NIPES

Journal of Materials Engineering, Structures and Computation

Journal homepage: www.nipesjournals.org.ng

A Proposed Framework for Enhanced Advanced Encryption Standard for Medical Image in Cloud System Using Fast Fourier Transform

Oladimeji Adegbola Isaac [a], Yusuf Hussaini Amana[b] Njoku Christian Chimere[c] Abolarinwa Michael Oluwagbenga[d]

[a,b,c]Department of Computer Science, Aminu Saleh College of Education, Azare Nigeria
[d]Department of Computer Science, Kwara State University, Malate, Nigeria
Corresponding Author:- oladimejiadeisaac@gmail.com

ARTICLE INFORMATION

Article history:
Received 09 July 2022
Revised 06 August 2022
Accepted 07 August 2022
Available online 9 October 2022

Keywords: *Fast Fourier Transform, Medical Images, Cloud Network*

ABSTRACT

Medical image storage on a cloud network has many advantages, including limitless storage, data portability, and migration. This framework aims to provide a more secure system capable of protecting data privacy in the cloud. This should address the fundamental issues that prevent users from trusting cloud services. The techniques developed in this study will be useful for encrypting confidential or personal images and information in a variety of digital systems such as mobile phones, personal digital gadgets, and so on. It will eliminate flaws, attack vulnerabilities, and threats of intruding into digital content. This proposal focuses on developing a cloud-based system for medical image authentication and encryption using the Enhanced Advanced Encryption Standard (EAES) and the Modified Discrete Wavelet Transform (MDWT). For encryption and decryption, the Fast Fourier Transform - Advanced Encryption Standard (FFT-AES) will be used, while the Discrete Wavelet Transform-Modified Particle Swarm Optimization (DWT-MPSO) will be used for watermarking patient information within the encrypted image

1.Introduction

Modern healthcare practitioners produce enormous amounts of medical images every day as a result of recent improvements in imaging techniques [1]. The adoption of telecommunication technology for medical diagnostics and patient care has heightened the demand for medical image security. A system called telemedicine is employed in situations where the beneficiary and client are geographically apart [2]. Because it enables distant specialist consultations, loss-free, instant access to specific patient data, and greater communication between medical system partners, telemedicine is viewed as being of utmost importance [2].

The increased rate of information exchange among diverse companies, including medical imaging system users, is driving the adoption of novel storage solutions such as the cloud. Cloud computing has emerged as a promising networking pattern for infrastructure patterns capable of deploying large scale applications in a cost-effective manner [3]. Cloud computing

is an environment that encapsulates Internet resources as dynamic, scalable, and virtualized services, allowing people to access a variety of on-demand services such as telemedicine [2]. By lowering the number of redundant tests, possibly saving money, and protecting people from the capacity, data migration, and patient-centric connected systems are all benefits of storing medical images in the cloud, cloud-based medical image sharing will increase patient safety and satisfaction [4].

According to Botta et al. [5], cloud computing has nearly infinite storage and processing power, is a far more established technology, and has at least partially overcome most internet of Things (IoT) challenges, However, Qusay et al. [3] stress that there are a number of significant cloud security concerns present in the cloud computing environment, including issues with mobility and application security, cloud security services and applications, cloud security data. According to Sefer and Abdulrahman [2], the multi-tenancy of the cloud can put data integrity, secrecy, and non-repudiation at risk. In order to prevent such assaults, a high level of integrity and confidentiality assurance is required when sending user data over the cloud environment, particularly medical data because it contains extremely sensitive patient information [6].

According to Nyeem [7], the patient has rights and obligations to health ethics because the protection of medical information is ensured by strong ethical and legal standards. In addition to protecting patient privacy, medical images and other data must be protected to thwart hostile tampering when transferred between medical facilities. A doctor's or radiologist's incorrect diagnosis could lead to major issues or even death if a medical image is tampered with and provided to them [7]. As a result, issues relating to the privacy of medical data must be thoroughly handled by utilizing relevant crypto standards [8]. Cloud storage data security is therefore a shared duty of users and service providers.

