Noise Resistant and Compression Sensing Image Encryption for Medical Image based on Chaos and Wavelet Domain in Matlab

Dr.R.Kathirvel
Professor,
Department of electronics and communication engineering,
Mahendra engineering college, namakkal, tamilnadu, India.

K.Raghul,
Department of electronics and communication engineering,
Mahendra engineering college, namakkal, tamilnadu, India.

M.Mohan Prasath
Department of electronics and communication engineering,
Mahendra engineering college, namakkal, tamilnadu, India.

A.Surya
Department of electronics and communication engineering,
Mahendra engineering college, namakkal, tamilnadu, India.

M.S.Mohamed Musthafa
Department of electronics and communication engineering,
Mahendra engineering college, namakkal, tamilnadu, India.

Abstract - The amount of medical data is rapidly increasing as a result of different disease diagnoses. Additionally, Telemedicine may result in incorrect disease diagnosis due to pixel distortion during medical picture transmission over a public network. In this case, DNA cryptography combined with various chaos-based scheme encryption of the image can be protective. Because chaotic schemes are very dependent on the beginning conditions, even a slight variation in those parameters results in completely uncorrelated sequences that guarantee the encryption strength. Several DNA encoding and computing rules are used to obtain high unpredictability. This thesis suggests a multi-stage chaotic encryption method using DNA cryptography and a logistic map in conjunction with a Lorenz attractor, where both systems have the highest value of control parameters. As a result, the successive deployment of them produces enormously chaotic sequences that guarantee the stability of the suggested method. First, applying the logistic map with the SHA-256 hash value results in a disorganized sequence that changes the straightforward medical image into a perplexing one. Now, to encrypt this hazy image, this sequence is employed to generate a confusion key. Afterwards, encode this blur image and Lorenz attractor-based key in accordance with DNA encoding rules in order to go beyond the constraints of DNA computing rules and obtain high randomness. Eight encoding rules are used to randomly decide these rules. Then, apply the four DNA computing rules—which are also established by a chaotic logistic sequence—to carry out DNA operations between the encoded blur image and Lorenz NIST a statistical and security attractor key. Consequently, the final A cipher is produced. Next, a randomness test is performed to confirm the cipher's strength.

I.INTRODUCTION

The application of medical imaging techniques has become essential in the field of contemporary healthcare for precise diagnosis, treatment planning, and condition monitoring. Nonetheless, there are several obstacles to overcome in order to transmit and store medical images securely and with integrity. Extensive research efforts have been made to develop robust encryption algorithms adapted to the specific properties of medical images in

response to the growing need for effective and secure methods of encrypting medical images. This study provides a novel approach for compression-sensitive and noise-resistant picture encryption specifically tailored for medical photos in answer to this requirement. Our suggested methodology leverages the synergistic combination of wavelet domain processing and chaos theory to provide a comprehensive solution that satisfies the two goals of being compatible with compression techniques and resilient against noise interference. An effective foundation for creating deterministic and complex cryptographic keys is provided by chaos theory, which raises the encryption scheme's level of security. Our encryption approach assures unpredictability and non- repeatability by taking advantage of the inherent chaotic dynamics. These are important features for protecting sensitive medical picture data from tampering or unwanted access. Moreover, the incorporation of wavelet transform in the encryption procedure permits the effective representation of picture features at various scales, hence promoting robustness against noise and compression. Our technique can adapt to different levels of noise contamination and compression artifacts by using the multi-resolution analysis that wavelet domain processing provides, maintaining the diagnostic integrity and image quality. Our suggested encryption system, which is implemented in MATLAB, provides a versatile and adaptable platform for medical image encryption that can handle a range of imaging modalities and data formats that are commonly used in clinical practice. We validate the appropriateness of our encryption technique for practical medical imaging applications by demonstrating its efficacy and robustness in reducing noise distortion and maintaining image quality under compression, which we achieved through comprehensive experimentation and performance evaluation.

To sum up, this study presents a novel approach that smoothly merges wavelet domain processing and chaos theory to accomplish noise-resistant and compression-sensitive encryption, providing a comprehensive solution to the urgent problems of medical picture encryption. Our suggested methodology has the potential to improve the confidentiality, integrity, and accessibility of sensitive medical image data by pushing the boundaries of medical image security. This will provide medical professionals with safe and dependable diagnostic tools for better patient care.

RELATED WORK

Many academics have successfully completed a large amount of security work on the security of digital data in recent years [32]– [38]. However, the majority of the current work still has certain shortcomings that need to be significantly addressed. The earlier research on digital data security is included in this section, along with certain disadvantages of the current encryption techniques. In order to save the computational time required for encryption, Wang et al. attempted to accomplish both confusion and diffusion at the digital images created with intricate chaos-based mathematical functions. He also suggested creating a new chaotic map by fusing various chaotic structures, which he then included into his suggested encryption method. In order to improve security, the encryption system uses five rounds as opposed to just one. For real-time applications, we needed processing times that were short.

