International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
***Article Received:** 25 January 2023 **Revised:** 12 February 2023 **Accepted:** 30 March 2023*

Enhancing Healthcare Security with Chaotic Reversible Watermarking for Medical Images

Manohar Gosul[1], Nisarg Gandhewar[2]

[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— The implementation and advancement of digital technologies in medicine have sparked a technical revolution, leading to new developments across various medical fields. Ensuring the confidentiality of Electronic Health Records (EHR) and maintaining patient privacy are critical security requirements for healthcare systems. In today's digitally connected world, malicious tampering of digital images has become increasingly common, representing a serious violation of intellectual property rights. Consequently, protecting images by establishing rightful ownership has become a priority. Reversible watermarking (RW) techniques offer a promising alternative to conventional watermarking systems, particularly for safeguarding highly sensitive images. It is crucial to authenticate the source and origin of medical images and associated patient information to ensure they correspond to the correct patient. This work presents a method for protecting medical images and patient-related information in healthcare using a chaotic reversible watermarking technique. The performance of this method is evaluated using metrics such as Mean Absolute Error (MAE), Peak Signal-to-Noise Ratio (PSNR), Normalized Cross-Correlation (NCC), and Root Mean Square Error (RMSE).

Keywords— Electronic Health records, medical images, Digital watermarking and Chaotic reversible watermarking Method

I. INTRODUCTION

Modern advancements in information and communication technologies have significantly transformed medical imaging and information management systems in hospitals. Digital storage has gradually replaced paper-based medical images on traditional film, and telemedicine systems now enable the direct exchange of medical images and electronic

patient records among qualified doctors worldwide [1]. Due to their importance in clinical diagnosis, treatment, research, and various public and private sector applications, medical information is inherently valuable and sensitive.

In recent years, rapid advances in information technologies (IT) have brought about substantial changes at both conceptual and application levels in the management of medical information. Modern and integrated healthcare systems, such as Hospital Information Systems (HIS) and Picture Archiving and Communication Systems (PACS), provide easy access, manipulation, and distribution of medical data. These systems support various telemedicine applications, including tele-consultation, tele-diagnosis, and tele-surgery, which also serve as tools for medical staff e-learning [2]. Patient healthcare data is used to create an Electronic Health Record (EHR) for each patient, which includes medical images, Electronic Patient Records (EPR), and other critical information essential for the diagnostic process. Thus, any tampering or manipulation of these records could result in fatal misdiagnoses. As EHRs are exchanged among hospitals, doctors, and insurance companies, maintaining their confidentiality and safeguarding patient privacy are vital security requirements.

The Electronic Patient Record (EPR) has replaced the outdated paradigm of hardcopy medical records. EPRs typically contain diagnostic reports, medical images, biomedical signals, demographic data, test results, treatment details, and prescriptions—information that is by definition highly confidential. However, the digitization of medical information has also introduced new risks associated with the misuse of easily manipulated and distributed digital data [3]. Consequently, the security and privacy of medical information have emerged as significant challenges in healthcare services.

Combining digital watermarking with cryptography is an effective solution for protecting medical data against misuse and unauthorized distribution. Digital watermarking is a key technique for proving ownership, safeguarding content, and authenticating medical information. It has become a prevalent method for protecting the ownership of digital images. However, the effectiveness of watermarking schemes depends on their robustness, imperceptibility, and capacity for embedding.

Digital image watermarking represents a significant technological advancement in recent years, providing a method for asserting copyright ownership and enhancing multimedia security. This technology involves embedding

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
***Article Received:** 25 January 2023 **Revised:** 12 February 2023 **Accepted:** 30 March 2023*

watermark data into multimedia content (such as text, images, audio, and video) and later extracting or detecting the watermark to confirm authenticity. The watermark data protects the host content, making it difficult for an eavesdropper to remove or alter it [4].

A medical image watermarking scheme must be free from distortion, as even minor changes can lead to misdiagnosis and pose risks to patients' lives. Given the sensitivity of medical images to visual quality, most copyright protection algorithms use reversible embedding strategies. Reversible watermarking is a critical branch of information hiding technology, essential for copyright protection and preventing tampering and forgery of digital data carriers (such as audio, images, videos, and software). In these applications, watermarks are embedded by adding or modifying data within the carrier medium. For software, the watermark must be hidden within the algorithm to prevent tampering or forgery [5].

Currently, encryption and watermarking techniques are used to ensure the authenticity and confidentiality of medical records. However, the watermarked media transmitted might be subject to unwanted channel noise or attacks, reducing the robustness of the technique and resulting in distorted media [6]. To address these challenges, this work presents a method for protecting medical images and patient-related information in healthcare using a chaotic reversible watermarking approach.