1.2 Overview of Advanced Encryption Standard (AES)

Symmetric block ciphers are used in the Advanced Encryption Standard (AES) encryption algorithm [9]. AES, like most symmetric ciphers, is widely used and studiedand it offers advantages over asymmetric ciphers like Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) in terms of needed computing power, processing time, and key length [10]. The majority of the aforementioned studies have common and significant drawbacks that are unique to Advanced Encryption Standard (AES) in terms of the cryptography algorithms used or combined with. Image interference, a lack of appropriate encryption techniques, out-of-date watermarking technology, and other issues exist in the current system [2].

AES provides simple key scheduling and encryption operations. As pointed out by commonlounge.com [11], many AES attacks are based on the ease of this key scheduling, and it is possible that an attack to defeat AES encryption will be created one day. The key must be communicated to the entity with whom you are sharing data, which is the most significant disadvantage of AES symmetric key encryption. Asymmetric techniques such as Rivest-Shamir-Adleman are frequently used to encrypt and transfer symmetric encryption keys separately. [12].

Patients are concerned about the security and ease of retrieval of medical data stored on a cloud platform. Bincy and Senthilnathan [13] proposed an efficient export enforcement coordination center (*E2C2*) visual cryptographic technique for cloud-based encryption of medical images. Based on an out-of-n visual cryptographic scheme, this paper proposes a visual cryptographic technique for secure storage and retrieval of medical images stored in the cloud. The combined effect of AES and visual cryptography makes the suggested method substantially more secure

and resistant to outside attacks. The results of the experiments show that the proposed system can safely store and retrieve medical photos with high clarity. However, it should be noted that the time complexity required to complete the entire procedure is substantial and should be reduced. Ijaz et al. [14] stress that because most known techniques use constant rounds of operation and a straightforward XOR-based diffusion, they are all susceptible to the chosen-plaintext attack. Although rounds of operations can make things more complex, they also take longer to execute, which reduces throughput. The encryption scheme must be complex, reversible, self-adaptive, and parameter sensitive to prevent cryptanalysis, particularly the chosen-plaintext attack [14].

According to Lakshmi et al. [8], the majority of existing image encryption solutions are vulnerable to the chosen-plaintext attack due to the drawbacks associated with the confidentiality of users' data in the cloud environment and subsequent investigation and study of the inadequacy of existing solutions. This is because of the advancement of computer power and the cunning of hackers. The conventional advanced encryption standard (AES) algorithm needs to be enhanced in order to address new security concerns in the cloud context, as Ijaz et al. [14] noted. This framework aims to create an improved advanced encryption standard for medical images in cloud systems by utilizing fast Fourier transforms to protect data privacy in the cloud environment. This should address the fundamental issues that prevent users from trusting cloud services. In other words, the study's goal was to give users control over their data files. Furthermore, the issue of the time complexity required to complete the entire process would be fully addressed.

Because of the shortcomings in advanced encryption standards that offer straightforward key scheduling and encryption functions. Assaults based on this key schedule's simplicity and the possibility that an attack to break advanced encryption standard encryption will be developed one day, as mentioned by commonlounge.com [11], its enhancement is required. This study uses fast Fourier transform to improve the performance of advanced encryption standards in securing medical images in cloud environment

1.3 Fast Fourier Transform (FFT)

An algorithm known as a fast Fourier transform (FFT) calculates the discrete Fourier transform (DFT) or its inverse for a sequence (IDFT). A signal is transformed using Fourier analysis from its native domain, which is frequently time or space, to a representation in the frequency domain, and vice versa [15]. When a sequence of values is broken down into its frequency components, the discrete Fourier transform is produced. Although computing it straight from the definition is typically too slow, this technique is useful in many fields [15]. A method for recreating a periodic graph series harmonics waveform, where the harmonic frequency is defined as a multiple of the fundamental frequency, is fast Fourier transform analysis. By factorizing the discrete Fourier transform matrix into a product of sparse (mainly zero) elements, a fast Fourier transform efficiently computes such transformations.

