Enhancement of Health Services: Advanced Security Mechanism for Telemedicine in Public Health Practice

Debarghya Biswas[1], Ankita Tiwari[2]

[1]*Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India*
[2]*Research Scholar, Department of CS & IT, Kalinga University, Raipur, India*

KEYWORDS
Telemedicine, public health, healthcare services, security, watermarking, encryption, wavelet crypto fast decomposition with penguin optimization (WCFD-PO)

ABSTRACT

The sudden advancement of telemedicine in the healthcare industry presents potential hazards such as cyber-attacks and network susceptibilities, in addition to difficulties in patient privacy, data protection, and public health monitoring. To avoid illegal access, digital watermarking and precise medical image transfer are essential. Thus, for telemedicine in public health action, we introduce a unique security mechanism termed wavelet crypto fast decomposition with penguin optimization (WCFD-PO). Rivest-Shamir-Adelman (RSA), wavelet transforms (WT), and fast random singular value decomposition (FRSVD) encryption algorithms make up the suggested security methodology. By using the methods WT and FRSVD, one can decrease computing complexity and increase robustness. The PO approach offers a better-optimized scale factor in the fewest groups and repetitions as compared to the RSA approach, which is used for encrypting the watermarked image. The proposed mechanism is implemented by employing a Python application. Comprehensive testing indicates that our novel approach functions better than the current techniques, demonstrating the technique's higher efficiency. With the assistance of secure telemedicine solutions, this investigation offers physicians and tech programmers insightful information that will boost public health management.

1. Introduction

Many developments are occurring in the healthcare system. The development of information and communications technology (ICT) was crucial to the change of the health system [1]. As a term used to indicate any treatment offered that involves a level of distance from the patient, telemedicine is explained. Telemedicine involves all forms of virtual patient care, including phone conversations and telerobotic surgery performed by doctors remotely [2]. In underprivileged communities such as remote areas where there is a deficiency or nonexistence of sufficient clinical treatment, telemedicine has been demonstrated to be quite helpful [9]. Telemedicine and telehealth services that are tried-and-true, dependable, and reasonably priced are now widely accessible in both industrialized and developing nations [12]. The field of medicine is information-focused, generating, transmitting, and distributing vast amounts of data regularly [3]. Because of the narrow definition of information and its sensitive nature, this massive amount of data must be disseminated and hidden back even while it is thoroughly verified [4]. Digital watermarking must be used, and medical image transmission must be exact, to prevent unwanted access. We provide Wavelet Crypto Fast Decomposition with Penguin Optimization (WCFD-PO), an inventive security approach for telemedicine in public health efforts.

Related Work

AlOsail et al. [5] examined the global state of healthcare today and highlighted the primary telemedicine integration issues that impede the delivery of all required medical assistance from a distance [13]. The suggested approach, which was examined by general physicians, reflects the primary and fundamental requirements for secure telemedicine services. The goal of Haleem et al. [15] study was to examine the key components, characteristics of treatment processes, and barriers to telemedicine implementation in the healthcare sector [6]. Using health apps for scheduled follow-up appointments could improve communication between doctors and patients as well as increase the chance of follow-up. This also lowers the number of cancellations and improves patient outcomes. Wang et al. [7] provided an outline of digital healthcare's background and applications, discusses its difficulties during the COVID-19 epidemic, and concludes by outlining the field's future possibilities. Future application opportunities for digital healthcare were presented in that paper. Furthermore, they offered policy suggestions for other nations utilizing digital technologies in their fight against COVID-19. Al-

Samarraie et al. [8] examined how telemedicine has been used and used in Middle Eastern nations. The main factors influencing how far along telemedicine was in these nations have been determined. The findings demonstrated that the Middle Eastern countries have made varying degrees of development in the use of telemedicine. Block Heal, an effective telehealth infrastructure developed by Bawany et al. [14] combines all essential medical facilities onto a single framework and ensures a completely working, reliable environment. Together with a variety of decentralized applications (DApps), it provided decentralized storage through the use of hyper ledger fabric. In conclusion, the Block Heal framework's efficacy was confirmed through the presentation of multiple applications. Poleto et al. [10] were to suggest a methodology for managing cyber security risks in telemedicine. The primary discovery of the work was that risk management and loss prevention are achievable for all parties engaged in the method of transferring medical image data via telemedicine services by using an organized model.