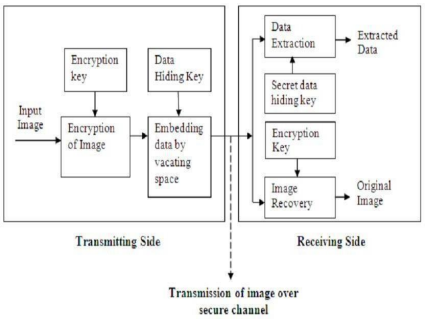
The processing time required for encryption and security are always trade-offs. It goes without saying that the encryption scheme's security improves as the number of rounds increases. However, increasing the number of rounds to improve security necessitates a trade-off in processing speed, making it unsuitable for real- time applications. Shafique et al. [41] proposed a bit-level encryption system (IEC-BPMC) in contrast to [40], where the author(s) simply applied the permutation function on the most important bit planes in order to minimize computational time. The MSBs bit-planes contain the majority of the information, which explains the situation. As we move from the MSBs to the LSBs bit-planes, the information content gradually diminishes. Even though the encryptiontechniques were created by the author(s) for real- time applications, security was breached and there was abreak-in [42]. Wen et al. conducted cryptanalysis on the encryption strategy that was suggested in[41] in [42]. To breach the IEC- BPMC, the author employed a specific plaintext attack mechanism.

In bit-plane encryption techniques, a plain image can be restored with minimal information loss by merging just four MSB bit-planes. It is possible to obtain great security with reduced processing time by using this technology, but the encryption system would be lossy, making it unsuitable for situations where precise information recovery is essential. Wang et al. [43] asserted in 2014 that the encryption approach suggested in [44] is not secure against attacks utilizing chosen-plaintext. Zhang and Xiao [45] developed a cryptosystem based on bit-level permutation and diffusion only method to overcome the shortcomings of the encryption scheme proposed in [44]. Shannon’s theory states that the presence of a confusion diffusion mechanism any strengthens, Cryptosystem. Although the encryption plan putforward [45] was only dependent on the diffusion mechanism, it can be seen as insecure as it does not meet Shannon's requirements. The encryption system proposed by the author(s) in [46] likewise fails to meet the requirements of the theory outlined in [21]. A novel bit-level permutation encryption was proposed by Xu et al. in [47], where the "permutation-diffusion" process was employed by the author or authors. A bit-level and pixel-level substitution-based encryption

technique was later presented in [48]. In some circumstances, pixel level substitution—such as multiple substitution box (S-box) encryption— may be robust [49]. However, bit-level replacement is ineffective in this scenario since bit-planes only have two values: 0 and 1. In [49], the pixel substitution issues are discussed. The single S-box encryption is inappropriate for images that contain both a higher and a lower number of gray scale. By tackling the single S-box encryption challenge, the author(s) proposed an encryption strategy to alleviate these problems. Several S-boxes were employed in his suggested work to increase the encryption algorithm's security. In substitution- based cryptosystems, the strength of the S-box is crucial, in addition to the use of numerous S- boxes. Shafique et al. suggested a novel approach in [50] for building a strong S-box to improve substitution-based encryption techniques. Researchers' interest in substitution-based encryption has grown significantly. Although substitution-based encryption techniques have advanced significantly in recent years, their long processing times remain a serious drawback.

EXISTING METHOD

In this paper, we offer a unique noise-resistant and compression-sensing-efficient approach for encrypting medical photos. The technique preserves image quality while achieving strong encryption by utilizing wavelet domain modifications and chaos theory. Discrete wavelet transform (DWT) is used in the process to convert the original medical image into the wavelet domain. Subsequently, wavelet coefficients are subjected to chaos-based scrambling in order to improve encryption security. Carefully chosen,the chaotic map for scrambling ensures resilienceto noise and threats. Following the scrambling process, compression sensing methods are used tominimize the encrypted image's size without sacrificing crucial diagnostic characteristics. A collection of medical photographs was used in the trials to assess the effectiveness of the suggested strategy. The suggested method's encrypted images were compared to those created by conventional encryption algorithms, and their noise resistance and compression sensing effectiveness were evaluated. The findings show that the suggested strategy performs better than current methods in terms of efficiency and security.



BLOCK DIAGRAM OF EXISTING METHOD

WORKING PROCEDURE

The following actions are suggested to encrypt medical images while guaranteeing noise resistance and effective compression sensing:

Step 1: Read the original, encrypted medical image.
Step 2: To make processing easier, convert the image to frames.
Step 3: To improve security, encrypt the frames using the XOR encryption method.
Step 4: To facilitate efficient processing, divide the encrypted frames into blocks of 4x4, 8x8, or 16x16 sizes.
Step 5: To find areas of notable motion, estimate motion based on both intra- and inter-frames.
Step 6: To make integration easier, convert the secret data that will be embedded inside the frames into integer numbers.
Step 7: Based on the motion that has been observed, locate areas inside the frames where data can be placed.
Step 8: Integrate the encrypted data into the frames' recognized motion regions.
Step 9: Restore the altered frames to their original image format so they can be processed and analyzed further.
Step 10: Use the proper decryption algorithm to decrypt each frame from the encrypted image.
Step 11: Extract the embedded data for additional research or troubleshooting from the decrypted frames.