When using finite-precision floating-point arithmetic, fast Fourier transform algorithms have errors, but these errors are typically quite small; most fast Fourier transform algorithms, e.g. Cooley-Tukey algorithms have excellent numerical properties due to their pairwise summation structure. Because it has made working in the frequency domain as computationally possible as working in the temporal or spatial domains, the fast Fourier transform is crucial [16]. Fast large-integer and polynomial multiplication, effective matrix-vector multiplication for Toeplitz, circulant, and other structured matrices, filtering algorithms, fast discrete cosine or sine transform algorithms, fast Chebyshev approximation, solving difference equations, and

modulation and demodulation of complexes are some of the key applications of the fast Fourier transform.

1.4 Related Work

Many researchers have proposed different approaches, algorithms, and techniques, involving cryptography, Steganography, and even a combination of both, to address all of these issues with Integrity, confidentiality, and non-repudiation of data in cloud-based medical images security, as noted by Lakshmi et al [8]. Image security is more crucial since processing images is more challenging than handling text-based data. Among these suggestions are:

Alowolodu et al. [17] proposed Quantum Cryptography for Medical Image Security, Shor's Algorithm, random secret key generation, and eavesdropping detection (Quantum N Shor's factorizing Algorithm) were used in the design.

Smita et al. [18] proposed medical image encryption and watermarking by combining encryption and watermarking schemes. The proposed approach starts by using saliency detection to derive the image's region of interest (ROI). The salient portion of the image is then encrypted with a complex and highly secure encryption technique, while the non-salient portion is watermarked and encrypted with a simple yet efficient encryption technique.

Askar et al, [19] present a brand-new two-dimensional chaotic logistic economic map-based encryption algorithm. The robustness of the introduced technique is demonstrated by using it on various kinds of photos. The algorithm's implementation and security are partially examined using statistical analyses such as key space sensitivity, pixel correlation, the entropy process, and contrast analysis. The comparisons and results reached lead to the conclusion that the introduced algorithm has high contrast, accepted information of entropy, few coefficients of correlation, a large key security space, and sensitivity to the secret key. The suggested approach is also robust to statistical, differential, brute-force, and noise attacks, according to experimental findings.

In his study on the degradation of medical image quality caused by data embedding in the frequency domain, Khalill [20] presented a different strategy. He employed the Rivest Cipher 4 (RC4) encryption technique for information encryption and decryption, the Least Significant Bit (LSB) technique in the spatial domain, and the discrete Fourier Transform (DFT) technique for steganography in the frequency domain.

Parah et al. [21] used the Pixel to Block (PTB) conversion approach as a less expensive and more computationally efficient alternative to interpolation for the production of cover images to assure the reversibility of medical images.

Based on Fridrich's conventional chaos-based image cryptography architecture, Sefer and Abdulrahman [2] suggested employing a chaos-based medical picture encryption method that has a few fundamental operations. Each of the medical image encryption keys and medical-related data obtained by splitting the DICOM file was used as steganography data after the medical images were encrypted using the LSB method. In order to maximize the robustness against attack attempts, the researchers recommended that future work include implementing the hybrid model using other encryption techniques, such as AES with least significant bit algorithm or using the selected logistic map with a watermarking method, such as reversible watermark.

2. Methodology

2.1 Overview of the Proposed Framework

In this proposed framework, a modified method for securing medical imaging in a cloud context will be created. The medical image dataset will be obtained online from the DICOM (Digital imaging and communications in Medicine) standard form and passed into the system for compression. An enhanced Advanced Encryption System (AES-FFT) will be used for encryption and decryption, and a modified Discrete Wavelet Transform - Modified Particle Swarm Optimization (DWT-MPSO) will be used for steganography to hide patient information inside encrypted images Discrete Wavelet Transform - Modified Particle Swarm Optimization (DWT-MPSO). This included image decomposition, quantization, and determining appropriate sub-bands before encryption to reduce execution time. Peak signal-to-noise ratio (PSNR), mean square error (MSE), and encryption and decryption times will be used to assess the effectiveness of the established approaches.

