Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 1s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Developing a secure and private tele pharmacy platform for remote medication management

Sanjay Kumar Mire[1], Kishor Kumar Sahu[2]

[1]Assistant Professor, Department of Pharmacy, Kalinga University, Raipur, India.
[2] Research Scholar, Department of Pharmacy, Kalinga University, Raipur, India.

Cite this paper as: Sanjay Kumar Mire, Kishor Kumar Sahu, (2025) Developing a secure and private tele pharmacy platform for remote medication management. *Journal of Neonatal Surgery*, 14 (1s), 537-541.

ABSTRACT
Implementing the e-healthcare paradigm has gained popularity recently throughout different research communities on a global scale. Through the use of contemporary information and communication technology, the e-healthcare solution sends the pertinent patient data to a distant healthcare facility and the relevant medical specialists. Sensitive data access and transmission methods over unprotected channels, however, are dangerous and provide serious security risks. Protecting patient medical information security from unauthorized access or users is crucial, according to standard agencies. Furthermore, studies have shown that identity theft pertaining to medical conditions is a growing and serious crime. Watermarking, steganography, and cryptography are the three methods used to safeguard medical data. Watermarking is the most widely used and promising of these strategies. Hence, medical image data and their dimensionalities are rapidly expanding. Because of these expansions in medical data, manually managing the file system is becoming increasingly challenging. Therefore, the management of medical data has become a major concern for healthcare practitioners. In the medical field, cloud computing is commonly utilised for storing, computing, and exchanging patient medical records. The hospital merely needs to collect patient information from files and upload the data to the cloud for storage via cloud computing.

Keywords: *health, information, DWT, DCT, experimental, management.*

1. INTRODUCTION

Telemedicine services are being used extensively in the current situation and are being accepted worldwide [1]. To properly sustain itself and meet the demands of those involved in the health sector, the constantly expanding health industry needs the newest technology developments [11]. According to a survey on identity theft, it is a major crime and a major contributor to fraud worldwide [3]. Furthermore, maintaining the security of patient and health data is a major challenge when implementing telecare [14]. These applications need the authentic and tamper-resistant dispensing of health information, which is ensured by adding a visible or invisible piece of data (watermark) that is secure and resistant to all types of attacks [2]. Researchers frequently focus on the ability of watermarking systems to resist attacks while maintaining security [15]. In order to address the issues surrounding the management of health data, researchers are increasingly combining digital watermarking with encryption-decryption systems [5]. The watermarking techniques are divided into domain-specific categories, such as transform and spatial approach [8]. The superiority of transform domain approaches over spatial methods has been demonstrated by analytical research [10]. Several prerequisites, including imperceptibility, robustness, capacity, and security, are essential for every watermarking technique, according to the literature review that was published [6]. However, it is a demanding topic for researchers and difficult to maintain these requirements (at the same time) [12]. Although several researchers have employed strong watermarking approaches, they are sacrificing other equally crucial needs in the process. Some are computationally complex yet extremely secure [4]. Therefore, this research project intends to suggest some solutions for medical information by using secure watermarking techniques, driven by such intriguing difficulties in the field of e-healthcare. Thus, the following are the main goals of the current work:

- To evaluate the effectiveness of several cutting-edge medical image watermarking techniques in order to determine which is the most promising.
- To improve performance in terms of important factors against attacks by developing the watermarking technique or techniques for medical data security.
- To simultaneously address the issues of computational complexity, security, imperceptibility, and robustness of confidential medical information.

- To assess how well the suggested technique or techniques perform against known signal processing assaults using a standard measure.

2. PROPOSED METHODOLOGY

The first approach suggests a transparent, safe, and reliable watermarking for medical photographs. This is accomplished by proposing a transform domain-based watermarking for e-healthcare. The proposed method subtly embeds the patient report or identification in the host image using DWT, DCT, and SVD [6]. The proposed work's goal is to offer affordable, reliable, and secure watermarking. The concept is the same as our earlier method (the dual watermarking approach in the NSCT domain); however, this cryptographic mechanism employs substitution-permutation networks and Fiestel networks to offer low-cost security. A thorough evaluation of the strategy demonstrated that it is secure [7], reliable, distortion-free, and computationally simple, outperforming the other strategies now in use. Furthermore, another contribution develops an enhanced DWT-SVD based method for medical applications. Our study aims to solve problems related to health data management. The technology combines chaotic encryption and hamming error correcting coding to provide security and robustness, respectively. We have subtly included less robust data in the cover image's low DWT level and more robust data at the high DWT level in accordance with health data management standards. Our method outperforms current methods for a variety of attacks, according to the performance comparisons. The suggested method is then evaluated using the rotation-13 encryption algorithm rather than chaotic encryption. Compared to other approaches, we found that this one performed better [13].

