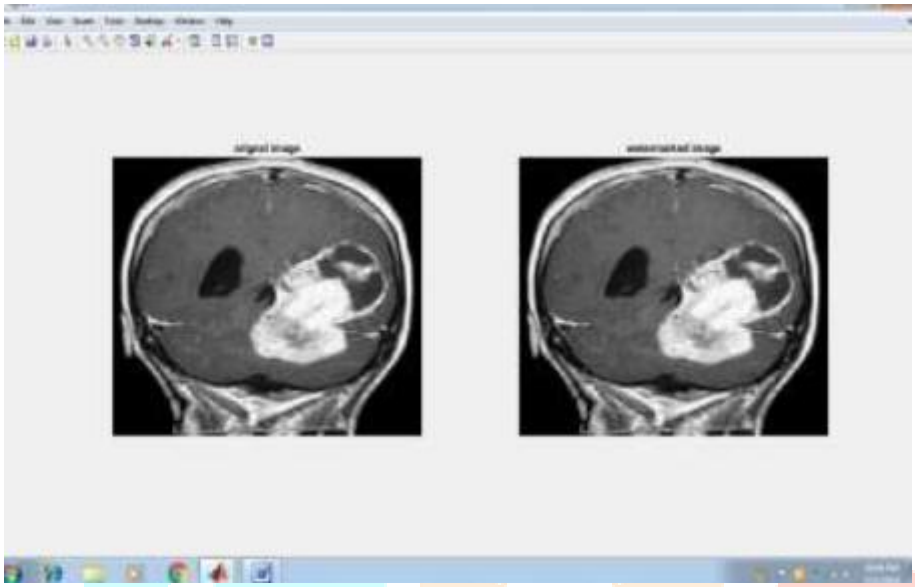
There is another watermarking technique called the ROI-lossless fragile watermarking technique. In this process, the technique emphasised medical image watermarking through ROI-lossless procedures. The technique offers a comprehensive approach to mitigate various plagiarism-related issues such as security measurement, and a safe and retrievable process. This process, involves incorporating encryption techniques and compression techniques to tabulate data, critical information like coded keywords and other types of critical information to examine medical images. In this process, a large set of electronic health records can be easily stored and retrievable and it can be used as a comprehensive solution tool in the field of information management, especially in the domain of medical documentation (Oh et al. 2021.,p.18). Apart from all of these, there is another process called block division through histogram modification to identify the differences in the given medical images. The process of the data hiding method requires a histogram modification method which includes reversible data by evaluating differences in the embedded pixels as high-quality pixels help to increase the capacity of data hiding.

Apart from that, the process is highly effective in increasing critical data-hiding capabilities through incorporating block division. It can be also used for comparing algorithms to conduct a comparison with tempered medical images which are presented in high quality. The next process of the image-based watermarking method is utilising RONI pixels through bit-planes for medical image watermarking (Roy, Basu&Chattopadhyay, 2023., p.168). In this method, the process of computation is highly integral to examining the watermark of the image border pixel. RONI refers to a region of non-interest which is intended for the diagnosis of border pixels of medical images.

This process is used to examine the areas which serve little to no interest level to any examining professional such as medical professionals, doctors and others. The process of RONI allows users to incorporate trackable elements with medical images without distorting the embedded region or keeping the distortion at a minimum level which may be negligible or highly untraceable irrespective of image modalities (Shi et al. 2023., p.42). Bit-planes of the border area serve as the main area of focus to protect the embedded watermarked image for diagnosis purposes. Despite the sophisticated process, there is an issue associated with ethical points of view regarding altering all types of pixels based on the medical images. Hence, RONI segmentation is not highly encouraged in the field of investigating medical images.

RESULT AND DISCUSSION

In this section, various types of medical images are used here such as brain, lung, lower back, and abdomen are used for medical imaging by applying different types of modalities. These modalities include CT scan, MRI scan, PET scan and ultrasound. The results that are obtained through applying these modalities are demonstrated here. At first, the image with no attack was presented here.



\Figure 1: Watermarked image without any tempering

(Source: Self-developed)

In the first process of attacking, modalities have been applied in medical images and different attacks have been applied alongside it. At first, the medical diagnostic technique called CT scan was applied. At first, no attacks had been applied and the result was 1. Later, JPEG compression was applied and the marked result 0.99954. Salt and pepper noise with a density of 0.005 was applied and it resulted in 0.98938. After that, Gaussian noise with a variance of 0.001 was applied which generated a result of 0.99932. Low-pass filtering is used and it generated resulted in 0.99905. The second process, MRI is used to record the deviation in comparison with no attack measurement. At first, no attack was applied and the result was 1. Later, JEPG compression with a compression ratio of 90% has been applied. The value after the attack has reached 1 to 0.97563. After that, salt and pepper noise was made and the result was 0.96015. Using Gaussian noise with a variance of 0.001 has resulted in 0.97155. Finally, low-passing filtering was applied and it generated an NC of 0.98394. Later, ultrasound modality was used to test the NC result and the result of NC when no attack was applied is represented as 1.