Proposed Work

The following wavelet crypto fast decomposition with penguin optimization (WCFD-PO) based watermarking method is used in the current work to examine how the scaling factor affects PSNR. The various metrics such as PSNR, NC, and SSIM are used to evaluate the study. Wavelet Transform (WT): The Wavelet transform, which was created to address the drawbacks of the Fourier transform, has strong capabilities in data processing and evaluation. Multiple domains, including signal processing, image processing, pattern recognition, and more, have effectively used it. This algorithm depends on the principles of multi-resolution evaluation and operates by initially filtering the processed signal followed by down-sampling the filtered outcomes to achieve fast decomposition of wavelets. The decomposition process for multi-level wavelets is applied in a cascading fashion, whereby the lower-frequency elements produced by the preceding decomposition are used to determine the wavelet transform of each layer. Furthermore, the equivalent decomposition algorithm's reversal operation is the rapid wavelet reconstruction procedure. Equation (1) provides the fundamental workings of the wavelet transform.

$$z[m]=(w*h)[m]=\sum_{l=-\infty}^{\infty} [w[l]h[m-l]] \quad (1)$$

Rivest-Shamir-Adelman (RSA): Encrypting data exchanged over the internet using a public-key encryption method that needs two keys is the industry norms. RSA is one of the methods used in Ubuntu and Launchpad software to provide fairly high privacy security. An enormous tangle of garbage that requires a lot of computing power as well as patience to decipher is the result of RSA encryption. The encryption key is very sophisticated, simple, and validated. It also happens to be one of the most widely researched and utilized cryptographic keys. Fast Randomized Singular Value Decomposition (FRSVD): The robust matrix decomposition technique known as RSVD has a lower computational complexity than SVD. The technique of random sampling is used to execute RSVD, which reduces the matrix and hence the processing duration and then performs the SVD process. FRSVD is explained in and is comparable to RSVD but faster than RSVD. It can be expressed mathematically as follows about a matrix B.

$$[A]=[qV\ qT\ sU^S] \quad (2)$$

The orthogonal matrices qV and qT are shown here, and the singular matrix sU^S is made up of singular values arranged in decreasing order. Penguins search optimization (PeSO): The collective hunting behavior of penguins to look for and find food has been influenced by this algorithm. Penguins typically travel in packs when seeking and reside in groups. The actual optimal value of the objective function shows where there is enough food or a significant amount of food fish resources; other solutions (penguins) will gravitate toward the best alternative after identifying these location sites that have been recognized. Here is how this movement is expressed mathematically:

$$〖Sol〗_{new}^j=〖Sol〗_{old}^j+(〖Sol〗_{best}-〖Sol〗_{old}^j)\times rand \quad (3)$$

Where 〖Sol〗_best= the best is identified solution, 〖Sol〗_new^j is the j^th changed solution, 〖Sol〗_old^jis the j^thsolution before modification, and rand is a random value between 0 and 1 that facilitates the search of more locations (creating answers diversity). Modified penguins search optimization (MPeSO): To keep things simple and work well enough, the original algorithm does not include an investigation operator. Adaptive algorithms depend on stochastic search to solve intricate issues. When examining penguins in the wild, one may see that they frequently abruptly alter their hunting route. It can be possible to improve the algorithm's efficiency by introducing this unforeseen movement as an exploring method. The technique derived from Equation (4) was modified in the current work to include a Gaussian exploration parameter. The findings of the algorithm's original version, in addition to its modified version, are presented below.

$$〖Sol〗\_new^{(j,i)}=〖Sol〗\_old^{(j,i)}+\sigma\times randn \quad (4)$$

Here, σ = Gaussian exploration dimension, 〖Sol〗_old^(j,i) = the i^th decision variable before modification relating to j^th solution, 〖Sol〗_new^(j,i) = the i^thdecision variable corresponding to j^th solution, and rand n demonstrate several normal distributions with mean equal to zero and deviation from mean equal to one. The Modified Penguins search algorithm flowcharts are displayed in Figure 1.