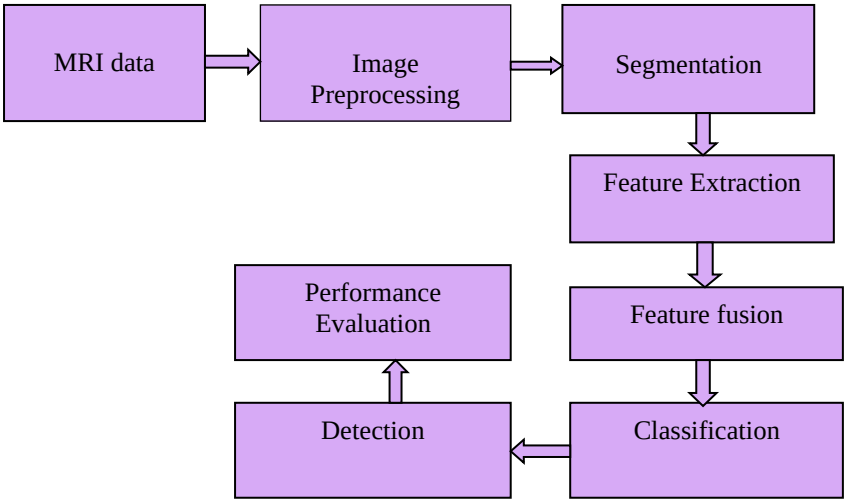

Figure 1: Schematic Diagram of proposed framework

3. EXPERIMENTAL RESULTS

For the purpose of embedding dual watermarks in the NSCTRDWT and SVD domains, a reliable and secure medical image watermarking system is created. In this research, we have developed some improved secure and robust medical image watermarking technique in wavelet domain. Our examination and results confirm that the technique is appropriate data security for medical application.

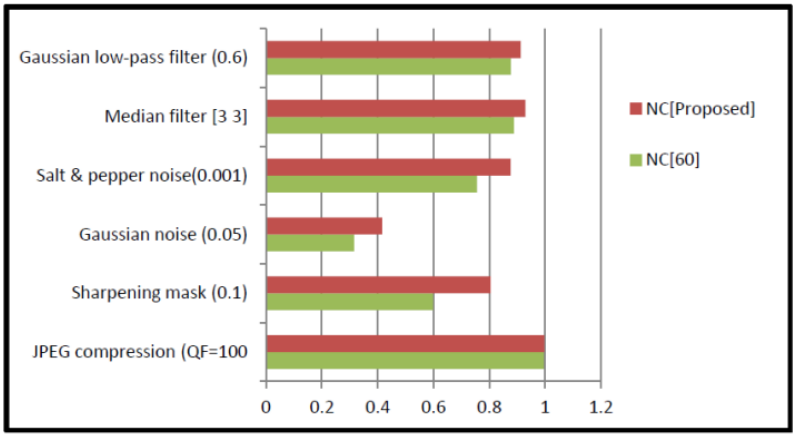

Figure 2: UACI values

The technique's confidentiality is increased by using a low-cost encryption algorithm on the watermarked image.

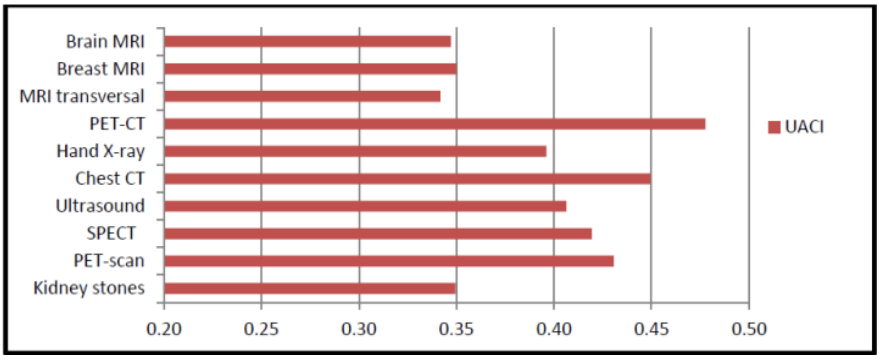

Figure 3: NPCR values

Our technique has been extensively tested on a selected gain value, six medical and four non-medical images, and a variety of common image processing assaults