Later, JEPG compression with a compression ratio of 90% was used to tamper the image and the NC result was 0.98828. Similarly, salt and pepper noise was applied with a density of 0.005 and the NC figure was 0.96746. Gaussian noise with a variance of 0.001 was applied which generated an NC of 0.95858 and low-pass filtering was applied which produced the NC which was 0.98285. Finally, a PET scan was applied for the final attack. At first, the medical image was normal and no tampering was applied and the NC result remained 1. Later, JEPG compression with a 90% compression ratio was used which influenced NC to reach

0.98969. The salt and pepper test resulted in an NC of 0.96924. Later, Gaussian noise resulted in the NC of 0.97727 and low passes filtering resulted in the NC of 0.99212.

The modality of medical images is variable and average PSNR, WPSNR, MSSIM and TPE are also different. CT scan produces an average PSNR of 74.0111, average WPSNR of 88.0917, average MSSIM of 0.9977 and average TPE of 0.000099. MRI scan produces an average PSNR of 78.4402, WPSNR was 93.5402, average MSSIM was 0.9971 and average TPE of 0.000043. Ultrasound produces an average PSNR of 59.2146, an average WPSNR of 73.7126 and an average TPE of 0.000214. The PET scan produces an average PSNR of 56.0176, an average WPSNR of 0.9937 and an average TPE of 0.000373

CONCLUSION

There are several types of algorithms related to medical image watermarking available and there are various segmentation algorithms to segment ROI are also available. Digital watermarking refers to the process of embedding digital information into multimedia data which is digital. Digital watermarking refers to the process of embedding digital information into multimedia data which is digital. Based on the "types of medical images such as CT, MRI, US, etc" the segmentation algorithms vary. The following study can further be extended to separate the ROI by developing a GUI tool-based approach. Furthermore, the further evolution of the new technique of separating ROI from the original image can be possible which also will apply to all kinds of medical images. However, the "separated ROI can be stored with xmax, ymin, ymax, and xmin values for making the segmented ROI" attached to the watermarked image. This attachment with a watermarked image can be done before the transmitting watermarked image at the end of the embedding process. The segmentation of the ROI from the medical image can become suitable in any medical image watermarking approach only with four values. After this whole process, the embedding of the watermark is possible on the entire medical image. However, in some cases, spaces to embedded more such as when the algorithm can solve the problem definition and when the proposed algorithm can improve the accuracy which is compared to the existing process.

REFERENCES

1. Anand, A., & Singh, A. K. (2021). Cloud based secure watermarking using IWT-Schur-RSVD with fuzzy inference system for smart healthcare applications. *Sustainable Cities and Society*, *75*, 103398. https://doi.org/10.1016/j.scs.2021.103398
2. Athanassopoulos, E., &Voskoglou, M. G. (2020).A philosophical treatise on the connection of scientific reasoning with fuzzy logic.Mathematics, 8(6), 875.https://doi.org/10.3390/math8060875.
3. Begum, M., &Uddin, M. S. (2020). Digital image watermarking techniques: a review. *Information*, *11*(2), 110. https://doi.org/10.3390/info11020110
4. Begum, M., &Uddin, M. S. (2020). Digital image watermarking techniques: a review. Information, 11(2), 110.https://doi.org/10.3390/info11020110.

5. Bhatia, S., &Almutairi, A. (2023).A Robust Fuzzy Equilibrium Optimization-Based ROI Selection and DWT-Based Multi-Watermarking Model for Medical Images. *Sustainability*, *15*(7), 6189.https://doi.org/10.3390/su15076189

6. Evsutin, O., Melman, A., &Meshcheryakov, R. (2021). Algorithm of error-free information embedding into the DCT domain of digital images based on the QIM method using adaptive masking of distortions. *Signal Processing*, *179*, 107811.https://doi.org/10.1016/j.sigpro.2020.107811

7. Gong, X., Chen, L., Yu, F., Zhao, X., & Wang, S. (2020).A secure image authentication scheme based on dual fragile watermark.*Multimedia Tools and Applications*, *79*, 18071-18088.https://doi.org/10.1007/s11042-019-08594-x

8. Gupta, S., Saluja, K., Solanki, V., Kaur, K., Singla, P., &Shahid, M. (2022).Efficient methods for digital image watermarking and information embedding. Measurement: Sensors, 24, 100520. https://doi.org/10.1016/j.measen.2022.100520.