2.2 Architecture of the Proposed Framework

The proposed framework's scheme is shown in Figure 1. Figure 2 depicted the proposed system's process schematic diagram. There are two ends to the authentication process: the sender/user end and the receiver end. The system would be split into two parts: symmetric cryptography and watermarking. The symmetric cryptography scheme AES-FFT will be used, with the same key to encrypt and decrypt the medical image file.

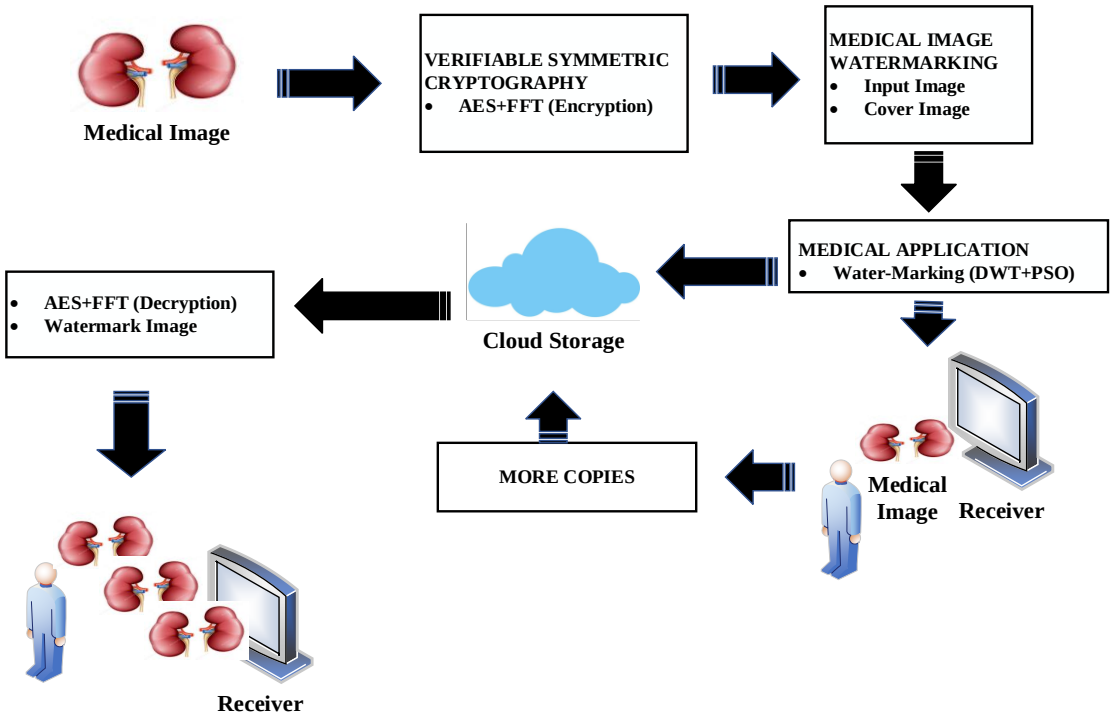

Figure 1: Schematic Diagram of the proposed framework

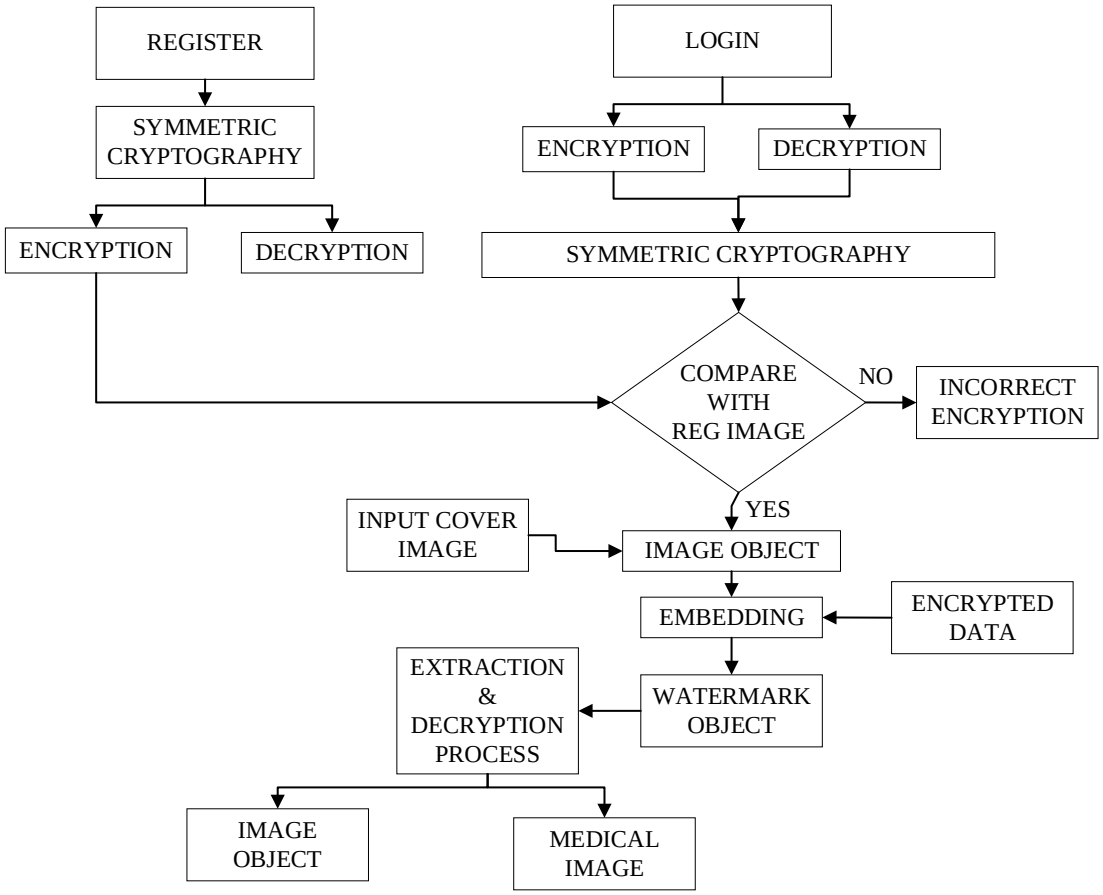

Figure 2: Overall System Architecture

3.0. Implementation View of the Proposed Framework

FFT will be used as a modification factor in the AES algorithm's Shift Row Transformation step and the mix column transformation. Figure 3 depicts the basic structure of the modification process. Every other step of the AES algorithm remains unchanged, with the exception of some changes at the "ShiftRows" and "MixColumn" levels using FFT, as detailed in section 3.4.2. The two modifications are described below.

1. ShiftRows: The first and fourth rows of the state remain unchanged if the element of the first row and column is even, while each byte in the second and third rows is cyclically shifted right over a different integer. The first and third rows of the state stay constant if the first row and first column elements are odd. However, each byte in the second and fourth rows of the state is cyclically shifted right over a new integer.
2. MixColumn: The mix column operates the 128-bit matrix, which is set up as a 4*4 state matrix, column by column. The new state matrix is obtained by multiplying the four elements of each column by the constant polynomial A(Y) = 03X4 + 01X3 + 01X2 + 01X + 02 with module X5+1. Swap the matrix's rows and columns after receiving the state matrix from step 1 of the process.