These procedures provide a methodical way to encrypt medical images that is noise-resistant and allows for effective compression sensing. The purpose of this method is to improve the security and effectiveness of

medical picture encryption in MATLAB by utilizing wavelet domain transforms and chaos theory.

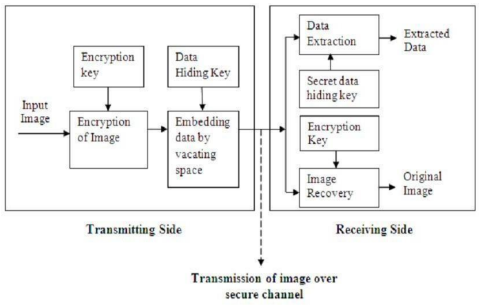
BIT XOR

Based on the ideas of bitwise XOR operations, the XOR cipher, also known as the exclusive OR cipher, is a kind of additive cipher used in cryptography. According to these rules, the result of an XOR operation between a value and 0 stays constant, but the result of an XOR operation between a value and itself is always 0. In addition, XORing C with B will yield A if A XOR B equals C.

When it comes to cryptography applications, the XOR operator has various benefits. First off, because of its ease of use and computational efficiency, it is frequently used in more intricate ciphers. The XOR operation is a favored option for encryption algorithms due to its low computational cost. In real-world applications, a text string can be made encrypted by bitwise XORing every character with a given key. The encryption procedure can then be successfully reversed by applying the same XOR function with the same key to decrypt the encrypted text.

Peak Signal-to-Noise Ratio (PSNR) is an important factor to take into account in cryptography applications, particularly when encrypting images. A high PSNR shows that there was little information lost during the encryption process and that the encrypted image resembles the original image. The fact that the XOR cipher little impairs the quality of the encrypted image is another benefit. This feature makes sure that the encrypted image looks the same as the original, which makes decryption and analysis more precise.

In conclusion, the XOR cipher is a useful tool in cryptographic applications, especially for picture encryption, where preserving data integrity and image quality is crucial. It provides simplicity, computational efficiency, and little impact on image quality.



CONCLUSION

To sum up, there are a lot of interesting opportunities to improve the security and effectiveness of medical picture transmission and storage through the use of noise-resistant and compression sensing image encryption formedical images based on chaotic and wavelet domain in MATLAB. Through the utilization of sophisticated encryption methods like wavelet transform and chaos-based encryption, this strategy may efficiently safeguard confidential medical data from unwanted access and provide optimal data compression to maximize bandwidth for both storage and transmission. Nevertheless, putting such encryption systems into practice comes with a number of concerns and problems, even with all of its potential advantages. These include the trade-off between security and compression efficiency, sensitivity to factors, computational complexity, and key management concerns. Concerns have also been raised about possible data loss, a lack of standardization, cyberattack susceptibility, resource limitations, the need for regulatory compliance, and difficulties integrating current medical imaging procedures and systems. Thus, even though compression-sensing and noise-resistant image encryption have a lot of potential to improve the security and privacy of medical image data, these issues must be properly addressed in order to guarantee the effective implementation and uptake of these encryption technologies in clinical settings. In order to advance the field of secure medical image encryption and improve patient care andhealthcare delivery, more research and development efforts are required to improve cybersecurity measures, address interoperability issues, optimize parameter settings, refineencryption algorithms, and streamline integration with current medical imaging infrastructure. 9. Regulatory Compliance: Complying with legal requirements, such as the Health Insurance Portability and Accountability Act (HIPAA)

in the US or the General Data Protection Regulation (GDPR) in the EU, makes encryption more difficult to use and may necessitate taking additional security precautions to protect patient privacy and data security.

REFERENCES

[1] Hong, W., Chen, T., and Wu, H. (Apr. 2012), "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202.

[2] Li, X. L., Yang, B., and Zeng, T. Y. (Dec. 2011), "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533.

[3] Ma, K., Zhang, W., et al. (2013). "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, 553-562.

[4] Shafique, Arslan, Jameel Ahmed, Mujeeb Ur Rehman, and Mohammad Mazyad Hazzazi. "Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain." IEEE Access 9 (2021): 59108-59130.

[5] M. Umar, B. L. Rhoads, and J. A. Greenberg, ‘‘Use of multispectral satellite remote sensing to assess mixing of suspended sediment downstream of large river confluences,’’ J. Hydrol., vol. 556, pp. 325–338, Jan. 2018.

[6] C.Nagarajan and M.Madheswaran - ‘Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter’ - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[7] C.Nagarajan and M.Madheswaran - ‘Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis’- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[8] C.Nagarajan and M.Madheswaran - ‘Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques’- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[9] C.Nagarajan and M.Madheswaran - ‘Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis’- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[10] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. “Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter” Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[11] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya “Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay” Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[12] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash “Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM” Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[13] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, “Perfromance Investigation of T-Source Inverter fed with Solar Cell” Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[14] C.Nagarajan and M.Madheswaran, “Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation” has been presented in ICTES’08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[15] M Suganthi, N Ramesh, “Treatment of water using natural zeolite as membrane filter”, Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022

[16] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, “Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District”, International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019