II. LITERATURE SURVEY

Fatima Abbasi, Nisar Ahmed Memon, and colleagues [7] present a reversible watermarking technique for securing medical image databases. The proposed system first segments the input medical image into a Region of Interest (ROI) and a Region of Non-Interest (RONI) and then embeds two different watermarks in these areas. Simulation results indicate that this approach enhances the security of medical images while addressing both authenticity and confidentiality concerns.

K. Balasamy, S. Ramakrishnan, and colleagues [8] propose an intelligent reversible watermarking system for authenticating medical images using Wavelet and Particle Swarm Optimization (PSO). The medical image undergoes wavelet transformation, while another image is processed with a tent map and a hash function to protect the secret watermark. The tent map provides sensitivity to initial value changes, enhancing protection and encryption of the original watermark. This method embeds the watermark with low distortion, retrieves the secret information, and recovers the original image, proving valuable in terms of robustness, capacity, and imperceptibility.

H.R. Lakshmi, B. Surekha, and S. Viswanadha Raju [9] discuss the real-time implementation of reversible watermarking techniques as a potential replacement for conventional watermarking methods. The proposed approach demonstrates superior performance compared to existing methods.

Zhengwei Zhang, Lifa Wu, Yunyang Yan, Shaozhang Xiao, and He Sun [11] propose an improved reversible image watermarking algorithm based on difference expansion. The algorithm divides watermark information into groups and calculates the value of each group. Experimental results show that this method achieves a high embedding rate, excellent visual quality, and complete recovery of the original image, offering advantages over other algorithms.

Abhilasha Sharma, Amit Kumar Singh, and Satya Prakash Ghrera [12] present a robust and secure multiple watermarking technique for medical images. The method combines discrete wavelet transform and discrete cosine transform to embed both image and electronic patient records (EPR) watermarks simultaneously, enhancing security and supporting patient identity verification.

Nai-Kuei Chen, Chung-Yen Su, Che-Yang Shih, and Yu-Tang Chen [13] introduce a reversible watermarking method for medical images using histogram shifting with location map reduction. This improved lossless data hiding technique effectively handles the pure black and white points in medical images, reducing the location map size by up to 95.04% compared to previous methods.

R. Surya Prakasa Rao and Dr. P. Rajesh Kumar [14] propose an efficient genetic algorithm-based grayscale digital image watermarking technique to improve robustness and imperceptibility. The method embeds the watermark in the third level of Discrete Wavelet Transform (DWT) of the original image after applying Singular Value Decomposition (SVD) to the watermark. The genetic algorithm optimization technique determines the best scaling factor to modify the SVD coefficients.

Asna Furqan and Munish Kumar [15] present a study and analysis of a robust digital image watermarking technique in the DWT-SVD domain using MATLAB. The paper discusses methods for achieving copyright protection through digital watermarking and other technologies, such as key-based cryptographic techniques, to prevent illegal duplication.

III. RESEARCH METHODOLOGY

The proposed framework, termed the "Content-based Self-Recovery Reversible Visible Watermarking (CSRVW)" scheme, focuses on encoding images. In this approach, we aim to adaptively select data embedding positions to accommodate the watermark using a visual perceptual model

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
***Article Received:** 25 January 2023 **Revised:** 12 February 2023 **Accepted:** 30 March 2023*

before encryption, thereby achieving a balance between watermark visibility and the quality of the watermarked image. Given the weak spatial correlation in encrypted images, the data embedding space is created before encryption using a traditional reversible data hiding algorithm, which allocates pixel bits to designated embedding positions. As a result, the visible watermark can be embedded into encrypted images by substituting pixel bits at the identified embedding locations.

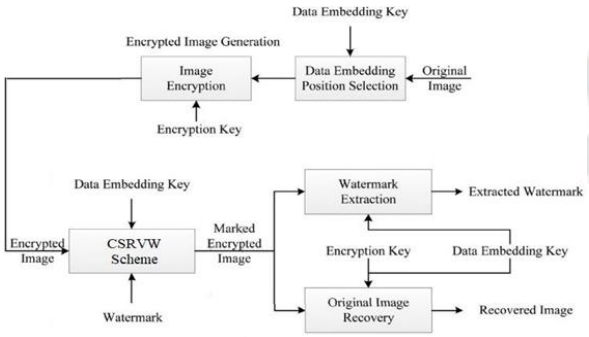

Figure 1. The system of the proposed scheme is appeared.