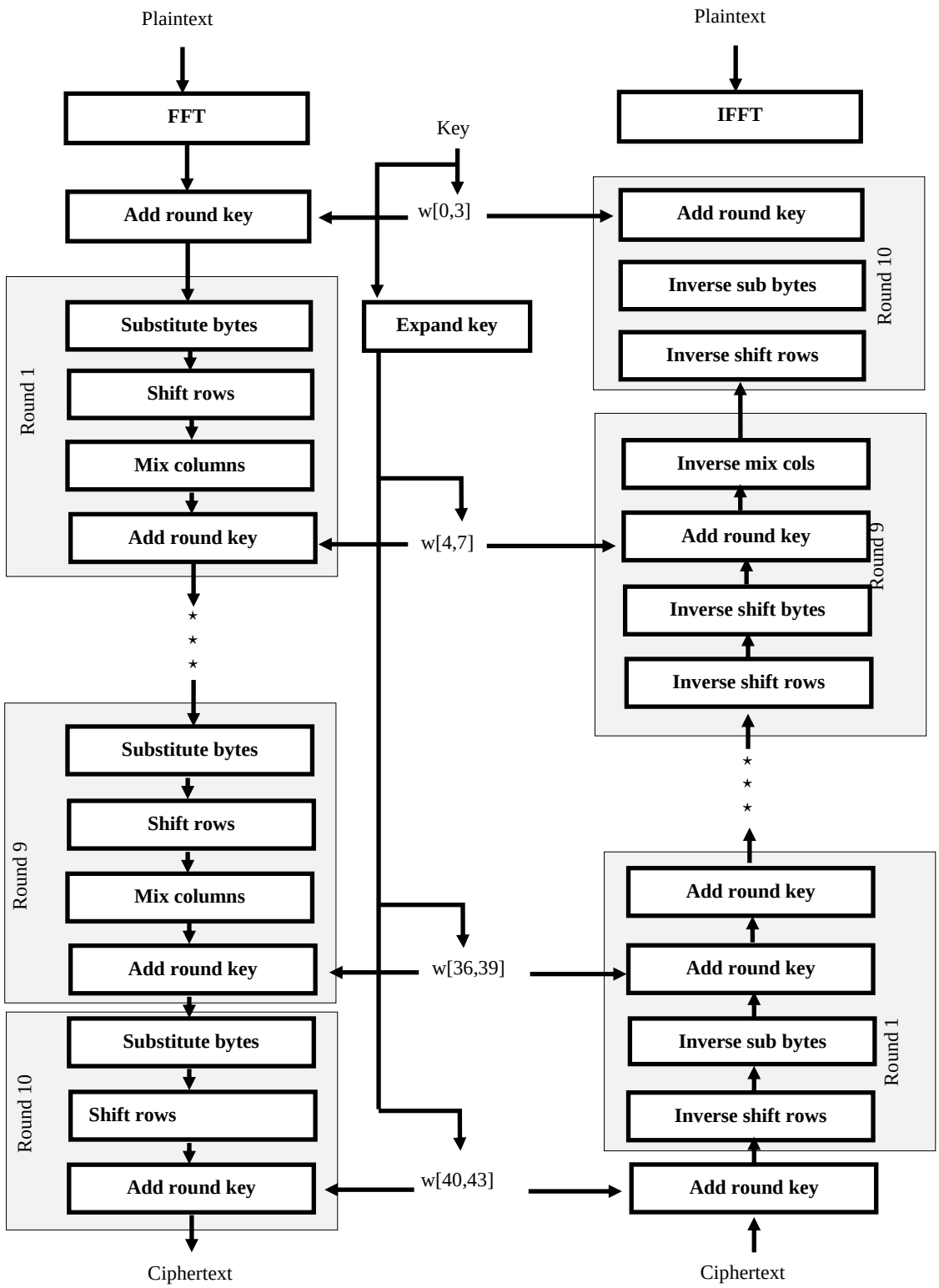

Figure 3: Basic Structure of AES-FFT

4. Conclusion

A Framework for Enhanced Advanced Encryption Standard of Medical Image in Cloud System Using Fast Fourier Transform is proposed in this paper. When implemented, this framework is expected to contribute to knowledge by demonstrating through experimental evidence that the use of FFT in conjunction with AES for encryption and decryption will be efficient in overcoming computational overhead when dealing with more complex medical images. It is also expected to demonstrate that the Discrete Wavelet Transform - Modified Particle Swarm Optimization (DWT-MPSO) technique can be used to improve the security, robustness, and quality of watermarked images.

References

[1] M Mbarek, K. Ali , Q. Hassan (2019). A Framework to Secure Medical Image Storage in Cloud Computing Environment. Journal of Electronic Commerce in Organizations vol. 23.2.