9. Gupta, S., Saluja, K., Solanki, V., Kaur, K., Singla, P., &Shahid, M. (2022).Efficient methods for digital image watermarking and information embedding. *Measurement: Sensors*, *24*, 100520.https://doi.org/10.1016/j.measen.2022.100520

10. Kadian, P., Arora, S. M., &Arora, N. (2021). Robust digital watermarking techniques for copyright protection of digital data: A survey. Wireless Personal Communications, 118, 3225-3249. https://doi.org/10.1007/s11277-021-08177-w.

11. Kaur, K., &Kaur, E. S. (2016). Advanced fuzzy logic based image watermarking technique for medical images. *Int J Adv Res Ideas InnovTechnol*, *3*(1), 1-7. https://d1wqtxts1xzle7.cloudfront.net/53844230/V3I1-1365.

12. Kumar, L., Singh, K. U., Kumar, I., Kumar, A., & Singh, T. (2023).Robust Medical Image Watermarking Scheme Using PSO, LWT, and Hessenberg Decomposition. *Applied Sciences*, *13*(13), 7673. https://doi.org/10.3390/app13137673

13. Megías, D., Mazurczyk, W., &Kuribayashi, M. (2021). Data hiding and its applications: Digital watermarking and steganography. Applied Sciences, 11(22), 10928. https://doi.org/10.3390/app112210928.

14. Megías, D., Mazurczyk, W., &Kuribayashi, M. (2021). Data hiding and its applications: Digital watermarking and steganography. *Applied Sciences*, *11*(22), 10928. https://doi.org/10.3390/app112210928

15. Oh, S. R., Seo, Y. D., Lee, E., & Kim, Y. G. (2021). A comprehensive survey on security and privacy for electronic health data.*International Journal of Environmental Research and Public Health*, *18*(18), 9668.https://doi.org/10.3390/ijerph18189668

16. Ravichandran, D., Praveenkumar, P., Rajagopalan, S., Rayappan, J. B. B., &Amirtharajan, R. (2021).ROI-based medical image watermarking for accurate tamper detection, localisation and recovery.*Medical & Biological Engineering & Computing*, *59*(6), 1355-1372.https://doi.org/10.21928/uhdjst.v4n1y2020

17. Roy, S. S., Basu, A., &Chattopadhyay, A. (2023).Prospects of Digital Watermarking in Providing Security, Reliability, and Privacy to Medical Images.*ECTI Transactions on Computer and Information Technology (ECTI-CIT)*, *17*(2), 168-182.https://doi.org/10.37936/ecti-cit.2023172.249484
18. Serrano-Guerrero, J., Romero, F. P., &Olivas, J. A. (2021). Fuzzy logic applied to opinion mining: a review. Knowledge-Based Systems, 222, 107018.https://doi.org/10.1016/j.knosys.2021.107018.

19. Shi, H., Yan, K., Geng, J., &Ren, Y. (2023). A cross-embedding based medical image tamper detection and self-recovery watermarking scheme. Multimedia Tools and Applications, 1-42.https://link.springer.com/article/10.1007/s11042-023-16679-x
20. Singh, O. P., Kumar, C., Singh, A. K., Singh, M. P., &Ko, H. (2023). Fuzzy-based secure exchange of digital data using watermarking in NSCT-RDWT-SVD domain. Concurrency and Computation: Practice and Experience, 35(16), e6251. https://doi.org/10.1002/cpe.6251.

21. Singh, O. P., Singh, A. K., Srivastava, G., & Kumar, N. (2021). Image watermarking using soft computing techniques: A comprehensive survey. *Multimedia Tools and Applications*, *80*, 30367-30398. https://link.springer.com/article/10.1007/s11042-020-09606-x
22. Singh, O. P., Singh, A. K., Srivastava, G., & Kumar, N. (2021). Image watermarking using soft computing techniques: A comprehensive survey. *Multimedia Tools and Applications*, *80*, 30367-30398. https://link.springer.com/article/10.1007/s11042-020-09606-x

23. Wang, J., Qu, H., Wei, Y., Xie, M., Xu, J., & Zhang, Z. (2022). Multi-focus image fusion based on quad-tree decomposition and edge-weighted focus measure.*Signal Processing*, *198*, 108590.https://doi.org/10.1016/j.sigpro.2022.108590
24. Wazirali, R., Ahmad, R., Al-Amayreh, A., Al-Madi, M., &Khalifeh, A. (2021). Secure watermarking schemes and their approaches in the IoT technology: an overview. Electronics, 10(14), 1744.https://doi.org/10.3390/electronics10141744.
25. Yuan, Y., Liu, Y., Guo, J., Han, Y., & Wang, X. (2023). Three-dimensional optical watermarking scheme using compressed sensing in integral imaging system. *Optik*, *295*, 171509.https://doi.o