The system of the proposed scheme is appeared in figure 1. The plan is made out of four principle parts: data implanting position determination, scrambled image age, watermark installing in encoded image, and watermark extraction and image recovery. To accomplish the tradeoff between watermark perceivability and stamped image quality,the central point of interest is choosing data implanting positions for obliging the watermark based on image content.
The accompanying algorithm is a twofold tree structure is utilized to tackle the issue about conveying different sets of pinnacle and least focuses to the beneficiary. These data implanting positions and comparing pixel bits should be saved as the side data.

Algorithm

1. Scan the image M in an inverse s-order. Calculate the pixel difference d between pixels pi-1 and pi by
2. Determine the peak point K from the pixel differences.
3. Scan the whole image in the same inverse s- order as in Step 1. If d > K, shift piby 1 unit Where wi is the watermarked value of pixel x.
4. If d = K, modify pi according to the message bit Where m is a message bit to be embedded.
5. At the receiving end, the recipient extracts message bits from the watermarked image by scanning the image in the same order as during the embedding. The message bit m can be extracted by Where pi-1 denotes the restored value of wi-1.
6. The original pixel value of pi can be restored.

Since it is generally difficult to create space in the encoded image without loss, it is necessary to reserve room for side data before image encryption. Traditional reversible data hiding algorithms can be employed to save this space prior to encryption. Consequently, the data hider (such as a database manager or a cloud worker) can easily embed a visible watermark into the encrypted image by replacing pixel bits at designated data embedding positions. After the image is decrypted and the watermark is extracted, the original image can be perfectly recovered.

In visible watermarking, a watermark—typically a binary image—is embedded visibly into a cover image so that it is perceptible to the human visual system. This process involves substituting pixel bits in different bit planes of the cover image with corresponding watermark data. Ideally, the embedded watermark should be noticeable but should not significantly obscure the underlying details of the marked image. However, these two requirements often conflict with each other. To address this issue, visible watermark embedding can be framed as a problem of selecting appropriate data embedding positions. This approach motivates the consideration of both the human visual perceptual model and the content of the cover image to achieve a balance between these conflicting requirements.

Recently, reversible watermarking schemes have focused on improving both payload capacity and imperceptibility. Increasing payload capacity is challenging because reversible watermarking requires control data to restore the host signal after extraction, which significantly reduces the available space for data embedding. On the other hand, achieving high imperceptibility is also difficult given the payload constraints of current applications. When the payload capacity is increased, the imperceptibility decreases due to the greater amount of embedded data, which leads to more distortion of the signal. To enhance imperceptibility, the payload capacity must be reduced to minimize the distortion of the watermarked signal.

The trade-off between payload capacity and imperceptibility is further complicated in reversible schemes that need to embed control data along with the watermarks. Reversible schemes must adopt strategies to minimize the size of control data to reduce perceptual impact while preserving the original data for reversibility. In scenarios where attacks may occur, fragile reversible schemes cannot reliably convey additional data, as it may be lost, preventing the reconstruction of the host signals. Although fragile reversible schemes are not suitable in scenarios where attacks are likely, there remains a need for the perfect reconstruction of host signals after data embedding and transmission through noisy channels.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
Article Received: *25 January 2023* ***Revised:*** *12 February 2023* ***Accepted:*** *30 March 2023*

IV. RESULT

In fields like business, military, and medicine, high-quality signals (such as images, audio, or video) are required. Some applications in these fields demand not only high-quality signals but also the transmission of additional data embedded as a hidden watermark, even when the signals are transmitted through noisy channels. After data extraction, the high-quality signals should maintain their integrity without loss, so watermarking schemes must be capable of compensating for the distortions caused by data embedding and any potential alterations occurring during transmission.

From Table 1, it has been seen that the inserting of watermark at scaling factor above will support to specific assaults while keeping up the image quality. In the event that scaling factor expanded to 0.5, the watermark is stronger to various kinds of assaults with decent debasement. That is implanted mystery logo ought not be eliminated by any sort of mutilation as strength is a vital and essential necessity of a watermarking framework.
The accompanying perceptions are contrived in the wake of executing the current crossover watermark implanting and extraction algorithms. Higher is the worth of PSNR, higher is the detectable quality and higher is the worth of CF, higher is the strength. Inthis plan, cover image and watermark image both are of same size.