[2] K. Sefer, A.J. Abdulrahman (2018). Cloud System for Encryption and Authentication Medical Images. IOSR Journal of Computer Engineering (IOSR-JCE) Volume 20, Issue 1, Ver. II , pp. 65-75.

[3] K.K. Qusay, Y. Robiah, S.M. Hamid, S. A. Sayed, R.S. Siti (2017). A Review Study on Cloud Computing Issues. IOP Conf. Series: Journal of Physics: Conf. Series 1018 (2018) 012006 .

[4] S.G. Shini, T.Tony, K.Chithraranjan (2012). Cloud Based Medical Image Exchange-Security Challenges. Procedia Engineering vol. 38, PP 3454 – 3461.

[5] W. Botta, W Donato, V. Persico, A. Pescapé (2016). Integration of cloud computing and internet of things: a survey. Futur. Gener. Comput. Syst., vol. 56, pp. 684–700.

[6] U. Mustafa (2011). "Medical image security and EPR hiding using Shamir's secret sharing scheme," The Journal of Systems and Software, pp.1-10.

[7] C.B. Nyeem, (2013). Review of medical image watermarking requirements for teleradiology. Journal of Digital Imaging, vol. 26, pp 326 – 343.

[8] C. Lakshmi, K. Thenmozhi, J. B. Rayappan, S. Rajagopalan, R. Amirtharajan, N. Chidambaram, (2020). Neural-assisted image-dependent

[9] J. Daemen , V. Rijmen (2002). The Design of Rijndael," Springer-Verlag, 2002.

[10] N. J. Parmar, P. K Verma. (2017). A Comparative Evaluation of Algorithms in the Implementation of an Ultra-Secure Router-to-Router Key Exchange System. Security and Communication Networks. 1-7.

[11] https://www.commonlounge.com/discussion/e32fdd267aaa4240a4464723bc74d0a5. Retrived 1/16/2021

[12] https://www.skillset.com/questions/what-is-the-primary-drawback-to-using-advanced-encryption-standard-aes-algorithm-with-a-256-bit-key-to-share-sensiti-4254-p 2016. Retrived 1/16/2021

[13] J. Bincy, T. Senthilnathan (2019). An Efficient E2C 2 Visual Cryptographic Technique to Secure Medical Images in Cloud Environment. International Journal of Innovative Technology and Exploring Engineering (IJITEE). Volume-9 Issue-2, 4709-4714.

[14] A.A. Ijaz, S. Muhammad, U. H. Muhammad, S. Qaisar, A. Rizwan, A. Ditta, (2020). Secure Framework Enhancing AES Algorithm in Cloud Computing. Hindawi Security and Communication Networks Volume 2020, Article ID 8863345.

[15] https://en.wikipedia.org/wiki/Fast_Fourier_transform. Retrived 19th, July 2022.

[16] D.N. Rockwave (2000). The FFT: an algorithm the whole family can use. Computing in Science & Engineering vol. 2(1).

[17] O.D. Alowolodu, G.K Adelaja, B.K. Alese, O.C. Olayemi, (2018). Medical image security using quantum cryptography. Issues in Informing Science and Information Technology, vol. 15, pp. 57-67.

[18] K. Smita, V. Bellamkonda, Rajasthan (2018). Selective medical image watermarking and encryption for image security International Journal of Pure and Applied Mathematics Volume 118 No. 14.

[19] S. S. Askar, A.A. Karawia, A. Al-Khedhairi, F. S. Al-Ammar (2019). An Algorithm of Image Encryption Using Logistic and Two-Dimensional Chaotic Economic Maps. Entropy, VOL. 21, 44.

[20] M.I.Khalil (2017). Medical Image Steganography: Study of Medical Image Quality Degradation when Embedding Data in the Frequency Domain. I. J. Computer Network and Information Security, vol. 2, pp. 22-28

[21] S.A Parah, J.A.Sheikh, F. Ahad, (2017). Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimed Tools Appl vol. 76, pp. 10599–1