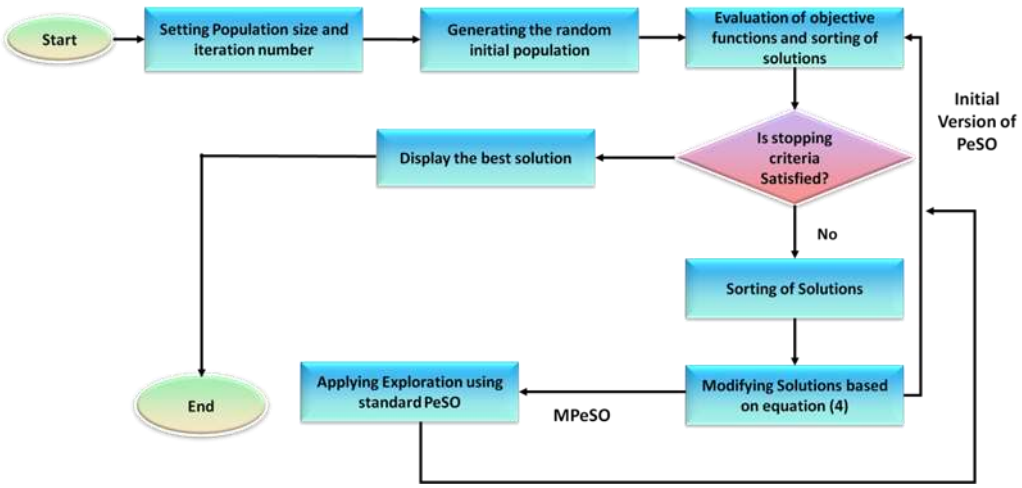
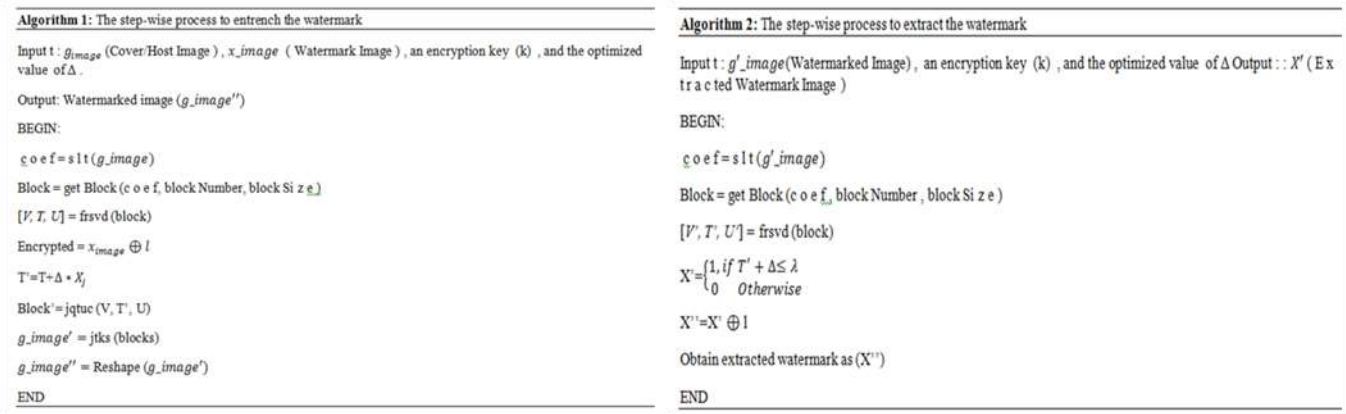


Figure 1. Modified penguins search algorithm

Watermark Embedding and Extraction

The process of watermark embedding entails changing the cover image with a WT, embedding it in a lower-frequency sub-band (Figure 2- algorithm 1), encrypting the watermark bits, enforcing an additive quantization mechanism, converting the coefficients into blocks, putting the watermark bits through FRSVD putrefaction, and using the PeSO to obtain a scaling factor D. Next, to get the watermarked image, the inverse RSA transform is used. The method for extracting watermarks using Figure 2 (Algorithm 2), which accepts as input h^' images, encryption key, and MSF. In step six, the retrieved watermark is deciphered after the watermarked image has been transformed using WT, the coefficients have been transformed into blocks, FRSVD has been resolved, and watermark bits have been recovered.



Algorithm 1: The step-wise process to entrench the watermark

Input t : g_{image} (Cover/Host Image) , x_image (Watermark Image) , an encryption key (k) , and the optimized value of Δ .

Output: Watermarked image (g_image'')

BEGIN:

$coef = slt(g\_image)$

Block = get Block (coef, block Number, block Size)

$[V, T, U]$ = frsvd (block)

Encrypted = $x_{image} \oplus l$

$T' = T + \Delta * X_j$

Block' = jqtuc (V, T', U)

g_image' = jtks (blocks)

g_image'' = Reshape (g_image')

END

Algorithm 2: The step-wise process to extract the watermark

Input t : g'_image(Watermarked Image) , an encryption key (k) , and the optimized value of Δ Output : : X'' (Extracted Watermark Image)

BEGIN:

$coef = slt(g'\_image)$

Block = get Block (coef, block Number , block Size)

$[V', T', U']$ = frsvd (block)

$$X' = \begin{cases} 1, if\ T' + \Delta \leq \lambda \\ 0 \quad Otherwise \end{cases}$$