- ✓ High intangibility is accomplished with the proposed conspire.
- ✓ Perceptibility diminishes with expanding scaling factor while vigor increments.
- ✓ The benefit of scaling factor is restricted inside the scope of 0.01 to 1 on the grounds that from there on the visual nature of watermarked image will be debased.
- ✓ This plan can undoubtedly recover the installed watermark by safeguarding the shading content of watermark regardless of whether the watermarked image is exposed to various sorts of assaults.
- ✓ Scaling factor is set at 0.5 to get high heartiness while keeping the image quality prerequisite at healthy levels.
- ✓ At a similar scaling element, heartiness and imperceptibility are impressively greatest in this strategy among all proposed techniques.
- ✓ Embedding of watermark at scaling factor above 0.1 just can support to various assaults.
- ✓ Good limit is accomplished with high power and adequate visual corruption of watermarked image.
- ✓ This conspire gives better tradeoff between indistinctness, strength and limit with respect to shading images with no deficiency of shading content.

This research focuses on the watermarking of color images to verify authenticity and protect copyrights. The goal of this study is to develop efficient watermarking algorithms for color images and video that achieve high levels of subtlety and robustness without compromising the color content of the recovered watermarks.
The proposed algorithms are evaluated based on their invisibility and robustness properties. The limitations of each watermarking method are analyzed, and advanced techniques are developed to overcome these limitations, achieving maximum transparency. The performance improvements in terms of Peak Signal-to-Noise Ratio (PSNR) for all the proposed non-blind invisible color image watermarking schemes are presented in Table 7.1. From this table, it is evident that the proposed hybrid color image watermarking scheme using Content-based Self-recovery Reversible Visible Watermarking (CSRVW) offers superior invisibility compared to the other two methods based on Singular Value Decomposition (SVD) and Discrete Wavelet Transform-Singular Value Decomposition (DWT-SVD).

Table 1 Comparison of PSNR values

Cover Images	SVD	DWT-SVD	CSRVW
Peppers	35.1822	58.7234	65.7642
Lena	32.8796	57.6364	64.2321
Sunset	33.9879	57.3452	64.4578
Balloon	30.5678	57.6843	64.7667
Autumn	35.2278	59.6345	66.9843

The embedding capacity is also enhanced with this scheme, varying from image to image depending on the chosen transformation method for color image watermarking. As the size of the cover image and watermark image increases, the capacity of the proposed scheme also increases. The visual quality, measured in terms of PSNR, for three different algorithms is graphically represented in Figure 5.15. Among the three algorithms, the third one demonstrates superior performance in terms of subtlety and robustness. This algorithm is applied to video watermarking to achieve excellent perceptual quality and resilience, while also providing a higher capacity to withstand both intentional and accidental attacks.

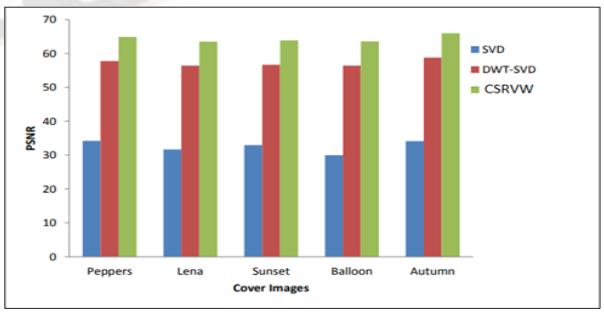

Figure 2. PSNR values of three different algorithms for various cover images

This chapter discusses the significant advancements in the newly developed scheme. The embedding and extraction of color images are successfully performed in the transformed domain of the image using the proposed hybridized approach. This scheme enhances watermark extraction performance while preserving the color data against all mentioned attacks. The effect of the scaling factor on watermark color extraction is clearly observed. Additionally, an improved capacity is maintained without compromising imperceptibility and robustness compared to previously proposed algorithms. Various experimental results of this scheme are presented and analyzed to demonstrate its superiority over other earlier algorithms. Since some degree of visual distortion is acceptable, this algorithm is applied with different scaling factors to optimize distortion-free results. The metrics of imperceptibility and robustness are objectively measured and compared with previous watermarking techniques. However, when the watermarked image undergoes image processing distortions such as noise, rotation, and filtering attacks, it is shown that while the algorithm is effective in detecting the watermark, it fails to retain the color of the extracted watermark under distortion. Therefore, there is a need to restore the color of the watermark extracted from the attacked watermarked media.