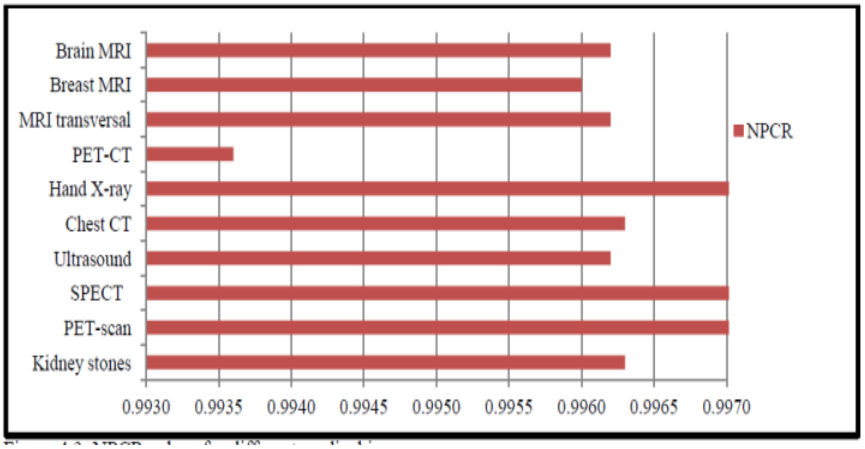

Figure 4: NCI values

Additionally, we have compared our Caesar cipher and chaotic encryption techniques with those suggested in [16], respectively.

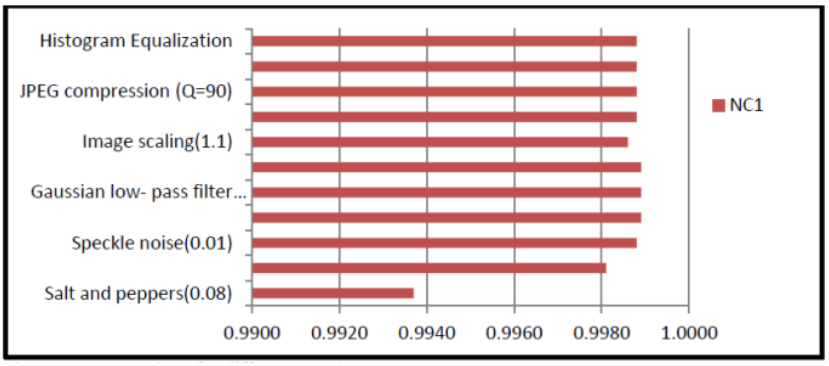

Figure 5: NC2 values

This method is applied over the EPR watermark and involves substituting the thirteenth letter of each related alphabet for each of the text watermark's letters. The entire process took less time because it was put over the text watermark.

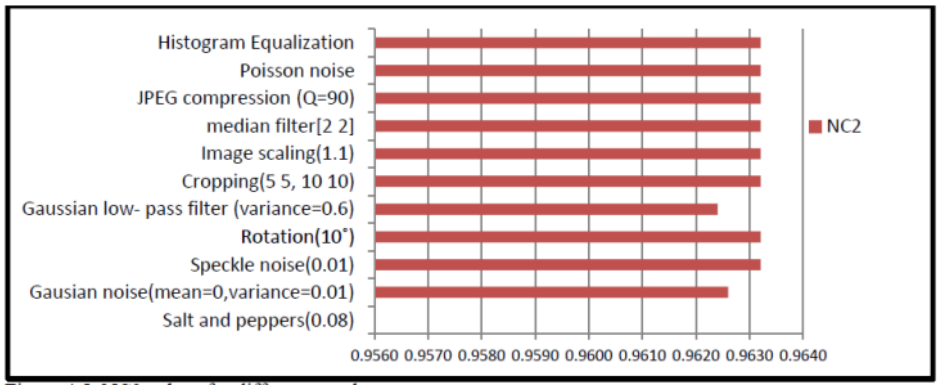

Figure 6: NC3 values

When compared to the previous methods, the new technique offers superior resilience. Our analysis and findings verify that the method is suitable for protecting data in medical applications.