$X'' = X' \oplus l$

Obtain extracted watermark as (X'')

END

Figure 2. Algorithm for watermark embedding and extraction

2. Results and discussion

The impacts of the WCFD-PO that have been examined are discussed in this section. In this investigation, a variety of medical image data have been used. The medical images no longer include any information about the patient. This section also covers the outcomes of our experiments and the implications of various quality metrics. Table 1 displays the medical image watermarking outcomes of PSNR, NC, SSIM, and UACI metrics. The work demonstrated a low gain factor and high PSNR ultrasonic image watermark perceptibility method. The expected approach has good perceptual quality and a large gain factor. The image ratio of change in terms of pixel values revealed modest changing intensity, and the SSIM value varied from 0.80 to 0.90. When it comes to integrating bitmap watermark pictures into host color medical images, the expected approach performs better overall.

Table 1.The outcomes of the proposed WCFD-PO

No. of images	PSNR	NC	SSIM	UACI
1	54.351	1.004	0.8081	0.2723
2	53.590	0.981	0.9557	0.3443
3	52.970	0.976	0.9762	0.3430
4	51.844	1.125	0.8561	0.3245
5	51.767	0.979	0.8861	0.3118
6	50.618	0.980	0.9110	0.3338
7	50.347	0.995	0.9431	0.3540
Average value	52.212	0.863	0.905	0.326

Using SSIM and PSNR measures, we compare the proposed WCFD-PO with the Finite Ridgelet Transform Hessenberg Decomposition (FRT-HD) [11]. This comparison assesses both techniques' efficacy and performance. The effectiveness of the suggested watermark extraction approach is tested using a set of medical images that have been watermarked. We have employed a range of image-processing operations to assess the effectiveness of the watermarking method and the watermark extraction procedure. As Table 1 illustrates, the SSIM value varied between 0.78 and 0.97. Following a median filter assault, the retrieved watermark's SSIM values are as follows: 0.89659 for sparse noise, 0.9890 for sharpening attack, 0.8976 for JPEG compression, 0.27290 for histogram equalization, 0.88399 for average filter, and 0.99602 for Gaussian low-pass filter. The retrieved watermarked images' SSIM values attest to the watermarked image's resilience against attacks. The expected strategy fared better under different kinds of image attacks, according to the SSIM values. Figure 3 illustrates the comparison outcomes of the proposed method and the existing method.

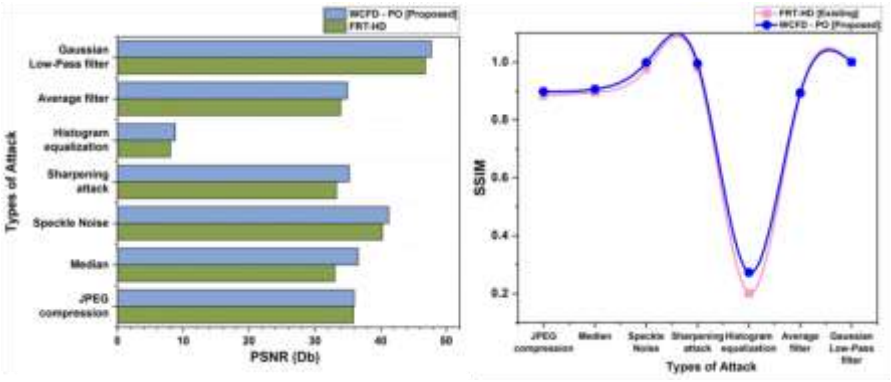


Figure 3. Comparison outcomes of proposed (WCFD-PO) and existing methods (FRT-HD)

3. Conclusion and future scope

Strategic planning, construction of infrastructure, and execution are necessary for the creation of creative and effective telemedicine, telehealth, and e-health initiatives. The study developed wavelet crypto fast decomposition with penguin optimization (WCFD-PO) for advanced security mechanisms for telemedicine in public health assessment. The proposed WCFD-PO approach was compared with various parameters such as PSNR, NC, SSIM, and UACI. Computing complexity can be reduced and robustness can be raised by utilizing the WT and FRSVD approaches. Compared to the RSA technique, which is utilized to encrypt the watermarked image, the MPSO approach provides a more optimized scale factor in the fewest groups and repetitions. Extensive testing demonstrates the higher efficiency of the current procedures and shows that the innovative strategy performs better than them. To illustrate the effectiveness of the proposed method as an advanced security mechanism for telemedicine in public health, it was compared to the existing systems. Its outcomes in public health telemedicine are noticeably superior to those of any other method now in use.