V. CONCLUSION

This work presents a method for protecting medical images and patient-related information in healthcare using a chaotic reversible watermarking technique. The Electronic Health Record (EHR) data is first processed with the Integer Wavelet Transform (IWT) to enable lossless recovery of the original medical image. By applying IWT, the method isolates high-frequency sub-bands within the medical image. In these sub-bands, non-overlapping blocks are identified, and the Discrete Gabor Transform (DGT) is applied to the image's integer wavelet coefficients using a chaotic sequence, which is then embedded into a cover image. The reversible watermarking technique ensures that secret data is embedded within the medical image in a lossless manner. At the receiver side, both the original medical image and the watermark information are extracted exactly as they were at the sender side, without requiring any additional information. The performance of the proposed method is evaluated using metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Absolute Error (MAE), Normalized Cross-Correlation (NCC), and Root Mean Square Error (RMSE). When compared to traditional healthcare data protection methods, the proposed approach effectively safeguards medical images and patient information.

References

[1] Narima Zermi, Amine Khaldi, Med Redouane Kafi, Fares Kahlessenane, Salah Euschi, “Robust SVD-based schemes for medical image watermarking”, Microprocessors and Microsystems 84 (2021) 104134, doi.org/10.1016/j.micpro.2021.104134

[2] Xiaoyi Zhou, Yue Ma, Qingquan Zhang, Mazin Abed Mohammed and Robertas Damaševi˘cius, “A Reversible Watermarking System for Medical Color Vol 9, Issue 11, November 2022 Images: Balancing Capacity, Imperceptibility, and Robustness”, Electronics 2021, 10, 1024, doi.org/10.3390/electronics10091024

[3] M. Cedillo-Hernandez, A. Cedillo-Hernandez, M. Nakano- Miyatakea, H. Perez-MeanaaaInstituto, “Improving the management of medical imaging by using robust and secure dual watermarking”, Biomedical Signal Processing and Control 56 (2020) 101695, doi.org/10.1016/j.bspc.2019.101695

[4] Mahbuba Begum and Mohammad Shorif Uddin, “Analysis of Digital Image Watermarking Techniques through Hybrid Methods”, Hindawi, Advances in Multimedia Volume 2020, Article ID 7912690, 12 pages, doi.org/10.1155/2020/7912690

[5] Lingzhuang Meng & Lianshan Liu & Gang Tian1 & Xiaoli Wang, “An adaptive reversible watermarking in IWT domain”, Multimedia Tools and Applications, 2020, Springer, doi.org/10.1007/s11042-020-09686-9

[6] Ashima Anand, Amit Kumar Singh, “An improved DWT-SVD domain watermarking for medical information security”, Computer Communications 152 (2020) 72–80, doi.org/10.1016/j.comcom.2020.01.038

[7] Fatima Abbasi, Nisar Ahmed Memon, “Reversible Watermarking for the Security of Medical Image Databases”, 2018 IEEE, 978-1-5386-4110-1/18

[8] K. Balasamy, S. Ramakrishnan, “An intelligent reversible watermarking system for authenticating medical images using Wavelet and PSO”, Cluster Computing, 2018, Springer, doi:10.1007/s10586-018-1991-8(0123456789().,- volV)(012345

[9] H.R. Lakshmi, B. Surekha and S. Viswanadha Raju, “Real-time Implementation of Reversible Watermarking”, Intelligent Techniques in Signal Processing for Multimedia Security, Studies in Computational Intelligence 660, DOI: 10.1007/978- 3-319-44790-2_6

[10] Priya S, Santhi B, Swaminathan P, RajaMohan J, “Hybrid Transform Based Reversible Watermarking Technique for Medical Images in Telemedicine Applications”, International Journal for Light and Electron dx.doi.org/10.1016/j.ijleo.2017.07.060

[11] 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

[12] Abhilasha Sharma, Amit Kumar Singh, Satya Prakash Ghrera, Optics, "Robust and Secure Multiple Watermarking for Medicalb Images", Wireless Pers Commun, 2016, Springer, DOI: 10.1007/s11277-016-3625-x

[13] Nai-Kuei Chen, Chung-Yen Su, Che-Yang Shih, Yu-Tang Chen, "Reversible Watermarking for Medical Images Using Histogram Shifting with Location Map Reduction", 2016 IEEE, 978-1-4673-8075-1/16

[14] R. Surya Prakasa Rao, Dr. P. Rajesh Kumar, "An Efficient Genetic Algorithm Based Gray Scale Digital Image watermarking for Improving the Robustness and Imperceptibility", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016, 978-1-4673-9939-5/16

[15] Asna Furqan, Munish Kumar, "Study and Analysis of Robust DWT-SVD Domain Based Digital Image Watermarking Technique Using MATLAB", 2015 IEEE International Conference on Computational Intelligence & Communication Technology, 10.1109/CICT.2015.74 978-1-4799-6023-1/15, DOI