4. CONCLUSIONS

An attacker looks for connections between the appropriate encrypted image and the plain text image. In order to prevent the attacker from accessing any information, encryption algorithms attempt to create a significant difference between the plain text image and the corresponding encrypted image. An effective method for embedding watermarks in the DWT-DCT and SVD domains for medical images was provided in this chapter. Medical data is protected using an encryption method based on chaos. The objective and subjective results demonstrated that the scheme is resilient to various attacks and that it improved the NC value compared to previous methods. However, the result is dependent on the watermark size, noise level, and gain factor value. The developed technique attempts to offer a possible solution to address security issue of EPR data.

REFERENCES

[1] Lechner NH. An overview of cybersecurity regulations and standards for medical device software. InCentral European Conference on Information and Intelligent Systems 2017 (pp. 237-249). Faculty of Organization and Informatics Varazdin.

[2] Govindarajan R, Dhanavandan S. Information Literacy among Ophthalmologists: A Study. SRELS Journal of Information Management. 2019 Feb 28;56(1):51-60. https://doi.org/ 10.17821/srels/ 2019/v56i1/139605

[3] Anderson S, Williams T. Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge?. Computer Standards & Interfaces. 2018 Feb 1;56:134-43. https://doi.org/10.1016/j.csi.2017.10.001

[4] Park HB, Kim Y, Jeon J, Moon H, Woo S. Practical Methodology for In-Vehicle CAN Security Evaluation. J. Internet Serv. Inf. Secur. 2019 May;9(2):42-56.

[5] Marotta A, Madnick S. Cybersecurity as a unifying factor for privacy, compliance and trust: The Haga Hospital case. Issues in Information Systems. 2022 Jan 1;23(1).

[6] Kwon J, Johnson ME. Healthcare security strategies for regulatory compliance and data security. In2013 46th Hawaii International Conference on System Sciences 2013 Jan 7 (pp. 3972-3981). IEEE. https://doi.org/10.1109/HICSS.2013.246

[7] Kelly B, Quinn C, Lawlor A, Killeen R, Burrell J. Cybersecurity in Healthcare. Trends of Artificial Intelligence and Big Data for E-Health. 2023 Jan 2:213-31. https://doi.org/10.1007/978-3-031-11199-0_11

[8] Laouamer L, Euchi J, Zidi S, Mihoub A. Image-to-Tree to Select Significant Blocks for Image Watermarking. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 2020;11(1):81-115.

[9] Thomasian NM, Adashi EY. Cybersecurity in the internet of medical things. Health Policy and Technology. 2021 Sep 1;10(3):100549. https://doi.org/10.1016/j.hlpt.2021.100549

[10] Dhamala K. Pharmacist-Delivered Interventions on Pain Management: Review and Cluster-Randomized Trial. Clinical Journal for Medicine, Health and Pharmacy. 2024 Dec 20;2(4):11-20.

[11] Lee CD, Ho KI, Lee WB. A novel key management solution for reinforcing compliance with HIPAA privacy/security regulations. IEEE Transactions on Information Technology in Biomedicine. 2011 May 12;15(4):550-6. https://doi.org/10.1109/TITB.2011.2154363

[12] Deepika J, Rajan C, Senthil T. Improved CAPSNET model with modified loss function for medical image

classification. Signal, Image and Video Processing. 2022 Nov;16(8):2269-77. https://doi.org/10.1007/s11760-022-02192-5

[13] Busdicker M, Upendra P. The role of healthcare technology management in facilitating medical device cybersecurity. Biomedical Instrumentation & Technology. 2017 Nov;51(s6):19-25. https://doi.org/10.2345/0899-8205-51.s6.19

[14] Udayakumar R, Anuradha M, Gajmal YM, Elankavi R. Anomaly detection for internet of things security attacks based on recent optimal federated deep learning model. J Internet Services Inform Secur.. 2023;13(3):104-21.

[15] Abraham C, Chatterjee D, Sims RR. Muddling through cybersecurity: Insights from the US healthcare industry. Business horizons. 2019 Jul 1;62(4):539-48. https://doi.org/10.1016/j.bushor.2019.03.010

[16] Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, Bonacina S. Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors. 2021 Jul 28;21(15):5119. https://doi.org/10.3390/s21155119