Reference

[1] D., N. Amino, and N. Mohammad, "Security issues and solutions in e-health and telemedicine", In *Computer Networks, Big Data, and IoT: Proceedings of ICCBI 2020. Springer Singapore 2021*, pp. 305-318, 2021. https://doi.org/10.1007/978-981-16-0965-7_26

[2] N.D. Hettikankanamage, and M.N. Halgamuge, "Digital health or internet of things in telehealth: a survey of security issues security attacks, sensors, algorithms, data storage, implementation platforms, and frameworks", *IoT in Healthcare and Ambient Assisted Living*, pp.263-292, 2021. https://doi.org/10.1007/978-981-15-9897-5_13

[3] S. Neelima, Manoj Govindaraj, Dr.K. Subramani, Ahmed ALkhayyat, & Dr. Chippy Mohan. (2024). Factors Influencing Data Utilization and Performance of Health Management Information Systems: A Case Study. Indian Journal of Information Sources and Services, 14(2), 146–152. https://doi.org/10.51983/ijiss-2024.14.2.21

[4] N. Jain, V. Gupta, and P. Dass, "Blockchain: A novel paradigm for secured data transmission in telemedicine", In *Wearable telemedicine technology for the healthcare industry*, *Academic Press*, pp. 33-52, 2022. https://doi.org/10.1016/B978-0-323-85854-0.00003-4

[5] A. Romanovs, E. Sultanovs, E. Buss, Y. Merkuryev, and G. Majore, "Challenges and solutions for resilient telemedicine services", In *2020 IEEE 8th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, pp. 1-7, *2021*. https://doi.org/10.1109/AIEEE51419.2021.9435776

[6] Sonya, A., & Kavitha, G. (2022). A Data Integrity and Security Approach for Health Care Data in Cloud Environment. Journal of Internet Services and Information Security, 12(4), 246-256.

[7] Q. Wang, M. Su, M. Zhang, and R. Li, "Integrating digital technologies and public health to fight Covid-19 pandemic: key technologies, applications, challenges and outlook of digital healthcare", *International Journal of Environmental Research and Public Health*, *18*(11), p.6053, 2021. https://doi.org/10.3390/ijerph18116053

[8] H. Al-Samarraie, S. Ghazal, A.I. Alzahrani, and L. Moody, "Telemedicine in Middle Eastern countries: Progress, barriers, and policy recommendations", *International journal of medical informatics*, *141*, p.104232, 2020. https://doi.org/10.1016/j.ijmedinf.2020.

[9] Malathi, K., Shruthi, S.N., Madhumitha, N., Sreelakshmi, S., Sathya, U., & Sangeetha, P.M. (2024). Medical Data Integration and Interoperability through Remote Monitoring of Healthcare Devices. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 15(2), 60-72. https://doi.org/10.58346/JOWUA.2024.I2.005

[10] T. Poleto, M.M. Silva, T.R.N. Clemente, A.P.H. de Gusmão, A.P.D.B. Araújo, and A.P.C.S. Costa, "A risk assessment framework proposal based on bow-tie analysis for medical image diagnosis sharing within telemedicine", *Sensors*, *21*(7), 2021. p.2426. https://doi.org/10.3390/s21072426

[11] Kumar, L. and Singh, K.U., "Color ultrasound image watermarking scheme using FRT and Hessenberg decomposition for telemedicine applications". *Journal of Universal Computer Science*, *28*(9), 2022. p.882. https://doi.org/10.3897/jucs.94127

[12] G. Márquez, H. Astudillo, and C. Taramasco, "Security in telehealth systems from a software engineering viewpoint: A systematic mapping study", *IEEE Access*, *8*, pp.10933-10950, 2020. https://doi.org/10.1109/ACCESS.2020.2964988

[13] Bobir, A.O., Askariy, M., Otabek, Y.Y., Nodir, R.K., Rakhima, A., Zukhra, Z.Y., Sherzod, A.A. (2024). Utilizing Deep Learning and the Internet of Things to Monitor the Health of Aquatic Ecosystems to Conserve Biodiversity. Natural and Engineering Sciences, 9(1), 72-83.

[14] N.Z.Bawany, T. Qamar, H. Tariq, and S. Adnan, "Integrating healthcare services using blockchain-based telehealth framework", *IEEE access*, *10*, pp.36505-36517, 2022. https://doi.org/10.1109/ACCESS.2022.3161944

[15] A. Haleem, M. Javaid, R.P. Singh, and R. Suman, "Telemedicine for healthcare: Capabilities, features, barriers, and applications", *Sensors international*, *2*, p.100117, 2021. https://doi.org/10.1016/j.sintl.2021.100117